Arithmetical Definability over Finite Structures

Troy Lee
CWI and University of Amsterdam

December 17, 2003

Abstract

Arithmetical definability has been extensively studied over the natural numbers. In this paper, we take up the study of arithmetical definability over finite structures, motivated by the correspondence between uniform AC^0 and $\mathrm{FO}(\mathrm{PLUS}, \mathrm{TIMES})$. We prove finite analogs of three classic results in arithmetical definability, namely that $<$ and TIMES can first-order define PLUS, that $<$ and DIVIDES can first-order define TIMES, and that $<$ and COPRIME can first-order define TIMES.

The first result sharpens the equivalence $\mathrm{FO}(\mathrm{PLUS}, \mathrm{TIMES})$ $=$$\mathrm{FO}(\mathrm{BIT})$ to $\mathrm{FO}(<, \mathrm{TIMES}) = \mathrm{FO}(\mathrm{BIT})$, answering a question raised by Barrington et al. about the Crane Beach Conjecture. Together with previous results on the Crane Beach Conjecture, our results imply that $\mathrm{FO}(\mathrm{PLUS})$ is strictly less expressive than $\mathrm{FO}(<, \mathrm{TIMES}) = \mathrm{FO}(<, \mathrm{DIVIDES}) = \mathrm{FO}(<, \mathrm{COPRIME})$. In more colorful language, one could say that, for parallel computation, multiplication is harder than addition.

1 Introduction

Three classic results in arithmetical definability over the natural numbers are:

- Successor and multiplication can first-order define addition [1]
- Successor and the divisibility relation can first-order define multiplication [1]
- Ordering and the coprime relation can first-order define multiplication [2]

In this paper, we seek analogues of these results over finite structures — that is, where the universe and relations are restricted to $\{0, 1, \ldots, n-1\}$ for some n in N. Letting PLUS, TIMES, DIVIDES, COPRIME be the finite restrictions of the usual addition, multiplication, divisibility predicate, and coprime predicate, we show the following:

- Ordering and TIMES can first-order define PLUS (Thm 3.1)
- Ordering and DIVIDES can first-order define TIMES (Thm 4.1)
- Ordering and COPRIME can first-order define TIMES (Thm 5.2)

We also present two related negative definability results which are analogous to the situation in the natural numbers, namely that TIMES without ordering cannot first-order define PLUS, and that PLUS cannot first-order define TIMES.

Our interest in definability over finite structures stems from the connection between logical expressiveness and complexity. Since Fagin's result that the complexity class NP coincides with existential second-order logic [3] most complexity classes have been given a logical characterization (see [4]). Of particular interest in our case is the correspondence between the circuit class AC^0 and first-order logic, and more specifically the equivalence of uniform AC^0 and $\mathrm{FO}(\mathrm{PLUS}, \mathrm{TIMES})$. With this equivalence in mind, our main positive results can be summarized as:

$$\text{uniform } \mathrm{AC}^0 = \mathrm{FO}(<, \mathrm{TIMES}) = \mathrm{FO}(<, \mathrm{DIVIDES}) = \mathrm{FO}(<, \mathrm{COPRIME}).$$

One application of our work is to the Crane Beach Conjecture. The Crane Beach Conjecture expresses an intuition about the first-order definability of languages with a neutral letter. A neutral letter for a language L is a letter e which can be inserted and deleted from a string without affecting the membership of that string in L. The idea of the Crane Beach conjecture is that, if a language L has a neutral letter, then membership in L does not depend on a specific relationship between positions of letters in the string, only on the relative positions of these letters. Following this intuition, the Crane Beach Conjecture is formulated as follows:

If a language with a neutral letter can be defined in first-order logic using some set $\mathcal{P}$ of numerical predicates, then it can be defined using only the ordering relation.

A recent paper on the Crane Beach Conjecture [5] shows that the Crane Beach Conjecture is true for $\{\mathrm{PLUS}\}$ — that is any language with a neutral letter definable in $\mathrm{FO}(\mathrm{PLUS})$ is definable in $\mathrm{FO}(<)$ — yet false for $\{\mathrm{PLUS}, \mathrm{TIMES}\}$. These results combined with our Thm (10) imply that $\mathrm{FO}(\mathrm{PLUS})$ is strictly contained in $\mathrm{FO}(<, \mathrm{COPRIME}) = \mathrm{FO}(<, \mathrm{DIVIDES}) = \mathrm{FO}(<, \mathrm{TIMES})$.

For a set of numerical predicates $\mathcal{P}$, these initial results set up a potentially interesting connection between the theory of $\mathrm{FO}(\mathcal{P})$ over finite structures being decidable, how high $\mathrm{FO}(\mathcal{P})$ can count, roughly the number of ones a formula from $\mathrm{FO}(\mathcal{P})$ can identify in a string, and the Crane Beach Conjecture being true for $\mathcal{P}$. We discuss this connection further in the conclusions.

2 Preliminaries

2.1 First-Order Logic

We use the standard definitions of a structure and signature, and unless mentioned otherwise assume structures have a finite universe and a finite relational signature, that is, finitely many relation symbols. Specifically we will deal with first-order logic over finite strings from an alphabet A. We identify a word $w = w_0 \cdots w_{n-1}$, where each $w_i \in A$, with the structure $w = \langle \{0, \ldots, n-1\}, \sigma_A^w \rangle$. Here $\sigma_A^w = \{I_a : a \in A\}$ and $I_a = \{i < n : w_i = a\}$ is a unary predicate containing the positions in w which hold the letter a.

In addition to the predicates I_a, we will be considering numerical predicates. A k-ary numerical predicate P_n has, for every $n \in N$, a fixed interpretation $P_n \subseteq \{0, \ldots, n-1\}^k$. In other words, the interpretation of numerical predicates depends only on the size of the input, and not the underlying letters of a string. A basic numerical predicate is the linear ordering $<$ on the string positions. Other numerical predicates we will consider are

- $\mathrm{PLUS}(x, y, z)$ iff $x + y = z$
- $\mathrm{TIMES}(x, y, z)$ iff $x \times y = z$
- $\mathrm{BIT}(x, i)$ iff the ith bit in the binary representation of x is 1
- $\mathrm{DIVIDES}(x, y)$ iff $x | y$
- $\mathrm{COPRIME}(x, y)$ iff $x \perp y$

We use this notation to avoid confusion with the usual arithmetic operations over the natural numbers— remember in the above that the variables range over a finite universe n, and so represent numbers in

$\{0, \ldots, n-1\}$. In equations when there is no danger of confusion we will sometimes use the familiar symbols for these arithmetic operations to save space.

We take equality as a logical constant. Atomic σ formulas, then, are of the form $x_1 = x_2$ or $P(x_1, \ldots, x_k)$, where $x_1, \ldots, x_k$ are variables and $P \in \sigma$ is a relation symbol of arity k. First-order σ formulas are built in the usual way from atomic σ-formulas with Boolean connectives $\vee, \wedge, \neg$, and universal $\forall x$ and existential $\exists x$ quantifiers. For every alphabet and set of numerical predicates $\mathcal{P}$, we denote as $\mathrm{FO}(\mathcal{P})$ the set of first order $\sigma_A \cup \mathcal{P}$ formulas. The semantics of first-order formulas is defined in the usual way; for a string $w \in A^*$ and formula $\phi \in \mathrm{FO}(\mathcal{P})$ we write $w \models \phi$ if the structure corresponding to w is a model of ϕ.

Definition 1 *We say that a constant a is* definable *in $\mathrm{FO}(\mathcal{P})$ iff there is a formula $\phi \in \mathrm{FO}(\mathcal{P})$ with one free variable such that for all n and $x \in n$*

$$x = a \iff \phi(x).$$

Example 2 *The constant 0 is definable in $\mathrm{FO}(<)$ by the formula $\forall y(x < y \vee x = y)$.*

Definition 3 *We say that a k-ary numerical predicate P is* definable *in $\mathrm{FO}(\mathcal{P})$ iff there is a formula $\phi \in \mathrm{FO}(\mathcal{P})$ with k free variables such that for all n and $x_1, \ldots, x_k \in n^k$,*

$$P(x_1, \ldots, x_k) \iff \phi(x_1, \ldots, x_k).$$

Example 4 *As an easy example, note that $\mathrm{FO}(\mathrm{PLUS})$ can define ordering as follows:*

$$x < z \iff \exists y(\mathrm{PLUS}(x, y, z) \wedge \neg\mathrm{PLUS}(y, y, y)).$$

Thus $\mathrm{FO}(<, \mathrm{PLUS})$ and $\mathrm{FO}(\mathrm{PLUS})$ have the same expressive power. We will use this fact, and the more difficult fact that $\mathrm{FO}(\mathrm{BIT})$ can define ordering [6], to our notational convenience by not explicitly listing ordering in a set of predicates which contains PLUS or BIT. For comparison, note that Thm (12) says that $\mathrm{FO}(\mathrm{TIMES})$ cannot define ordering.

Example 5 *Another construction we will need to use later is that $\mathrm{FO}(\mathrm{BIT})$ can define PLUS—in fact, $\mathrm{FO}(\mathrm{BIT})$ can define addition of n-bit integers.*

To show this, we use the "carry-look-ahead" algorithm. To compute the ith bit of $X + Y$ we first see if a carry has been propagated to bit i:

$$\begin{aligned} \phi_{carry}(X, Y, i) &\equiv \exists j(j < i \wedge \mathrm{BIT}(X, j) \wedge \mathrm{BIT}(Y, j) \\ &\wedge \forall k(j < k < i \rightarrow \mathrm{BIT}(X, k) \vee \mathrm{BIT}(Y, k)) \end{aligned}$$

The formula $\phi_{carry}(X, Y, i)$ holds if a carry is generated at a position less than i and is then propagated through all the intervening positions. Now the i^{th} bit of $X + Y$ will be one if exactly one of $\mathrm{BIT}(X, i), \mathrm{BIT}(Y, i), \phi_{carry}(i)$ hold, or if all three of them hold. The easiest way to express this is with the exclusive or operation $\oplus$,

$$\begin{aligned} \alpha \oplus \beta &\equiv \alpha \leftrightarrow \neg\beta \\ \phi_{add}(X, Y, i) &\equiv (\mathrm{BIT}(X, i) \oplus \mathrm{BIT}(Y, i)) \oplus \phi_{carry}(X, Y, i) \end{aligned}$$

2.2 Languages and AC^0

Let A be an alphabet. A *language* $L \subset A^*$ is a set of finite strings composed of letters from A.

A boolean circuit is a directed acyclic graph with input nodes, output nodes, and nodes labelled AND, OR, and NOT. The input nodes have fan-in zero and the output nodes have fan-out zero. A circuit C_n with n input nodes and a single output node computes a boolean function from $\{0,1\}^n$ to $\{0,1\}$. We say that the circuit C_n *accepts* the word $w = w_0 w_1 \dots w_{n-1} \in \{0,1\}^n$ if C_n outputs 1 on input w. A circuit family $\{C_n\}_{n \in N}$ *recognizes* the language $L \in \{0,1\}^*$ iff for all n and $w \in \{0,1\}^i$,

$$C_n \text{ accepts } w \iff w \in L.$$

The circuit family $\{C_n\}$ has size $s(n)$ if each circuit C_n has at most s(n) nodes; it has depth $d(n)$ if the length of the longest path from an input node to an output node is at most $d(n)$. The language L is said to be in AC^0 if it is recognized by a family of circuits with depth $O(1)$ and size $n^{O(1)}$ consisting of NOT gates and unbounded fan-in AND and OR gates.

As mentioned earlier, the class AC^0 is of interest because of its connection with definability in first-order logic. This is made precise in the next theorem. The non-uniform version of this theorem is given as Thm 6.2 in [7]; the details needed for the uniform version and a description of DLOGTIME uniformity, now the most widely accepted uniformity condition for circuit classes, are given in [8].

Theorem 6 *Let L be a language over the alphabet $\{0,1\}$. Then the following are equivalent:*

1. *L is recognized by a $\mathrm{D}LOGTIME$ uniform family of AC^0 circuits.*
2. *Over the vocabulary $\sigma_{\{0,1\}}$ there is a sentence $\phi \in \mathrm{FO}(\mathrm{PLUS}, \mathrm{TIMES})$ whose set of finite models is L.*

2.3 Crane Beach Conjecture

We now state the Crane Beach Conjecture more formally.

Definition 7 *Let A be an alphabet and $L \subseteq A^*$. A letter $e \in A$ is called neutral for L if for any $u, v \in A^*$, it holds that $uv \in L$ iff $uev \in L$.*

As an example, 0 is a neutral letter for PARITY. As membership in PARITY only depends on the number of ones a string contains, zeros can be arbitrarily inserted to no effect. As PARITY is outside of non-uniform AC^0 [9], PARITY cannot be expressed in $\mathrm{FO}(\mathcal{P})$ for any set of numerical predicates $\mathcal{P}$.

An example of a language without a neutral letter in $\{0,1\}$ is $\{0^n 1^n : n \in N\}$, as membership in this language depends on a very specific numerical relationship between the positions of zeros and ones in the string. Though the language $\{0^n 1^n : n \in N\}$ cannot be defined in $\mathrm{FO}(<)$, the fact that the first half of the string is populated by only zeros and the second half only ones can be described in $\mathrm{FO}(\mathrm{PLUS})$.

The Crane Beach Conjecture expresses an intuition developed by examples like these.

Definition 8 *(Crane Beach Conjecture) Let $\mathcal{P}$ be a set of numerical predicates. We say the Crane Beach Conjecture is true for $\mathcal{P}$ iff every language $L \in \mathrm{FO}(<, \mathcal{P})$ that has a neutral letter is also definable in $\mathrm{FO}(<)$.*

A useful concept in relation to the Crane Beach Conjecture is *counting*.

Definition 9 *For a nondecreasing function $f(n) \leq n$, the logical system $\mathrm{FO}(\mathcal{P})$ is said to* count up to $f(n)$ *if there is a formula $\phi \in \mathrm{FO}(\mathcal{P})$ such that for all n and $w \in \{0,1\}^n$,*

$$w \models \phi(c) \iff c \leq f(n) \wedge c = \text{number of ones in } w.$$

It is conjectured in [5] that the Crane Beach is true of a set of numerical predicates $\mathcal{P}$ iff $\mathrm{FO}(\mathcal{P})$ cannot count beyond a constant.

3 Defining PLUS with TIMES and ordering

Julia Robinson defined addition with multiplication and successor by the following formula:

$$x + y = z \iff S(x \cdot z) \cdot S(y \cdot z) = S(z \cdot z \cdot S(x \cdot y)). \tag{1}$$

This formula, however, cannot be naïvely applied to define addition over finite structures. When x, y satisfy $n^{1/4} < x, y < n/2$ then $x + y < n$ and so $\mathrm{PLUS}(x, y, z)$ holds for some $z \in n$. Yet in this case $S(x \cdot z) \cdot S(y \cdot z) > n$ and thus this product cannot be defined with TIMES.

We proceed by a different method to show that addition can be defined over finite structures with multiplication and ordering.

Theorem 10 *Let τ be a vocabulary that includes ordering. If $\mathrm{TIMES} \in \tau$ then PLUS is first-order definable.*

Proof: With ordering, we can define the constant 0 and the successor relation. Thus we can also define any constant k, in particular the constant 2. Clearly with TIMES we can define the relations, "x divides y" and "y is prime". With these we can then define the relation "y is a power of 2" as y is a power of 2 iff all the prime divisors of y are equal to 2. This relation is denoted $p_2(y)$.

We now define the relation $\mathrm{BIT}'(x, y)$, which holds iff $y = 2^i$ and $\mathrm{BIT}(x, i)$. That is, $\mathrm{BIT}'(x, 2^i)$ iff $\lfloor x/2^i \rfloor$ is odd, which we can define in $\mathrm{FO}(<, \mathrm{TIMES})$ as follows:

$$\mathrm{BIT}'(x, y) \equiv p_2(y) \wedge \exists u(y(S(2u)) \leq x \ \wedge \ x < y(S(S(2u)))).$$

With $\mathrm{BIT}'(x, y)$ we can define PLUS using the carry-look-ahead method described in example (2.5), over powers of 2. $\square$

Remark 11 *Although $\mathrm{BIT}'(x, y)$ seems unnatural as an arithmetic predicate, it is in fact FO equivalent to an extensively studied arithmetical predicate, Pascal's triangle modulo 2, denoted $B_2(x, y)$. See, for example, [10] and [11]. $B_2(x, y)$ is the binomial coefficient $\binom{x+y}{x}$ modulo 2, and the essence of its definability properties derive from Lucas' theorem, which implies that $B_2(x, y) = 0$ iff there exists z such that $\mathrm{BIT}'(x, z)$ and $\mathrm{BIT}'(y, z)$.*

We can also define BIT' using B_2. Let $x \sqsubseteq y$ mean that in each position of a one in the binary representation of x there is a one in the binary representation of y. This can be defined by

$$x \sqsubseteq y \iff \forall z(B_2(x, z) = 0 \rightarrow B_2(y, z) = 0).$$

We can now define a predecessor relation $\prec$ in the partially ordered set formed by $\langle n; \sqsubseteq \rangle$,

$$x \prec y \iff x \sqsubseteq y \wedge \neg \exists z(x \sqsubseteq z \wedge z \sqsubseteq y).$$

Powers of 2 can now be defined quite simply: x is a power of 2 iff $0 \prec x$. We can also define carry-free addition by

$$CFadd(x, y, z) \iff B_2(x, y) \wedge x \sqsubseteq z \wedge y \subseteq z \wedge \forall w(x \sqsubseteq w \wedge y \sqsubseteq w \rightarrow z \sqsubseteq w).$$

Now we can define $\mathrm{BIT}'(x, y)$ by

$$\mathrm{BIT}'(x, y) \iff 0 \prec y \wedge \exists z(CFadd(z, y, x)).$$

Theorem 12 $\mathrm{FO}(\mathrm{TIMES})$ *cannot first-order define* PLUS *or ordering.*

Proof: As discussed in [1], multiplication cannot first-order define addition over the positive integers. This can be seen since isomorphisms preserve the truth of first-order formulas, yet there are automorphisms of the positive integers with respect to multiplication which permute the primes in an arbitrary way, thus not preserving addition. This method of proof is attributed to Padoa [12].

Being a bit careful, we can adopt this idea to show that $\mathrm{FO}(\mathrm{TIMES})$ cannot define ordering. Note that this implies that $\mathrm{FO}(\mathrm{TIMES})$ cannot define PLUS as well, since PLUS can first-order define ordering. By Bertrand's Postulate [1] for any $m \geq 1$ there is a prime between m and $2m$. More recent results of Pintz [15] that there is always a prime between m and $m + m^{17/31}$ can be used to show that for $m \geq 7$ we can always find two primes between m and $2m$. (Note that by the prime number theorem there are really about $m/\log m$ primes between m and $2m$.) Thus we can define an automorphism on the structure $\langle n, \mathrm{TIMES}\rangle$ by permuting two primes p_1, p_2 satisfying $n/2 < p_1, p_2 < n$. This mapping does not preserve ordering, and by the choice of these primes, the only relation we must check to see that TIMES is preserved is $\mathrm{TIMES}(1, p_{1,2}, p_{1,2}) \iff \mathrm{TIMES}(1, f(p_{1,2}), f(p_{1,2}))$, which clearly holds.

□

As work on the Crane Beach Conjecture has shown that the Crane Beach Conjecture is false for $\mathrm{FO}(\mathrm{PLUS}, \mathrm{TIMES})$, our Thm (10) implies that the Crane Beach Conjecture is also false for $\mathrm{FO}(<, \mathrm{TIMES})$. This has the consequence that $\mathrm{FO}(<, \mathrm{TIMES})$ is strictly more expressive than $\mathrm{FO}(\mathrm{PLUS})$.

Corollary 13 $\mathrm{FO}(\mathrm{PLUS}) \subset \mathrm{FO}(<, \mathrm{TIMES})$

Proof: As the Crane Beach Conjecture is false for $\mathrm{FO}(<, \mathrm{TIMES})$, there is a language L with a neutral letter definable in $\mathrm{FO}(<, \mathrm{TIMES})$ but not in $\mathrm{FO}(<)$. But L is not definable in $\mathrm{FO}(\mathrm{PLUS})$ as every language with a neutral letter definable in $\mathrm{FO}(\mathrm{PLUS})$ is definable in $\mathrm{FO}(<)$. □

4 Defining TIMES with DIVIDES and ordering

We again cannot naïvely use Julia Robinson's definition as it breaks down on finite structures in the same way as her definition of addition in formula (1).

We proceed by first showing that DIVIDES can express simpler predicates like "z is the least common multiple of x and y", denoted $\mathrm{LCM}(x, y, z)$, and "z is the greatest common divisor of x and y", denoted $\mathrm{GCD}(x, y, z)$. To conserve space in equations, we will write DIVIDES with the traditional | symbol.

$$\begin{aligned}
\mathrm{LCM}(x, y, z) &\equiv (x|z \wedge y|z \wedge \forall z'(x|z' \wedge y|z' \rightarrow z \leq z')) \\
\mathrm{GCD}(x, y, z) &\equiv (z|x \wedge z|y \wedge \forall z'(z'|x \wedge z'|y \rightarrow z' \leq z))
\end{aligned}$$

The key of our approach to defining TIMES is the fact that if the GCD of x and y is 1, that is if x and y are relatively prime, then the LCM of x and y is their product, $\mathrm{LCM}(x, y, xy)$.

Theorem 14 *Let τ be a vocabulary that includes ordering. If* $\mathrm{DIVIDES} \in \tau$ *then* TIMES *is first-order definable. In particular,* $\mathrm{FO}(<, \mathrm{DIVIDES}) = \mathrm{FO}(<, \mathrm{TIMES})$.

[1] First proved by Chebychev in 1850. For details, see [13] or the friendly treatment in *The Book* [14].

Proof: Let $x, y \in n$. We wish to express the product xy using DIVIDES and ordering. As before we can define 0 in $\mathrm{FO}(<, \mathrm{DIVIDES})$, and easily handle the case where x or y is zero. Now assuming x and y are nonzero, we can break x uniquely into two parts z_1 and z_2 such that $x = z_1 z_2$ and z_1 is the largest factor of x relatively prime to y.

Claim 15 *z_1 and z_2 are relatively prime.*

Proof: Suppose p is a prime dividing both z_1 and z_2. Either p divides y or p does not divide y. If p divides y then p cannot divide z_1 as z_1 and y are relatively prime by definition. On the other hand, if p does not divide y then $z_1 p$ would be relatively prime to y, contradicting the definინition of z_1. □

We also need to check that z_1, z_2 can be so defined in $\mathrm{FO}(<, \mathrm{DIVIDES})$.

$$z_1 | x \wedge \mathrm{GCD}(z_1, y, 1) \wedge \forall z_1' (z_1' | x \wedge \mathrm{GCD}(z_1', y, 1) \rightarrow z_1' \leq z_1)$$

$$\mathrm{GCD}(z_1, z_2, 1) \wedge \mathrm{LCM}(z_1, z_2, x)$$

We have now reduced the problem to defining the product $z_2 y$. As z_1 is relatively prime to z_2 and relatively prime to y, it is also relatively prime to the product $z_2 y$. Thus if we can define $z_2 y$, then we can define $z_1 z_2 y$ as $\mathrm{LCM}(z_1, z_2 y)$.

Now z_2 does not necessarily divide y, but because of our definition of z_1, every prime divisor of z_2 is also a prime divisor of y.

Claim 16 *z_2 and $y + 1$ are relatively prime*

Proof: Assume there exists a prime $p > 1$ such that $p | z_2$ and $p | y + 1$. But as p is a factor of z_2, it is also a factor of y, thus $p | y$. Then $p | (y + 1 - y)$ which implies that p divides 1, a contradiction. □

The same reasoning can be used to show $\mathrm{GCD}(z_2, y - 1, 1)$. Thus as z_2 is relatively prime to $y - 1$ and $y + 1$, we can define the products $z_2(y - 1) = \mathrm{LCM}(z_2, y - 1)$ and $z_2(y + 1) = \mathrm{LCM}(z_2, y + 1)$. We use these products to bookend the product $z_2 y$.

Claim 17 $z_2 y = t \iff z_2(y - 1) < t < z_2(y + 1) \wedge z_2 | t$

Proof: $\Rightarrow$ $z_2(y - 1) < z_2 y < z_2(y + 1)$ and $z_2 | z_2 y$

$\Leftarrow$ Since $z_2 | t$ there is some k such that $t = z_2 k$. By the inequality, we have

$$z_2(y - 1) < z_2 k < z_2(y + 1).$$

As z_2 is not zero,

$$y - 1 < k < y + 1.$$

Thus $k = y$, and so $t = z_2 y$. □

□

5 Defining TIMES with COPRIME and ordering

In his thesis [2], Alan Woods shows that there is a bounded first-order formula with ordering and the coprime relation which defines multiplication over the natural numbers. It turns out that his method also works for our case. We follow the argument of his proof here, checking that it satisfies our needs.

Lemma 18 $\mathrm{FO}(\mathrm{PLUS}, \mathrm{COPRIME})$ *can define* TIMES.

Proof: First we note that we can define the relation $\mathrm{prime}(y)$, meaning that y is prime, in $\mathrm{FO}(\mathrm{PLUS}, \mathrm{COPRIME})$ by

$$\mathrm{prime}(y) \iff y \neq 0 \wedge y \neq 1 \wedge \forall x(0 < x < y \to \mathrm{COPRIME}(x, y)).$$

We can define multiplication over primes, as the product of primes p_1, p_2 is the smallest nonzero number not coprime to both p_1 and p_2.

$$\begin{array}{rcl} \mathrm{TIMES}(p_1, p_2, z) & \iff & 1 < z \wedge \neg\mathrm{COPRIME}(p_1, z) \wedge \neg\mathrm{COPRIME}(p_2, z) \wedge \\ & \forall & x(1 < x \wedge \neg\mathrm{COPRIME}(p_1, z) \wedge \neg\mathrm{COPRIME}(p_2, z) \to z \leq x) \end{array}$$

To define TIMES in general, we can use the fact that every integer can be expressed as the sum of fewer than a finite number k of primes [16]. Although all we require is for k to be finite, it is interesting to know that more recent results [17] show that we can take k as 7. Thus for $x, y \geq 2$, there exists $p_1, \dots, p_7$ and $q_1, \dots, q_7$ where each p_i, q_i is prime or zero, and such that $x = \Sigma_i p_i$ and $y = \Sigma_i q_i$. Then we can define TIMES as the sum of a constant number (fewer than 49) of products of primes,

$$\mathrm{TIMES}(x, y, z) \iff z = \sum_{i,j} p_i q_j.$$

$\square$

Theorem 19 *Let τ be a vocabulary that includes ordering. If* $\mathrm{COPRIME} \in \tau$ *then* TIMES *is first-order definable. In particular,* $\mathrm{FO}(<, \mathrm{COPRIME}) = \mathrm{FO}(<, \mathrm{TIMES})$.

Proof: By Lemma (18) it suffices to define PLUS in $\mathrm{FO}(<, \mathrm{COPRIME})$. Lemma (20) gives a method to define addition, which, as we will see in Lemma (21), can be formulated in a first-order way. Recall that, for a real number a the floor function $\lfloor a \rfloor$ gives the greatest integer $\leq a$, and for all real numbers a, b the following inequality holds:

$$\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor \leq \lfloor a \rfloor + \lfloor b \rfloor + 1. \tag{2}$$

Lemma 20 *$z = x + y$ iff z is the least number such that:*

1. $x \leq z \wedge y \leq z$
2. $z \equiv x + y \pmod 6$
3. *For every prime $p \leq z$ and $p \neq 7$, either*

$$\begin{array}{rcl} \left\lfloor \frac{z}{p} \right\rfloor & \equiv & \left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{y}{p} \right\rfloor \pmod 7 \\ \text{or } \left\lfloor \frac{z}{p} \right\rfloor & \equiv & \left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{y}{p} \right\rfloor + 1 \pmod 7 \end{array}$$

Proof: Clearly, $z = x + y$ satisfies the three given conditions, thus we must show that for any $z < x + y$ one of these conditions must fail. Suppose $z < x + y$ satisfies (1) and (2). By (2) we have $x + y - z = 6m$ for some $m \geq 1$. By Bertrand's Postulate for any $n \geq 1$ there is a prime p satisfying $n \leq p \leq 2n$. Thus with a quick check we see that for any $m \geq 1$ there is a prime $p \neq 7$ such that $\frac{3}{2}m \leq p \leq 3m$. Hence there is a prime $p \neq 7$ satisfying $2p \leq x + y - z \leq 4p$.

It follows that $2 \leq \left\lfloor \frac{x}{p} + \frac{y}{p} - \frac{z}{p} \right\rfloor \leq 4$. Using (2), we obtain

$$2 + \left\lfloor \frac{z}{p} \right\rfloor \leq \left\lfloor \frac{x}{p} + \frac{y}{p} \right\rfloor \leq 5 + \left\lfloor \frac{z}{p} \right\rfloor,$$

and once more gives,

$$1 + \left\lfloor \frac{z}{p} \right\rfloor \leq \left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{y}{p} \right\rfloor \leq 5 + \left\lfloor \frac{z}{p} \right\rfloor.$$

This means that

$$\left\lfloor \frac{z}{p} \right\rfloor - \left\lfloor \frac{x}{p} \right\rfloor - \left\lfloor \frac{y}{p} \right\rfloor = -1, -2, -3, -4, \text{or} -5.$$

So

$$\left\lfloor \frac{z}{p} \right\rfloor - \left\lfloor \frac{x}{p} \right\rfloor - \left\lfloor \frac{y}{p} \right\rfloor \not\equiv 0, 1 \pmod 7$$

As $p \leq x + y - z \leq z + z - z = z$ by condition (1), condition (3) fails. □

Lemma 21 PLUS *can be defined in* $\mathrm{FO}(<, \mathrm{COPRIME})$.

Proof: We show that the three conditions above can be defined in $\mathrm{FO}(<, \mathrm{COPRIME})$.

Condition (1) is clear.

For condition (2), suppose that $z \equiv k \pmod 6$. To define $x + y \equiv z \pmod 6$ we notice that this only happens when $x \equiv i \pmod 6$ and $y \equiv j \pmod 6$ and $i + j \equiv k \pmod 6$. We can define $x \equiv i \pmod 6$ as $x = i \vee (x \geq 6 \wedge \neg(2 \perp x - i) \wedge \neg(3 \perp x - i))$. Thus

$$x + y \equiv z \pmod 6 \iff \bigvee_{\substack{i,j,k \leq 5 \\ i+j=k \pmod 6}} (x \equiv i \pmod 6 \wedge y \equiv j \pmod 6 \wedge z \equiv k \pmod 6).$$

In condition (3) we can do addition mod 7 similarly to above, thus it is enough to define

$$\mathrm{prime}(p) \wedge p \neq 7 \wedge \left\lfloor \frac{x}{p} \right\rfloor \equiv i \pmod 7$$

in $\mathrm{FO}(<, \mathrm{COPRIME})$. We showed how to define $\mathrm{prime}(p)$ above. To define $\left\lfloor \frac{x}{p} \right\rfloor \equiv i \pmod 7$ notice that if x satisfies this condition iff there is a $u \leq x$ such that $\neg\mathrm{COPRIME}(p, u) \wedge \neg\mathrm{COPRIME}(7, u)$ and with there being exactly i distinct numbers v satisfying $u < v \leq x \wedge \neg\mathrm{COPRIME}(p, v)$. To see this more explicitly:

$$u = 7pw < p(7w + 1) < p(7w + 2) < \cdots < p(7w + i) \leq x < p(7w + i + 1)$$

□

□

6 Discussion

The results presented here all indicated analogies between definability on finite structures and the case over the natural numbers. The similarities continue on the unknown side as well. Similar to the "gap" in undecidability, that is the rarity of known structures which are undecidable yet unable to define multiplication and addition, there is a gap in counting in the finite case—there are no natural predicates (that is other than purely counting predicates) known which can count beyond a constant yet which do not have the full definability of PLUS and TIMES. Perhaps this is only a superficial resemblence created by our lack of imagination in defining predicates, but it presents a tantalizing connection between decidability, counting, and the Crane Beach Conjecture.

In this paper we did not consider definability with the successor relation. This was in part because order seems like a more natural relation on finite structures and also because in applications to complexity ordering is almost always assumed to be present. However, the most outstanding open problem in arithmetical definability, originally posed in [1], involves successor—can successor and the coprime relation first-order define multiplication? Alan Woods [2] furthered interest in this question, which has been coined Robinson's problem, by showing a positive answer is equivalent to the existence of a $k \in N$ such that for all pairs (x, y), if $x + i$ and $y + i$ have the same prime divisors for all $0 \leq i \leq k$ then $x = y$. This last statement is a weakening of a conjecture made by Erdős, now called the Woods-Erdős conjecture. The finite version of Robinson's problem might be interesting to investigate: though a positive answer is most likely difficult—even a positive resolution of the Woods-Erdős conjecture does not obviously help—perhaps a negative answer could be obtained.

Acknowledgments

We would like to thank David Mix Barrington and Neil Immerman for introducing us to this problem and for many helpful discussions. Steven Lindell provided many insights on a earlier draft of this paper, including suggesting a simplified proof of Thm (3.1), which is presented here. This work also benefitted from discussions with Alan Woods, Alexis Bès, Harry Buhrman and the helpful comments of the anonymous referee.

References

[1] J. Robinson, Definability and decision problems in arithmetic, The Journal of Symbolic Logic **14**, pp. 98–114 (1949).

[2] A. Woods, Ph.D. Thesis, University of Manchester (1981).

[3] R. Fagin, Generalized first-order spectra and polynomial-time recognizable sets, Complexity of Computation, SIAM-AMS Proceedings Vol. 7, pp. 43–73, (1974).

[4] N. Immerman, Descriptive Complexity (Springer-Verlag, New York, 1998).

[5] D. A. Mix Barrington, N. Immerman, C. Lauteman, N. Schweikardt and D. Thérien, The Crane Beach conjecture, in LICS'01, pp. 187–196, 2001.

[6] A. Dawar, Elementary properties of finite ranks, Math. Logic Quart. **44**, pp. 349–353 (1998).

[7] N. Immerman, Languages that capture complexity classes, SIAM J. of Comp. **16**, pp. 760–778 (1987).

[8] D. A. Mix Barrington, N. Immerman, and H. Straubing, On uniformity within NC^1, J. Comp. Sys. Sci. **41**, pp. 274–306 (1990).

[9] M. Furst, J. Saxe, and M. Sipser, Parity, circuits, and the polynomial-time hierarchy, Math. Sys. Theory, **17**, pp. 13–27 (1984).

[10] I. Korec, Structures related to Pacal's Triangle modulo 2 and their elementary theories, Math. Slovaca **44**, pp. 531-554 (1994).

[11] A. Bès, Ann. Pure App. Logic **89**, 17–35 (1997).

[12] A. Padoa, Un nouveau système irréductible de postulats pour l'algèbre, in: Comptes rendus du 2-e Congrès International des Mathématiciens", pp. 249–256 (1902).

[13] G. Hardy and E. Wright, An Introduction to the Theory of Numbers (Oxford University Press, London, 1960).

[14] M. Aigner and G. Ziegler, Proofs from the Book (Springer-Verlag, Berlin, 1998), pp. 7–12.

[15] J. Pintz, On primes in short intervals, Studia Sci. Math. Hungar. **19**, pp. 89–96 (1984).

[16] L. Schnirelmann, Über additive Eigenschaften von Zahlen, Math. Ann. **107**, pp. 649–690 (1933).

[17] O. Ramaré, On Schnirelmann's constant, Ann. Sc. Norm. Super Pisa **22**, pp. 645–706 (1995).