DEPOSIT

Some New Results in Monadic Second-Order Arithmetic

STANISLAV O. SPERANSKI
Sobolev Institute of Mathematics, Novosibirsk, Russia

This is a version of the article published in
Computability 4:2, 159–174 (2015). DOI: 10.3233/COM-150036

Abstract. Let σ be a signature and $\mathfrak{A}$ a σ-structure with domain $\mathbb{N}$. Say that a monadic second-order σ-formula is Π^1_n iff it has the form

$$\forall X_1 \, \exists X_2 \, \forall X_3 \, \ldots \, X_n \, \psi$$

with $X_1, \ldots, X_n$ set variables and ψ containing no set quantifiers. Consider the following properties:

- `AC` for each $n \in \mathbb{N} \setminus \{0\}$, the set of Π^1_n-σ-sentences true in $\mathfrak{A}$ is Π^1_n-complete;
- `AD` for each $n \in \mathbb{N} \setminus \{0\}$, if $A \subseteq \mathbb{N}$ is Π^1_n-definable in the standard model of arithmetic and closed under automorphisms of $\mathfrak{A}$, then it is Π^1_n-definable in $\mathfrak{A}$.

We use $\mid$ and $\perp$ to denote the divisibility relation and the coprimeness relation, respectively. Given a prime p, let bc_p be the function which maps every $(x, y) \in \mathbb{N} \times \mathbb{N}$ into $\binom{x+y}{x} \bmod p$. In this paper we prove: $\langle \mathbb{N}, \mid \rangle$ and all $\langle \mathbb{N}, \mathsf{bc}_p, = \rangle$ have both `AC` and `AD`; in effect, even $\langle \mathbb{N}, \perp \rangle$ has `AC`. Notice — these results readily generalise to arbitrary arithmetical expansions of the corresponding structures, provided that the extended signature is finite.

§1. Introduction

Let $\mathsf{f}_0, \mathsf{f}_1, \ldots$ be a list of all computable functions and $\mathsf{R}_0, \mathsf{R}_1, \ldots$ be a list of all computable relations. Then the standard model $\mathfrak{N}$ of arithmetic expands to

$$\mathfrak{T} \;:=\; \langle \mathbb{N}, \mathsf{f}_0, \mathsf{f}_1, \ldots, \mathsf{R}_0, \mathsf{R}_1, \ldots \rangle.$$

The paper is devoted to monadic second-order properties of natural reducts of $\mathfrak{T}$ — which are considerably less studied than first-order properties of such structures (see (Bès, 2002; Korec, 2001; Cegielski, 1996) for further information and references). More precisely, we shall concentrate on issues of computability and definability.

For each $n > 0$, consider the class $\mathscr{A}_n$ of Π^1_n-sets. From now on assume all Π^1_n-formulas are monadic and contain exactly n set quantifiers.

FOLKLORE. *For any $A \subseteq \mathbb{N}$ and $n > 0$, the following hold:*

i. $A \in \mathscr{A}_n$ *iff A is definable in $\mathfrak{N}$ by a Π^1_n-formula;*
ii. $A \in \mathscr{A}_n$ *iff A is m-reducible to the set of Π^1_n-sentences true in $\mathfrak{N}$.*

This fact is closely connected with the fundamental properties we shall be interested in, i. e. `AC` and `AD`. Given the reduct $\mathfrak{A}$ of $\mathfrak{T}$ to a finite signature, they say (for all A and n):

- `AC` one can replace $\mathfrak{N}$ in (ii) by $\mathfrak{A}$;
- `AD` whenever A is closed under automorphisms of $\mathfrak{A}$, one can replace $\mathfrak{N}$ in (i) by $\mathfrak{A}$.

The article illustrates an attractive general approach to proving that certain structures have `AC` and/or `AD` (actually the first steps towards our present framework were already taken in (Speranski, 2013)) — these properties can be employed for establishing complexity lower bounds in the context of the analytical hierarchy, for example, cf. (Speranski, 2015).

© 2015 Author

2 August 2016

Certain naturally arising reducts of $\mathfrak{T}$ have gained much popularity in logic and computer science over the last several generations. The research programme focuses on

1. issues of computability and definability in the first-order setting, and
2. issues of computability and definability in the monadic second-order setting.

Substantial progress has been made in (1). While (2) remain largely unstudied. One of the most important exceptions deals with the successor function s:

THEOREM (Büchi, 1962). *The monadic second-order theory of* $\langle \mathbb{N}, \mathsf{s}, = \rangle$ *is decidable.*

The same holds for $\langle \mathbb{N}, < \rangle$. And the analogous result for the binary tree can be found in (Rabin, 1969). The situation with $+$ points towards degrees of unsolvability, however.

THEOREM (Halpern, 1991). *The set of* Π^1_1*-sentences true in* $\langle \mathbb{N}, +, = \rangle$ *is* Π^1_1*-complete.*

Halpern's proof, being designed for this special complexity result, could not shed much light on AD or AC with $n > 1$. Luckily a very different line of reasoning leads to

THEOREM (Speranski, 2013). $\langle \mathbb{N}, +, = \rangle$ *has* AC *and* AD. $\langle \mathbb{N}, \times, = \rangle$ *has* AC.

As expected, we shall analyse (2) with the help of (1) — keeping in mind that $\mathfrak{N}$ can be identified with every arithmetical structure in which $+$ and $\times$ are first-order definable (but for applications to AC and the like, interpretability should suffice). The reader may consult (Korec, 2001) for a collection of 'variants of $\mathfrak{N}$'. In particular those discovered by A. Bès, I. Korec and D. Richard will play a role.

A few words about the reducts we shall be concerned with are in order. Structures associated with the divisibility relation $|$ and the coprimeness relation $\perp$ have achieved quite a lot of attention since (Robinson, 1949). Intuitively, our theorems below may be contrasted with the well-known decidability results obtained in (Büchi, 1962; Rabin, 1969). Modular Pascal's triangles were intensively explored during the 1990's. We list them as

$$\mathscr{B}_2,\ \mathscr{B}_3,\ \ldots$$

where for any $k \geqslant 2$, $\mathscr{B}_k$ denotes the algebra whose only operation is given by

$$\mathsf{bc}_k(x,y) \;=\; \binom{x+y}{x} \bmod k.$$

As a matter of fact, it will turn out that — in view of some earlier contributions of A. Bès, I. Korec and the author — we only need to investigate every $\langle \mathbb{N}, \mathsf{bc}_p, = \rangle$ with p prime.

Among other things, we shall answer the questions emerging from (Speranski, 2013):

Does $\langle \mathbb{N}, \times, = \rangle$ *have* AD*?* *Does* $\langle \mathbb{N}, | \rangle$ *have* AC *and* AD*?*

The rest of the paper is organised as follows. §2. consists of preliminary material. In §3. we develop our basic ideas into an efficient tool, which is used to prove $\langle \mathbb{N}, | \rangle$ has AC and AD. §4. presents a slight variant of our technique, yielding AC and AD for each $\langle \mathbb{N}, \mathsf{bc}_p, = \rangle$. In §5. we show how one can derive sharper complexity results by exploiting the notion of (first-order) interpretability instead of that of definability (but the price paid for this is that such arguments do not take AD into account): even $\langle \mathbb{N}, \perp \rangle$ has AC. We conclude the article with a few general comments.

§**2. Preliminaries** In monadic second-order arithmetic we have

i. *individual variables* $x, y, z, \dots$ (intended to range over $\mathbb{N}$) and
ii. *set variables* $X, Y, Z, \dots$ (intended to range over all subsets of $\mathbb{N}$).

Accordingly we distinguish between *individual* and *set quantifiers*:

$$\forall x, \exists x, \forall y, \exists y, \forall z, \exists z, \dots \quad \text{and} \quad \forall X, \exists X, \forall Y, \exists Y, \forall Z, \exists Z, \dots$$

Let σ be a signature, i. e. a collection of constant, function and predicate symbols, each of which is assigned an arity. *Monadic second-order σ-formulas* are built up from first-order atomic σ-formulas and expressions of the form $t \in X$ with t a (first-order) σ-term and X a set variable using connective symbols and quantifiers in the customary way.

A monadic second-order σ-formula is Π^1_n, where $n \in \mathbb{N} \setminus \{0\}$, iff it has the form

$$\underbrace{\forall X_1 \, \exists X_2 \, \forall X_3 \dots X_n}_{n-1 \text{ alternations}} \, \psi$$

with $X_1, \dots, X_n$ set variables and ψ containing no set quantifiers. Still, throughout this text "definable" and "formula" mean "first-order definable" and "first-order formula", respectively, unless otherwise indicated (like in "defined by a Π^1_n-formula" or "Π^1_n-definable").

For a σ-structure $\mathfrak{A}$ with domain $\mathbb{N}$, we bring in the following notation:

$$\begin{aligned} \mathrm{Def}(\mathfrak{A}) &:= \text{the collection of all sets definable in } \mathfrak{A}, \\ \mathrm{Aut}(\mathfrak{A}) &:= \text{the collection of all automorphisms of } \mathfrak{A}, \\ \mathrm{Th}^1(\mathfrak{A}) &:= \text{the first-order theory of } \mathfrak{A}, \quad \text{and} \\ \mathrm{Th}^*(\mathfrak{A}) &:= \text{the monadic second-order theory of } \mathfrak{A}. \end{aligned}$$

We shall be concerned with two fundamental properties:

`AC` for every $n \in \mathbb{N} \setminus \{0\}$, the Π^1_n-fragment of $\mathrm{Th}^*(\mathfrak{A})$ is Π^1_n-complete;
`AD` for every $n \in \mathbb{N} \setminus \{0\}$, if $A \subseteq \mathbb{N}$ is Π^1_n-definable in $\mathfrak{N} := \langle \mathbb{N}, 0, \mathsf{s}, +, \times, = \rangle$ and closed under $\mathrm{Aut}(\mathfrak{A})$, then it is Π^1_n-definable in $\mathfrak{A}$.

Intuitively, the letters `A`, `C` and `D` stand for "analytical" (which reminds us of the *analytical hierarchy*), "complexity" and "definability". For example,

$$\langle \mathbb{N}, +, = \rangle \text{ and } \langle \mathbb{N}, \times, = \rangle \text{ have } \mathtt{AC} \quad \text{and} \quad \langle \mathbb{N}, +, = \rangle \text{ has } \mathtt{AD},$$

as was shown in (Speranski, 2013).

We also use the binary predicate symbols $|$ and $\perp$ to denote the *divisibility relation* and the *coprimeness relation*, respectively — in other words, for any $\{x, y\} \subset \mathbb{N}$,

$$\begin{aligned} x \,|\, y &\iff x \text{ divides } y \quad \text{and} \\ x \perp y &\iff x \text{ and } y \text{ have no common prime divisor.} \end{aligned}$$

Given $k \geqslant 2$, let bc_k be the function which maps each $(x, y) \in \mathbb{N} \times \mathbb{N}$ into the remainder of integer division of the binomial coefficient $\binom{x+y}{x}$ by k, i. e.

$$\binom{x+y}{x} \bmod k \;=\; \frac{(x+y)!}{x! \times y!} \bmod k.$$

In the present work we shall concentrate on the structures

$$\mathscr{N} := \langle \mathbb{N}, | \rangle, \quad \mathscr{C} := \langle \mathbb{N}, \perp \rangle \quad \text{and} \quad \mathscr{B}_k := \langle \mathbb{N}, \mathsf{bc}_k, = \rangle$$

where $k \geqslant 2$. And primes will play a key role in our study. For $n \in \mathbb{N} \setminus \{0\}$, define

$$\mathbb{P}_n := \{p^n \mid p \text{ is a prime}\} \quad \text{and} \quad \sqsubset_n := \text{ the restriction of } < \text{ to } \bigcup_{i=1}^{n} \mathbb{P}_n.$$

Occasionally we write $\mathbb{P}$ instead of $\mathbb{P}_1$. In the limit, one gets

$$\overline{\mathbb{P}} := \bigcup_{n=1}^{\infty} \mathbb{P}_n \quad \text{and} \quad \sqsubset := \bigcup_{n=1}^{\infty} \sqsubset_n.$$

Several results are worth mentioning here:

1. if $k \notin \overline{\mathbb{P}}$, then $+$ and $\times$ are definable in $\mathscr{B}_k$ (Korec, 1993);
2. if $k \in \overline{\mathbb{P}} \setminus \mathbb{P}$, then $+$ is definable in $\mathscr{B}_k$ and $\mathrm{Th}^1(\mathscr{B}_k)$ is decidable (Bès, 1997).

Thus for every $k \notin \mathbb{P}$, $\mathscr{B}_k$ has `AC` and `AD`. On the other hand, if $p \in \mathbb{P}$, then

- $\mathrm{Th}^1(\mathscr{B}_p)$ is decidable (Korec, 1995) and
- neither $+$ nor $\times$ is definable in $\mathscr{B}_p$ (Bès & Korec, 1998).

Further, we shall employ the relational signature

$$\sigma_\star := \{=^2, \Gamma_0^1, \Gamma_{\mathsf{s}}^2, \Gamma_+^3, \Gamma_\times^3\},$$

paying special attention to the conjunction $\mathsf{A}_\star$ of the following $\sigma_\star$-sentences:

E1. $\forall x\,(x = x)$;
E2. $\forall x \forall y\,(x = y \to y = x)$;
E3. $\forall x \forall y \forall u\,((x = y \wedge y = u) \to x = u)$;
E4. $\forall x \forall y \forall u \forall v\,((x = u \wedge y = v \wedge \Gamma_{\mathsf{s}}(x,y)) \to \Gamma_{\mathsf{s}}(u,v))$;
E5. $\forall x \forall y \forall z \forall u \forall v \forall w\,((x = u \wedge y = v \wedge z = w \wedge \Gamma_+(x,y,z)) \to \Gamma_+(u,v,w))$;
E6. $\forall x \forall y \forall z \forall u \forall v \forall w\,((x = u \wedge y = v \wedge z = w \wedge \Gamma_\times(x,y,z)) \to \Gamma_\times(u,v,w))$;
A1. $\forall x \forall y\,(\exists u \exists v\,(\Gamma_{\mathsf{s}}(x,u) \wedge \Gamma_{\mathsf{s}}(y,v) \wedge u = v) \to x = y)$;
A2. $\forall x \forall y \forall u\,((\Gamma_0(x) \wedge \Gamma_{\mathsf{s}}(y,u)) \to \neg x = u)$;
A3. $\forall x\,(\Gamma_0(x) \vee \exists y \exists u\,(\Gamma_{\mathsf{s}}(y,u) \wedge x = u))$;
A4. $\forall x \forall y\,(\Gamma_0(y) \to \exists u\,(\Gamma_+(x,y,u) \wedge u = x))$;
A5. $\forall x \forall y \forall z \forall u \forall v \forall w\,((\Gamma_{\mathsf{s}}(y,z) \wedge \Gamma_+(x,z,u) \wedge \Gamma_+(x,y,v) \wedge \Gamma_{\mathsf{s}}(v,w)) \to u = w)$;
A6. $\forall x \forall y\,(\Gamma_0(y) \to \exists u\,(\Gamma_\times(x,y,u) \wedge u = y))$;
A7. $\forall x \forall y \forall z \forall u \forall v \forall w\,((\Gamma_{\mathsf{s}}(y,z) \wedge \Gamma_\times(x,z,u) \wedge \Gamma_\times(x,y,v) \wedge \Gamma_+(v,x,w)) \to u = w)$;
C. $\exists x\,(\Gamma_0(x) \wedge \forall y\,(\Gamma_0(y) \leftrightarrow y = x))$;
F1. $\forall x \exists y\,\Gamma_{\mathsf{s}}(x,y) \wedge \forall x \forall y \forall u\,((\Gamma_{\mathsf{s}}(x,y) \wedge \Gamma_{\mathsf{s}}(x,u)) \to y = u)$;
F2. $\forall x \forall y \exists u\,\Gamma_+(x,y,u) \wedge \forall x \forall y \forall u \forall v\,((\Gamma_+(x,y,u) \wedge \Gamma_+(x,y,v)) \to u = v)$;
F3. $\forall x \forall y \exists u\,\Gamma_\times(x,y,u) \wedge \forall x \forall y \forall u \forall v\,((\Gamma_\times(x,y,u) \wedge \Gamma_\times(x,y,v)) \to u = v)$.

Certainly $\mathsf{A}_\star$ is a reformulation of Robinson arithmetic. Henceforth we identify $\mathfrak{N}$ with its $\sigma_\star$-version. So in particular, the $\sigma_\star$-formula

$$\gamma_<(x,y) := \exists u\,(\Gamma_+(x,u,y) \wedge \neg \Gamma_0(u))$$

expresses $<$ in $\mathfrak{N}$. For convenience, we also introduce

$$\mathbb{N}' := \mathbb{N} \setminus \{0\}, \quad \mathbb{F} := \{k! \mid k \in \mathbb{N}\} \quad \text{and} \quad \sigma^\dagger := \sigma \cup \{U^1\}$$

where U is a fresh unary predicate symbol. Remark that §3.–§5. involve some "local notation" as well: for instance, σ stands for the signature in question and $(\sharp)$ for a very special list of formulas in $\sigma^\dagger$ (possibly augmented by individual constants).

§**3. The Case of the Natural Lattice** Assume $\sigma = \{|^2\}$. Throughout this section we shall be concerned with the σ-structure $\mathscr{N}$.

Clearly the constants 0 and 1, the equality relation =, the sets $\mathbb{P}$ and $\overline{\mathbb{P}}$, the coprimeness relation $\perp$ and the least common multiple operation lcm are all definable in $\mathscr{N}$:

$$\begin{aligned}
x = 0 &\iff \neg x \,|\, x,\\
x = 1 &\iff \forall y\,(x \,|\, y),\\
x = y &\iff (x = 0 \wedge y = 0) \vee (x \,|\, y \wedge y \,|\, x),\\
x \in \mathbb{P} &\iff \neg x = 0 \wedge \neg x = 1 \wedge \forall y\,(y \,|\, x \to (y = 1 \vee y = x)),\\
x \in \overline{\mathbb{P}} &\iff \exists y\,(y \in \mathbb{P} \wedge y \,|\, x \wedge \forall u\,((u \in \mathbb{P} \wedge u \,|\, x) \to u = y)),\\
x \perp y &\iff \neg \exists u\,(\neg u = 1 \wedge u \,|\, x \wedge u \,|\, y) \quad \text{and}\\
z = \mathsf{lcm}\,(x, y) &\iff x \,|\, z \wedge y \,|\, z \wedge \forall u\,((x \,|\, u \wedge y \,|\, u) \to z \,|\, u).
\end{aligned}$$

Furthermore, each $\mathbb{P}_n$ belongs to $\mathrm{Def}\,(\mathscr{N})$ as well — because

$$x \in \mathbb{P}_n \quad\iff\quad x \in \overline{\mathbb{P}} \wedge \exists y_0 \ldots \exists y_n \left(y_0 = 1 \wedge y_n = x \wedge \bigwedge\nolimits_{i=0}^{n-1} y_i \prec y_{i+1}\right).$$

In what follows $x = y$, $x = 0$, etc. in σ- and $\sigma^\dagger$-formulas should be understood merely as convenient abbreviations. Also we shall exploit two specific σ-formulas:

$$x \prec y \;:=\; x \,|\, y \wedge \neg x \,|\, y \quad\text{and}\quad x \lessdot y \;:=\; x \prec y \wedge \neg \exists u\,(x \prec u \wedge u \prec y)$$

— so the latter can be viewed as a covering relation for the former.

PROPOSITION 3.1. *For every $n \in \mathbb{N}'$, $\sqsubset_n$ is definable in $\langle \mathscr{N}, \mathbb{F} \rangle$.*

Proof. Since $x < y$ is equivalent to $x! \prec y!$ for any x and y in $\mathbb{N}'$, it suffices to establish the definability of a (partial) function which maps each $k \in \mathbb{P}_1 \cup \cdots \cup \mathbb{P}_n$ into $k!$

Provided that $x \in \mathbb{N}'$ and $y \in \mathbb{P}$, the σ-formula

$$\varphi_1\,(x, y, z) \;:=\; x \lessdot z \wedge \forall u \left(\left(u \in \overline{\mathbb{P}} \wedge u \,|\, x \wedge y \,|\, u\right) \to \exists v \left(v \in \overline{\mathbb{P}} \wedge v \,|\, z \wedge u \lessdot v\right)\right)$$

says "$z = x \times y$", and more generally, for every $k \in \{1, \ldots, n\}$, the σ-formula

$$\begin{aligned}
\varphi_k\,(x, y, z) \;:=\; &\exists v_0 \ldots \exists v_k \left(v_0 = x \wedge v_k = z \wedge \bigwedge\nolimits_{i=0}^{k-1} v_i \lessdot v_{i+1}\right) \wedge\\
&\forall u \left(\left(u \in \overline{\mathbb{P}} \wedge u \,|\, x \wedge y \,|\, u\right) \to \exists v_0 \ldots \exists v_k \left(v_k \in \overline{\mathbb{P}} \wedge v_k \,|\, z \wedge v_0 = u \wedge \bigwedge\nolimits_{i=0}^{k-1} v_i \lessdot v_{i+1}\right)\right)
\end{aligned}$$

says "$z = x \times y^k$". On the other hand, assuming $x \in \mathbb{F} \setminus \{1\}$, the σ'-formula

$$\varphi_*\,(x, y) \;:=\; U\,(y) \wedge y \prec x \wedge \forall u\,((U\,(u) \wedge u \prec x) \to u \,|\, y)$$

expresses that y is the predecessor of x in $\mathbb{F}$, i. e., $y = (k-1)!$ whenever $x = k!$ Obviously, for all $x \in \mathbb{P}_1 \cup \cdots \cup \mathbb{P}_n$, we have

$$y \;=\; x! \quad\iff\quad \begin{array}{c} y \text{ belongs to } \mathbb{F},\ y \text{ is not equal to } 1,\ \text{and} \\ \text{the predecessor of } y \text{ multiplied by } x \text{ equals } y; \end{array}$$

thus one can define in $\langle \mathscr{N}, \mathbb{F} \rangle$ a function with the required property by an appropriate σ'-formula using $\varphi_1, \ldots, \varphi_n$ and φ_*. The rest is straightforward. □

As was proved in (Bès & Richard, 1998), $+$ and $\times$ are definable in

$$\langle \mathbb{N}, |, \sqsubset \rangle.$$

Aiming to obtain the same for some expansion of $\mathcal{N}$ to $\sigma^\dagger$, let $\mathbb{K}$ denote

$$\{p^k \times q^m \mid \{p,q\} \subset \mathbb{P},\ p < q,\ \{k,m\} \subset \mathbb{N}',\ p^k < q^m \text{ and } \mathsf{max}\{k,m\} \geqslant 4\}.$$

Then $\mathbb{E} := \mathbb{F} \cup \mathbb{K}$ encodes $\sqsubset$ in the following sense.

PROPOSITION 3.2. *$\sqsubset$ is definable in $\langle \mathcal{N}, \mathbb{E} \rangle$.*

Proof. First observe that

$$A \ := \ \{(p^k, q^m) \mid \{p,q\} \subset \mathbb{P},\ p \neq q,\ \{k,m\} \subset \mathbb{N}' \text{ and } \mathsf{max}\{k,m\} \geqslant 4\}$$
$$\text{and} \quad B \ := \ \{k \times m \mid (k,m) \in A\}$$

are defined in $\mathcal{N}$ by the σ-formulas

$$\varphi_A(x,y) \ := \ x \in \overline{\mathbb{P}} \wedge y \in \overline{\mathbb{P}} \wedge x \perp y \wedge \exists u\,(u \in \mathbb{P}_4 \wedge (u \,|\, x \vee u \,|\, y))$$
$$\text{and} \quad \varphi_B(x) \ := \ \exists u \exists v\,(\varphi_A(u,v) \wedge x = \mathsf{lcm}(u,v)).$$

Consequently — since $\mathbb{F} \subset \mathbb{N} \setminus B$ and $\mathbb{K} \subset B$ — the $\sigma^\dagger$-formulas

$$\varphi_{\mathbb{F}}(x) \ := \ x \in U \wedge \neg\varphi_B(x) \quad \text{and} \quad \varphi_{\mathbb{K}}(x) \ := \ x \in U \wedge \varphi_B(x)$$

define $\mathbb{F}$ and $\mathbb{K}$, respectively, in $\langle \mathcal{N}, \mathbb{E} \rangle$. So in particular — remembering Proposition 3.1. — $\sqsubset_3$ is expressible. Hence

$$\begin{aligned} \varphi_{\sqsubset}(x,y) \ := \ & x \in \overline{\mathbb{P}} \wedge y \in \overline{\mathbb{P}} \wedge x \prec y \vee x \sqsubset_3 y \vee \\ & (\varphi_A(x,y) \wedge \exists u \exists v \exists w\,(u \,|\, x \wedge v \,|\, y \wedge u \sqsubset_1 v \wedge \varphi_{\mathbb{K}}(\mathsf{lcm}(x,y)))) \\ & (\varphi_A(x,y) \wedge \exists u \exists v\,(u \,|\, x \wedge v \,|\, y \wedge v \sqsubset_1 u \wedge \neg\varphi_{\mathbb{K}}(\mathsf{lcm}(x,y)))), \end{aligned}$$

defines $\sqsubset$ in $\langle \mathcal{N}, \mathbb{E} \rangle$, as can be readily checked. □

Combining this with the result of A. Bès and D. Richard, we immediately get

COROLLARY 3.3. *$+$ and $\times$ are definable in $\langle \mathcal{N}, \mathbb{E} \rangle$.*

We are now ready to establish

THEOREM 3.4. *$\mathcal{N}$ has* `AC`.

Proof. Pick an infinite $A \subseteq \mathbb{N} \setminus \mathbb{E}$ from $\mathrm{Def}(\mathcal{N})$ — for instance, $A := \mathbb{P}_2$ — and let $\theta(x)$ be a σ-formula defining A in $\mathcal{N}$. By Corollary 3.3., we can find $\sigma^\dagger$-formulas

$$\varphi_=(x,y), \quad \varphi_0(x), \quad \varphi_{\mathsf{s}}(x,y), \quad \varphi_+(x,y,z) \quad \text{and} \quad \varphi_\times(x,y,z) \qquad (\sharp)$$

which define $=$, 0, s, $+$ and $\times$, respectively, in $\langle \mathcal{N}, \mathbb{E} \rangle$. Consider the modified list

$$\psi_=(x,y), \quad \psi_0(x), \quad \psi_{\mathsf{s}}(x,y), \quad \psi_+(x,y,z) \quad \text{and} \quad \psi_\times(x,y,z) \qquad (\natural)$$

obtained from ($\sharp$) by replacing each occurrence of the form $u \in U$ by $u \in U \wedge \neg\theta(u)$. Thus ($\natural$) plays the role of ($\sharp$) for every $\sigma^\dagger$-structure $\langle \mathcal{N}, \mathbb{E} \cup B \rangle$ with $B \subseteq A$.

Next, given a second-order $\sigma_\star$-formula φ, take

$$\tau\varphi \ := \ \text{the result of replacing } =,\ \Gamma_0,\ \Gamma_{\mathsf{s}},\ \Gamma_+ \text{ and } \Gamma_\times$$
$$\text{in } \varphi \text{ by } \psi_=,\ \psi_0,\ \psi_{\mathsf{s}},\ \psi_+ \text{ and } \psi_\times, \text{ respectively.}$$

Some expansions of $\mathcal{N}$ to $\sigma^\dagger$ can induce, via ($\natural$), non-standard models even when $\tau\mathsf{A}_\star$ is satisfied. To avoid this, it suffices to ensure that ψ_{s} behaves in the standard manner, i. e.

$$\psi_{\mathsf{s}} \text{ always expresses a relation isomorphic to } \langle \mathbb{N}, \mathsf{s} \rangle.$$

Choose a $\sigma_\star$-formula $\phi(x,y)$ defining the obvious isomorphism between

$$\langle \mathbb{N}, \mathsf{s}\rangle \quad \text{and} \quad \langle \{2^k \mid k \in \mathbb{N}'\}, \lessdot\rangle$$

(viewed as $\{\Gamma_\mathsf{s}\}$-structures) — viz. the numerical function $y = 2^x$ — in $\mathfrak{N}$. Let $\chi_{\mathtt{st}}$ denote the conjunction of the following $\sigma^\dagger$-sentences:

S1. $\forall x \forall u \forall v\left((\tau\phi(x,u) \wedge \tau\phi(x,v)) \to \psi_=(u,v)\right)$;
S2. $\forall x \forall y \forall u\left((\tau\phi(x,u) \wedge \tau\phi(y,u)) \to \psi_=(x,y)\right)$;
S3. $\exists x\left(x \in \mathbb{P} \wedge \forall y \exists v\left(v \in \overline{\mathbb{P}} \wedge x \mid v \wedge \tau\phi(y,v)\right) \wedge \forall v\left(\left(v \in \overline{\mathbb{P}} \wedge x \mid v\right) \to \exists y\, \tau\phi(y,v)\right)\right)$;
S4. $\forall x \forall y \exists u \exists v\left(\tau\phi(x,u) \wedge \tau\phi(y,v) \wedge (\psi_\mathsf{s}(x,y) \leftrightarrow u \lessdot v)\right)$.

With any expansion $\mathfrak{A}$ of $\mathscr{N}$ to $\sigma^\dagger$ we associate, via ($\natural$), the $\sigma_\star$-structure $\mathfrak{A}_\star$ with domain $\mathbb{N}$, such that

$$\mathfrak{A}_\star \vDash k = m \iff \mathfrak{A} \vDash \psi_=(k,m), \quad \mathfrak{A}_\star \vDash \Gamma_0(k) \iff \mathfrak{A} \vDash \psi_0(k), \quad \text{etc.}$$

Clearly if $\mathfrak{A}$ satisfies $\tau\mathsf{A}_\star \wedge \chi_{\mathtt{st}}$, then $\mathfrak{A}_\star$ is isomorphic (although not necessarily identical) to $\mathfrak{N}$. Fix a $\sigma_\star$-formula $\vartheta(x,y)$ defining in $\mathfrak{N}$ some function f mapping $\mathbb{N}$ one-one onto A — and let $\chi_{\mathtt{tr}}$ be the conjunction of the following $\sigma^\dagger$-sentences:

T1. $\forall x \forall u \forall v\left((\tau\vartheta(x,u) \wedge \tau\vartheta(x,v)) \to \psi_=(u,v)\right)$;
T2. $\forall x \forall y \forall u\left((\tau\vartheta(x,u) \wedge \tau\vartheta(y,u)) \to \psi_=(x,y)\right)$;
T3. $\forall x \exists u\left(\theta(u) \wedge \tau\vartheta(x,u)\right) \wedge \forall u\left(\theta(u) \to \exists x\, \tau\vartheta(x,u)\right)$.

So $\mathfrak{A} \vDash \chi_{\mathtt{tr}}$ implies that $\tau\vartheta$ expresses a one-one function from $\mathbb{N}$ onto A in $\mathfrak{A}$.

Further, given a second-order $\sigma_\star$-formula φ, take

$$\iota\varphi := \text{the result of replacing each } u \in U \text{ in } \varphi \text{ by } \exists v\left(\vartheta(u,v) \wedge v \in U\right)$$

where v is the first variable not occurring in φ. Then for an arbitrary Π^1_n-$\sigma_\star$-sentence

$$\forall X_1 \exists X_2 \ldots \psi(X_1, X_2, \ldots)$$

with $X_1 = U$ and ψ containing no second-order quantifiers — by the properties of f and ι — we have

$$\begin{aligned}\mathfrak{N} \vDash \forall U \exists X_2 \ldots \psi \quad &\iff \quad \mathfrak{N} \vDash \forall U \exists X_2 \ldots \iota\psi(f(U), X_2, \ldots)\\ &\iff \quad \mathfrak{N} \vDash \forall U \exists X_2 \ldots \iota\psi(U \cap A, X_2, \ldots)\\ &\iff \quad \mathfrak{N} \vDash \forall U \exists X_2 \ldots \iota\psi(U, X_2, \ldots).\end{aligned}$$

Observe that by the construction of ($\natural$), for all subsets C and D of $\mathbb{N}$,

$$C \setminus A = D \setminus A \quad \Longrightarrow \quad \text{the associated } \sigma_\star\text{-structures } \langle \mathscr{N}, C\rangle_\star \text{ and } \langle \mathscr{N}, D\rangle_\star \text{ coincide.}$$

Hence we can use $x \in U \wedge \theta(x)$ as a free unary predicate without changing the inner layer of the isomorphic copy of $\mathfrak{N}$ in question. It is straightforward to verify now that

$$\mathfrak{N} \vDash \forall U \exists X_2 \ldots \iota\psi(U, X_2, \ldots) \iff \mathscr{N} \vDash \forall U \exists X_2 \ldots \left((\tau\mathsf{A}_\star \wedge \chi_{\mathtt{st}} \wedge \chi_{\mathtt{tr}}) \to \tau\iota\psi(U, X_2, \ldots)\right),$$

which completes the argument. □

Note that whenever a set is second-order definable in $\mathscr{N}$ (without parameters), it has to be closed under $\mathrm{Aut}(\mathscr{N})$ — hence we cannot express, for instance, $x \in A$ with A a proper non-empty subset of $\mathbb{P}$. However, a minor modification of the above argument yields

THEOREM 3.5. *$\mathscr{N}$ has* AD.

Proof. Let $\gamma_{\mathrm{Dvs}}(x,y)$ denote the $\sigma_\star$-formula $\exists u\,(\Gamma_\times(x,u,y)\wedge\neg\Gamma_0(u))$. The idea is simply to add the $\sigma^\dagger$-sentence

S5. $\forall x\forall y\,(x\,|\,y\leftrightarrow\tau\gamma_{\mathrm{Dvs}}(x,y))$

to the conjunction of S1–S4, thus updating $\chi_{\mathtt{st}}$ to $\chi^*_{\mathtt{st}}$. Suppose $\mathfrak{A}\vDash\tau\mathsf{A}_\star\wedge\chi^*_{\mathtt{st}}$. Then there exists an isomorphism f between $\mathfrak{A}_\star$ and $\mathfrak{N}$. For any $\{k,m\}\subseteq\mathbb{N}$, we have

$$\begin{aligned} k \text{ divides } m \quad &\overset{\text{S5}}{\Longleftrightarrow}\quad \mathfrak{A}\vDash\tau\gamma_{\mathrm{Dvs}}(k,m)\quad\Longleftrightarrow\quad\mathfrak{A}_\star\vDash\gamma_{\mathrm{Dvs}}(k,m)\\ \Longleftrightarrow\quad \mathfrak{N}\vDash\gamma_{\mathrm{Dvs}}(f(k),f(m))\quad&\overset{\text{S5}}{\Longleftrightarrow}\quad f(k)\text{ divides }f(m).\end{aligned}$$

So $f\in\mathrm{Aut}(\mathscr{N})$. Consequently, for each natural number k and each Π^1_n-$\sigma_\star$-formula

$$\forall U\,\exists X_2\,\ldots\,\psi(U,X_2,\ldots,x)$$

with $X_1=U$ and ψ containing no set quantifiers,

$$\begin{aligned}\mathfrak{N}\vDash\forall U\,\exists X_2\,\ldots\,\psi(U,X_2,\ldots,f(k))\text{ for all }f\in\mathrm{Aut}(\mathscr{N})\quad&\Longleftrightarrow\\ f(\mathfrak{N})\vDash\forall U\,\exists X_2\,\ldots\,\psi(U,X_2,\ldots,k)\text{ for all }f\in\mathrm{Aut}(\mathscr{N})\quad&\Longleftrightarrow\\ \mathscr{C}\vDash\forall U\,\exists X_2\,\ldots\,((\tau\mathsf{A}_\star\wedge\chi^*_{\mathtt{st}}\wedge\chi_{\mathtt{tr}})\to\tau\iota\psi(U,X_2,\ldots,x))&\end{aligned}$$

where $f(\mathfrak{N})$ is the $\sigma_\star$-structure with domain $\mathbb{N}$, such that

$$\mathfrak{N}\vDash R(i_1,\ldots,i_m)\quad\Longleftrightarrow\quad f(\mathfrak{N})\vDash R(f(i_1),\ldots,(i_m)).$$

for any m-ary $R\in\sigma_\star$ and $(i_1,\ldots,i_m)\in\mathbb{N}^m$ (certainly $\mathfrak{N}$ and $f(\mathfrak{N})$ are isomorphic). □

Given $n\in\mathbb{N}'$, it is not hard to construct Π^1_n-complete sets closed under $\mathrm{Aut}(\mathscr{N})$. But if one wants to turn $\mathrm{Aut}(\mathscr{N})$ into $\{\mathsf{id}\}$, where id is the identity function, some extra information has to be incorporated into the structure. For example, consider

$$\mathscr{N}_\circ\ :=\ \langle\mathbb{N},|,\sqsubset_1\rangle$$

in the signature $\sigma^\ddagger:=\sigma\cup\{\sqsubset^2_1\}$. Since, as was proved earlier in (Maurin, 1997), the first-order theory of $\langle\mathbb{N},=,\times,\sqsubset_1\rangle$ is decidable, so is $\mathrm{Th}^1(\mathscr{N}_\circ)$. Furthermore, one easily checks that each non-trivial $f\in\mathrm{Aut}(\mathscr{N})$ permutes at least two primes; thus $\mathrm{Aut}(\mathscr{N}_\circ)=\{\mathsf{id}\}$.

COROLLARY 3.6. *Let $n\in\mathbb{N}'$. Every Π^1_n-set is Π^1_n-definable in $\mathscr{N}_\circ$.*

Assume the intended interpretation of the binary predicate symbol $\|$ is

$$\{(k,m)\in\mathbb{N}\times\mathbb{N}\mid k\,|\,m\text{ or }m\,|\,k\}.$$

We finish with a relatively simple yet interesting fact about $\mathscr{D}:=\langle\mathbb{N},\|\rangle$.

PROPOSITION 3.7. *$\mathscr{N}$ and $\mathscr{D}$ are interdefinable.*

Proof. It is a routine matter to verify that

$$\begin{aligned} x=0\quad&\Longleftrightarrow\quad\neg x\,\|\,x,\\ x=1\quad&\Longleftrightarrow\quad\forall u\,(x\,\|\,u),\\ x=y\quad&\Longleftrightarrow\quad\forall u\,(x\,\|\,u\leftrightarrow y\,\|\,u),\\ x\in\overline{\mathbb{P}}\quad&\Longleftrightarrow\quad\neg x=0\wedge\neg x=1\wedge\exists u\,(\neg x=u\wedge x\,\|\,u\wedge\forall v\,(u\,\|\,v\to x\,\|\,v))\end{aligned}$$

and the compound formula

$$x = 1 \vee \big(x \in \overline{\mathbb{P}} \wedge y \in \overline{\mathbb{P}} \wedge \forall u\,(y \,\|\, u \to x \,\|\, u)\big) \vee \\ \big(\neg x = 0 \wedge \neg x \in \overline{\mathbb{P}} \wedge \neg y = 1 \wedge \neg y \in \overline{\mathbb{P}} \wedge \forall u\,\big(\big(u \in \overline{\mathbb{P}} \wedge x \,\|\, u\big) \to y \,\|\, u\big)\big)$$

(where $x \in \overline{\mathbb{P}}$, $x = 0$, etc. are understood as abbreviations) defines $x \,|\, y$ in $\mathscr{D}$.

The other direction is trivial. □

§**4. The Case of Modular Pascal's Triangles** As has been observed earlier, we need only consider $\mathscr{B}_n$ with n prime, assuming $\sigma = \left\{\mathsf{bc}_n^2, =^2\right\}$.

Fix $p \in \mathbb{P}$. By a *p-ary expansion* of $x \in \mathbb{N}$ we mean any $(x_0, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k$ for which $\sum_{i=0}^{k} x_i \times p^i = x$, written $x = [x_k, \ldots, x_0]_p$. Of course, each number has infinitely many p-ary expansions:

$$x \;=\; [x_k, \ldots, x_0]_p \quad\Longleftrightarrow\quad x \;=\; [0, \ldots, 0, x_k, \ldots, x_0]_p.$$

So given $\{x, y\} \subset \mathbb{N}$, we can always find expansions of x and y with the same length. Now for $x = [x_k, \ldots, x_0]_p$ and $y = [y_k, \ldots, y_0]_p$, let

$$x \Subset y \quad\Longleftrightarrow\quad x \neq y \text{ and } x_i \leqslant y_i \text{ for all } i \in \{0, \ldots, k\}.$$

Intuitively, $\Subset$ is a sort of "multiset inclusion". Korec (1993) showed that:

i. the relation $\Subset$ and the set $\mathbb{G}_p := \left\{p^k \mid k \in \mathbb{N}'\right\}$ belong to $\mathrm{Def}(\mathscr{B}_p)$;
ii. $+$ and $\times$ are definable in $\langle \mathscr{B}_2, \mathrm{Sq}\rangle$ where Sq denotes $\left\{k^2 \mid k \in \mathbb{N}\right\}$.

Furthernore, as was proved in (Bès & Korec, 1998), (ii) holds for each $\langle \mathscr{B}_p, \mathrm{Sq}\rangle$.

For our present purposes, it is useful to introduce

$$A_p \;:=\; \left\{p + p^{2+k} \mid k \in \mathbb{N}\right\}.$$

Certainly there exists a σ-formula $\theta_p(x, v)$ such that for every $m \in \mathbb{N}$,

$$m \in A_p \quad\Longleftrightarrow\quad \mathscr{B}_p \vDash \theta_p(m, p)$$

(think of v as a parameter). To be more precise, define

$$\theta_p(x, v) \;:=\; v \Subset x \wedge \exists u\,(u \in \mathbb{G}_p \wedge \neg u = v \wedge u \Subset x \wedge \neg\exists z\,(v \Subset z \wedge u \Subset z \wedge z \Subset x)).$$

We also employ the signature $\sigma^{\ddagger} := \sigma^{\dagger} \cup \{c\}$ including an extra constant symbol c whose role is similar to that of v in the above discussion. Accordingly we write $\langle \mathscr{B}_p, B, k\rangle$ for the $\sigma^{\ddagger}$-structure obtained from $\mathscr{B}_p$ by interpreting U as B and c as k.

THEOREM 4.8. *$\mathscr{B}_p$ has* $\mathtt{AC}$.

Proof. Take $A := A_p$ — evidently $A \cap \mathrm{Sq} = \varnothing$ — and let $\theta(x)$ be the formula $\theta_p(x, c)$. By analogy with the proof of Theorem 3.4., we obtain the new (♯), (♮) and τ.

To avoid "non-standard" expansions of $\mathscr{B}_p$ to $\sigma^{\ddagger}$, it suffices to ensure that

$$\tau\gamma_{<} \text{ always expresses a relation embeddable in } \Subset$$

— because the latter is well-founded. Choose a $\sigma_\star$-formula $\phi(x, y)$ defining the numerical function $y = \sum_{k=1}^{x} p^k$ — which embeds $\langle \mathbb{N}, <\rangle$ into $\langle \mathbb{N}, \Subset\rangle$, obviously — in $\mathfrak{N}$. Next, let ρ be a σ-formula defining $\Subset$ in $\mathscr{B}_p$, and denote by $\chi_{\mathtt{st}}$ the conjunction of:

S1. $\forall x \forall u \forall v\left(\left(\tau\phi(x,u) \wedge \tau\phi(x,v)\right) \rightarrow u = v\right)$;
S2. $\forall x \forall y \forall u\left(\left(\tau\phi(x,u) \wedge \tau\phi(y,u)\right) \rightarrow x = y\right)$;
S3. $\forall x \exists u\, \tau\phi(x,u)$;
S4. $\forall x \forall y \exists u \exists v\left(\tau\phi(x,u) \wedge \tau\phi(y,v) \wedge \left(\tau\gamma_{<}(x,y) \leftrightarrow \rho(u,v)\right)\right)$.

As before, with every expansion $\mathfrak{A}$ of $\mathscr{B}_p$ to $\sigma^{\ddagger}$ we associate, via ($\natural$), the $\sigma_{\star}$-structure $\mathfrak{A}_{\star}$. Suppose $\mathfrak{A} \vDash \tau\mathsf{A}_{\star} \wedge \chi_{\mathtt{st}}$ but $\mathfrak{A}_{\star}$ is not isomorphic to $\mathfrak{N}$. Then there exists a chain $k_0, k_1, \ldots$ of pairwise distinct natural numbers with the property:

$$\mathfrak{A}_{\star} \vDash \gamma_{<}(k_{m+1}, k_m) \text{ — and hence } \mathfrak{A} \vDash \tau\gamma_{<}(k_{m+1}, k_m) \text{ — for each } m \in \mathbb{N}.$$

Thus we get an infinite descending chain in $\langle \mathbb{N}, \Subset \rangle$, contradicting the well-foundedness of $\Subset$. Let ϑ, $\chi_{\mathtt{tr}}$ and ι be as in the proof of Theorem 3.4. We have the following:

- $\langle \mathscr{B}_p, B, k \rangle \vDash \chi_{\mathtt{tr}}$ implies that $\tau\vartheta$ defines a one-one function from $\mathbb{N}$ onto
$$\Theta_k \;:=\; \left\{ m \in \mathbb{N} \mid \mathscr{B}_p \vDash \theta_p(m,k) \right\}$$
(which may or may not be identical to A) in $\langle \mathscr{B}_p, B, k \rangle$;
- for all $k \in \mathbb{N}$, $C \subseteq \mathbb{N}$ and $D \subseteq \mathbb{N}$,
$$C \setminus \Theta_k \;=\; D \setminus \Theta_k \quad \Longrightarrow \quad \begin{array}{c}\text{the associated } \sigma_{\star}\text{-structures} \\ \langle \mathscr{B}_p, C, k \rangle_{\star} \text{ and } \langle \mathscr{B}_p, D, k \rangle_{\star} \text{ coincide.}\end{array}$$

Viewing c as an individual variable, it is now straightforward to check that

$$\mathfrak{N} \vDash \forall U\, \exists X_2 \ldots\, \psi(U, X_2, \ldots) \quad \Longleftrightarrow$$
$$\mathscr{N} \vDash \forall U\, \exists X_2 \ldots \forall c\left(\left(\tau\mathsf{A}_{\star} \wedge \chi_{\mathtt{st}} \wedge \chi_{\mathtt{tr}}\right) \rightarrow \tau\iota\psi(U, X_2, \ldots)\right)$$

where ψ contains no second-order quantifiers. □

As a matter of fact, for $p \neq 2$, one can also take $A := \left\{ 2 \times p^k \mid k \in \mathbb{N} \right\}$ which is directly definable in $\mathscr{B}_p$ (without parameters). Unfortunately, this will not work for $p = 2$.

THEOREM 4.9. *$\mathscr{B}_p$ has* AD.

Proof. Fix a $\sigma_{\star}$-formula $\gamma_p(x,y,z)$ defining bc_p in $\mathfrak{N}$, and add the $\sigma^{\dagger}$-sentence

S5. $\forall x \forall y \forall z\left(\mathsf{bc}_p(x,y) = z \leftrightarrow \tau\gamma_p(x,y,z)\right)$

to the conjunction of S1–S4, i. e. $\chi_{\mathtt{st}}$. Now proceed as in the proof of Theorem 3.5. □

§**5. About the Coprimeness Relation** Assume $\sigma = \left\{ \perp^2 \right\}$. Of course, we shall focus our attention on the σ-structure $\mathscr{C}$.

Obviously 0, 1 and $\overline{\mathbb{P}}$ are definable in $\mathscr{C}$ — because

$$\begin{aligned} x = 1 \quad &\Longleftrightarrow \quad \forall u\,(u \perp x), \\ x = 0 \quad &\Longleftrightarrow \quad \forall u\,(u \perp x \rightarrow u = 1) \quad \text{and} \\ x \in \overline{\mathbb{P}} \quad &\Longleftrightarrow \quad \neg x = 1 \wedge \forall u \forall v\left((\neg u \perp x \wedge \neg v \perp x) \rightarrow \neg u \perp v\right). \end{aligned}$$

By analogy with the previous section, we also introduce $\sigma^{\ddagger} := \sigma^{\dagger} \cup \{c\}$.

As was proved by Bès & Richard (1998), $\mathfrak{N}$ is first-order interpretable in

$$\mathscr{N}_{\bullet} := \langle \mathbb{N}, \perp, \sqsubset_2 \rangle,$$

and they employed an infinite collection of primes with the usual ordering to play the role of $\mathbb{N}$ here. Naturally the same holds for the substructure $\mathscr{S}$ of $\mathscr{N}_\bullet$ with domain

$$S \;:=\; \{0\} \cup \{k \in \mathbb{N} \mid 2 \perp k \text{ and } 3 \perp k\}.$$

For our present purposes, consider the function $h : S \to \mathbb{N}$ given by

$$h(k) \;:=\; \begin{cases} 2 \times k & \text{if } k \in \mathbb{P}_2 \cap S \\ 3 \times k & \text{if } k \in \big(\overline{\mathbb{P}} \setminus (\mathbb{P} \cup \mathbb{P}_2)\big) \cap S \\ k & \text{otherwise} \end{cases}$$

Certainly $\mathscr{S}$ is isomorphic to $\mathscr{H} = \langle H, \perp^h, \sqsubset_2^h \rangle$ where

$$H \;:=\; h(S), \quad \perp^h \;:=\; \{(h(k), h(m)) \mid \{k,m\} \subset S \text{ and } k \perp m\}$$
$$\text{and} \quad \sqsubset_2^h \;:=\; \{(h(k), h(m)) \mid \{k,m\} \subset S \text{ and } k \sqsubset_2 m\}.$$

Notice that $h(x) = x$ for all $x \in \mathbb{P} \cap S$. Let $\mathbb{X}$, $\mathbb{Y}$ and $\mathbb{O}$ denote

$$h(\mathbb{P}_2 \cap S), \quad h\big(\big(\overline{\mathbb{P}} \setminus (\mathbb{P} \cup \mathbb{P}_2)\big) \cap S\big) \quad \text{and}$$
$$\{p^k \times q^m \mid \{p,q\} \subset \mathbb{P},\; 3 < p < q,\; \{k,m\} \subset \mathbb{N}' \text{ and } p^2 > q\},$$

respectively. Then

$$\mathbb{D} \;:=\; \mathbb{P} \cup (\mathbb{F} \setminus \{6, 24\}) \cup \mathbb{X} \cup \mathbb{Y} \cup \mathbb{O}$$

encodes $\mathscr{H}$ as follows.

PROPOSITION 5.10. *H, $\perp^h$ and $\sqsubset_2^h$ are definable in $\langle \mathscr{C}, \mathbb{D}, 2 \rangle$.*

Proof. First observe that

$$A \;:=\; \{p^k \times q^m \mid \{p,q\} \subset \mathbb{P},\; p \neq q \text{ and } \{k,m\} \subset \mathbb{N}'\}$$

is defined in $\mathscr{C}$ by the σ-formula

$$\varphi_A(x) \;:=\; \neg x = 0 \wedge \exists u \exists v \big(u \in \overline{\mathbb{P}} \wedge v \in \overline{\mathbb{P}} \wedge u \perp v \wedge$$
$$\neg u \perp x \wedge \neg v \perp x \wedge \neg \exists w \big(w \in \overline{\mathbb{P}} \wedge w \perp u \wedge w \perp v \wedge \neg w \perp x\big)\big).$$

Consequently — since

$$\mathbb{D} \cap \overline{\mathbb{P}} \;=\; \mathbb{P}, \quad \mathbb{D} \cap A \;=\; \mathbb{X} \cup \mathbb{Y} \cup \mathbb{O} \quad \text{and} \quad \mathbb{D} \cap \big(\mathbb{N} \setminus \big(A \cup \overline{\mathbb{P}}\big)\big) \;=\; \mathbb{F} \setminus \{2, 6, 24\}$$

— the $\sigma^\ddagger$-formulas

$$\begin{aligned}
\varphi_{\mathbb{P}}(x) &:= x \in U \wedge x \in \overline{\mathbb{P}}, \\
\varphi_2(x) &:= \varphi_{\mathbb{P}}(x) \wedge \neg x \perp c, \\
\varphi_{\mathbb{X}}(x) &:= x \in U \wedge \varphi_A(x) \wedge \neg x \perp c, \\
\varphi_3(x) &:= \varphi_{\mathbb{P}}(x) \wedge \forall u (\varphi_{\mathbb{X}}(u) \to x \perp u), \\
\varphi_{\mathbb{Y}}(x) &:= x \in U \wedge \varphi_A(x) \wedge \exists u (\varphi_3(u) \wedge \neg x \perp u), \\
\varphi_{\mathbb{O}}(x) &:= x \in U \wedge \varphi_A(x) \wedge x \perp c \wedge \exists u (\varphi_3(u) \wedge x \perp u) \quad \text{and} \\
\varphi_{\widetilde{\mathbb{F}}}(x) &:= x \in U \wedge \neg \varphi_A(x) \wedge \neg x \in \overline{\mathbb{P}}
\end{aligned}$$

define $\mathbb{P}$, 2, $\mathbb{X}$, 3, $\mathbb{Y}$, $\mathbb{O}$ and $\mathbb{F} \setminus \{2, 6, 24\}$, respectively, in $\langle \mathscr{C}, \mathbb{D}, 2 \rangle$. Hence

$$\varphi_H(x) \;:=\; \varphi_{\mathbb{X}}(x) \vee \varphi_{\mathbb{Y}}(x) \vee \big(\big(\varphi_{\mathbb{P}}(x) \vee \neg x \in \overline{\mathbb{P}}\big) \wedge x \perp c \wedge \exists u (\varphi_3(u) \wedge x \perp u)\big)$$

expresses H. Now $(x,y) \in \perp^h$ can be written as

$$\varphi_H(x) \wedge \varphi_H(x) \wedge \neg\exists u\,(\varphi_{\mathbb{P}}(u) \wedge \neg\varphi_2(u) \wedge \neg\varphi_3(u) \wedge \neg u\perp x \wedge \neg u \perp y).$$

Further, for any $\{x,y\} \subset \mathbb{P}$,

$$x < y \quad \Longleftrightarrow \quad x \text{ divides } y! \text{ but not vice versa;}$$

so the restriction of $<$ to $\mathbb{P} \cap S$ is expressed by

$$\varphi_{\widetilde{\sqsubset}_1}(x,y) \;:=\; \neg\varphi_2(x) \wedge \neg\varphi_3(x) \wedge \varphi_{\mathbb{P}}(x) \wedge \varphi_{\mathbb{P}}(y) \wedge \forall u\,((\widetilde{\varphi}_{\mathbb{F}}(x) \wedge \neg y\perp u) \to \neg x \perp u) \wedge \exists v\,(\widetilde{\varphi}_{\mathbb{F}}(x) \wedge \neg x\perp v \wedge y \perp v).$$

Finally, one easily sees that

$$\varphi_{\widetilde{\sqsubset}_1}(x,y) \vee \Big(\varphi_{\mathbb{P}}(x) \wedge \varphi_{\mathbb{X}}(y) \wedge \exists v\,\Big(\varphi_{\mathbb{P}}(v) \wedge \neg v\perp y \wedge \varphi_{\widetilde{\sqsubset}_1}(x,v)\Big)\Big) \vee$$
$$\Big(\varphi_{\mathbb{X}}(x) \wedge \varphi_{\mathbb{X}}(y) \wedge \exists u\,\exists v\,\Big(\varphi_{\mathbb{P}}(u) \wedge \varphi_{\mathbb{P}}(v) \wedge \neg u\perp x \wedge \neg v\perp y \wedge \varphi_{\widetilde{\sqsubset}_1}(u,v)\Big)\Big) \vee$$
$$\Big(\varphi_{\mathbb{X}}(x) \wedge \varphi_{\mathbb{P}}(y) \wedge \exists u\,\Big(\varphi_{\mathbb{P}}(u) \wedge \neg u\perp x \wedge \varphi_{\widetilde{\sqsubset}_1}(u,y)\Big) \wedge \neg\exists z\,(\varphi_{\mathbb{O}}(z) \wedge \neg x\perp z \wedge \neg y\perp z)\Big) \vee$$
$$\Big(\varphi_{\mathbb{P}}(x) \wedge \varphi_{\mathbb{X}}(y) \wedge \exists v\,\Big(\varphi_{\mathbb{P}}(v) \wedge \neg v\perp y \wedge \varphi_{\widetilde{\sqsubset}_1}(v,x)\Big) \wedge \exists z\,(\varphi_{\mathbb{O}}(z) \wedge \neg x\perp z \wedge \neg y\perp z)\Big)$$

defines $\sqsubset_2^h$ in $\langle \mathscr{C}, \mathbb{D}, 2\rangle$. □

This time we immediately get

COROLLARY 5.11. *$\mathfrak{N}$ is first-order interpretable in $\langle \mathscr{C}, \mathbb{D}, 2\rangle$.*

In other words, there exist $\sigma^{\ddagger}$-formulas

$$\varphi_{\mathbb{N}}(x), \quad \varphi_{=}(x,y), \quad \varphi_0(x), \quad \varphi_{\mathsf{s}}(x,y), \quad \varphi_{+}(x,y,z) \quad \text{and} \quad \varphi_{\times}(x,y,z) \qquad (\sharp)$$

satisfying the following requirements:

- $M := \{k \in \mathbb{N} \mid \langle \mathscr{C}, \mathbb{D}, 2\rangle \vDash \varphi_{\mathbb{N}}(k)\}$ is non-empty;
- $\mathfrak{N}$ is isomorphic to the $\sigma_\star$-structure $\mathfrak{M}$ with domain M, such that
  - — for any k-ary $\Gamma_R \in \sigma_\star$ and $(m_1,\dots,m_k) \in M^k$,
  $$\mathfrak{M} \vDash \Gamma_R(m_1,\dots,m_k) \quad \Longleftrightarrow \quad \langle \mathscr{C}, \mathbb{D}, 2\rangle \vDash \varphi_R(m_1,\dots,m_k),$$
  - — and for all $(m_1,m_2) \in M \times M$,
  $$\mathfrak{M} \vDash m_1 = m_2 \quad \Longleftrightarrow \quad \langle \mathscr{C}, \mathbb{D}, 2\rangle \vDash \varphi_{=}(m_1,m_2).$$

Moreover, as has been already remarked, we can (and will) assume that

$$M \subseteq \mathbb{P} \setminus \{2,3\} \quad \text{and} \quad \gamma_{<} \text{ defines in } \mathfrak{M} \text{ the restriction of } < \text{ to } M.$$

In conclusion, we establish

THEOREM 5.12. *$\mathscr{C}$ has* `AC`.

Proof. Consider the σ-formula

$$\alpha(x,y) \;:=\; \neg x = 0 \wedge \neg x = 1 \wedge \neg x \in \overline{\mathbb{P}} \wedge \neg\varphi_C(x) \wedge x \perp y$$

with φ_C taken from the proof of Proposition 5.10. Evidently

$$A \;:=\; \{k \in \mathbb{N} \mid \mathscr{C} \vDash \alpha(k,2)\}$$

is a subset of $\mathbb{N}\setminus\mathbb{D}$, so let $\theta(x)$ be $\alpha(x,c)$. Accordingly we shall exploit the list

$$\psi_{\mathbb{N}}(x),\quad \psi_{=}(x,y),\quad \psi_0(x),\quad \psi_{\mathtt{s}}(x,y),\quad \psi_{+}(x,y,z)\quad\text{and}\quad \psi_{\times}(x,y,z) \qquad (\natural)$$

obtained from $(\sharp)$ by replacing each occurrence of the form $u\in U$ by $u\in U\wedge\neg\theta(u)$.

Next, given a second-order formula φ in $\sigma_\star\cup\sigma^\ddagger$, take

$$\begin{aligned}\tau\varphi \;:=\; &\text{the result of replacing } =,\ \Gamma_0,\ \Gamma_{\mathtt{s}},\ \Gamma_+ \text{ and } \Gamma_\times \text{ in}\\ &\varphi \text{ by } \psi_=,\ \psi_0,\ \psi_{\mathtt{s}},\ \psi_+ \text{ and } \psi_\times, \text{ respectively, and}\\ &\text{then relativising all individual quantifiers to } \psi_{\mathbb{N}}.\end{aligned}$$

Similarly to before, with any expansion $\mathfrak{A}$ of $\mathscr{C}$ to $\sigma^\ddagger$ we associate, using $(\natural)$, the $\sigma_\star$-structure $\mathfrak{A}_\star$ with domain $\{k\in\mathbb{N}\mid\mathfrak{A}\vDash\psi_{\mathbb{N}}(k)\}$, such that

$$\mathfrak{A}_\star\vDash k=m \;\Leftrightarrow\; \mathfrak{A}\vDash\psi_=(k,m),\quad \mathfrak{A}_\star\vDash\Gamma_0(k) \;\Leftrightarrow\; \mathfrak{A}\vDash\psi_0(k),\quad \text{etc.}$$

For $\mathfrak{A}$ satisfying $\tau\mathsf{A}_\star$ we have

$$\mathfrak{A}_\star \text{ is isomorphic to } \mathfrak{N} \quad\Longleftrightarrow\quad \gamma_< \text{ defines a well-founded relation in } \mathfrak{A}_\star.$$

By construction, $\psi_{\mathbb{N}}(x)\wedge\psi_{\mathbb{N}}(y)\wedge\tau\gamma_<(x,y)$ defines in $\langle\mathscr{C},\mathbb{D},2\rangle$ the restriction of $<$ to M. Also we know that $\mathbb{F}\setminus\{2,6,24\}$ is defined in $\langle\mathscr{C},\mathbb{D},2\rangle$ by the $\sigma^\ddagger$-formula

$$\phi(x) \;:=\; x\in U\wedge\neg\theta(x)\wedge\neg\varphi_C(x)\wedge\neg x\in\overline{\mathbb{P}},$$

Let $\chi_{\mathtt{st}}$ denote the conjunction of the following $\sigma^\dagger$-sentences:

S1. $\forall x\left(\psi_{\mathbb{N}}(x)\to\left(x\in\overline{\mathbb{P}}\wedge x\bot c\right)\right)$;
S2. $\forall x\forall y\left(\left(\psi_{\mathbb{N}}(x)\wedge\psi_{\mathbb{N}}(y)\wedge\tau\gamma_<(x,y)\right)\to x\bot y\right)$;
S3. $\forall x\left(x\in\overline{\mathbb{P}}\to\exists y\left(\neg y=0\wedge\phi(y)\wedge\neg x\bot y\right)\right)$;
S4. $\forall x\forall u\forall v\left(\left(\phi(x)\wedge\psi_{\mathbb{N}}(u)\wedge\psi_{\mathbb{N}}(v)\wedge\neg x\bot v\wedge\tau\gamma_<(u,v)\right)\to\neg x\bot u\right)$.

Suppose $\mathfrak{A}\vDash\tau\mathsf{A}_\star\wedge\chi_{\mathtt{st}}$ but the relation defined in $\mathfrak{A}_\star$ by $\gamma_<$ is not well-founded, i. e. there exists a chain $k_0,k_1,\dots$ of pairwise coprime elements of $\overline{\mathbb{P}}$ with the property:

$$\mathfrak{A}\vDash\psi_{\mathbb{N}}(k_m)\wedge\psi_{\mathbb{N}}(k_{m+1})\wedge\tau\gamma_<(k_{m+1},k_m)\ \text{ for all } m\in\mathbb{N}.$$

Applying S3, we find a positive integer K such that $\mathfrak{A}\vDash\phi(K)$ and $\neg k_0\bot K$. Thus by S4, K has infinitely many prime divisors, a contradiction.

Now consider an arbitrary Π^1_n-$\sigma_\star$-sentence

$$\forall X_1\,\exists X_2\dots\psi(X_1,X_2,\dots)$$

with $X_1=U$ and ψ containing no set quantifiers. To get ψ_* from ψ:

i. replace each $u\in U$ in ψ by $\exists v\left(v\in U\wedge\theta(v)\wedge\neg u\bot v\right)$ where v is the first individual variable not occurring in ψ — remember the requirements S1–S2;
ii. then replace $=$, Γ_0, $\Gamma_{\mathtt{s}}$, Γ_+ and $\Gamma_\times$ by $\psi_=$, ψ_0, $\psi_{\mathtt{s}}$, ψ_+ and $\psi_\times$, respectively;
iii. finally, relativise all individual quantifiers except those containing v to $\psi_{\mathbb{N}}$.

It is straightforward to check that

$$\mathfrak{N}\vDash\forall U\,\exists X_2\dots\psi \quad\Longleftrightarrow\quad \mathscr{C}\vDash\forall U\,\exists X_2\dots\forall c\left(\left(\tau\mathsf{A}_\star\wedge\chi_{\mathtt{st}}\right)\to\psi_*\right)$$

(here we view c as an individual variable). □

Still, the argument does not show how to get an analogue of Theorem 3.5.

§**6. Further Discussion** Certainly we come to

HYPOTHESIS. $\mathscr{C}$ *has* AD.

It would be nice to prove this by adapting the method developed in the paper, because

the above results readily generalise to all possible arithmetical expansions of the corresponding structures (provided that the extended signature is finite).

For example, we can pass from $\mathscr{N}$ to $\langle \mathbb{N}, \times, = \rangle$ in Theorem 3.5. On a technical note — there are two simple modifications worth mentioning:

i. in AD one can take $\mathbb{N}^k$ (with $k \geqslant 1$) instead of $\mathbb{N}$;
ii. in AD one can add to both $\mathfrak{N}$ and $\mathfrak{A}$ parameters for sets closed under $\mathrm{Aut}(\mathfrak{A})$.

Of course, perfectly analogous arguments apply here.

Acknowledgements I would like to thank Alexis Bès for his useful comments.

The research was supported by the Alexander von Humboldt Foundation.

Bibliography

Bès, A. (2002). A survey of arithmetical definability. In Crabbé, M., et al., eds. *A tribute to Maurice Boffa*, pp. 1–54. Société Mathématique de Belgique.

Bès, A. (1997). On Pascal triangles modulo a prime power. *Annals of Pure and Applied Logic*, **89**, 17–35.

Bès, A., & Korec, I. (1998). Definability within structures related to Pascal's triangle modulo an integer. *Fundamenta Mathematicae*, **156**, 111–129.

Bès, A., & Richard, D. (1998). Undecidable extensions of Skolem arithmetic. *Journal of Symbolic Logic*, **63**, 379–401.

Büchi, J. R. (1962). On a decision method in restricted second order arithmetic. In Nagel, E., Suppes, P., & Tarski, A., eds. *Logic, Methodology and Philosophy of Science*, pp. 1–11. Stanford University Press.

Cegielski, P. (1996). Definability, decidability, complexity. *Annals of Mathematics and Artificial Intelligence*, **16**, 311–341.

Halpern, J. Y. (1991). Presburger arithmetic with unary predicates is Π^1_1 complete. *Journal of Symbolic Logic*, **56**, 637–642.

Korec, I. (2001). A list of arithmetical structures complete with respect to the first-order definability. *Theoretical Computer Science*, **257**, 115–151.

Korec, I. (1995). Elementary theories of structures containing generalized Pascal triangles modulo a prime. In Shtrakov, S., & Mirchev, I., eds. *Discrete Mathematics and Applications* (Blagoevrad/Predel, 1994), pp. 91–102. Blagoevgrad.

Korec, I. (1993). Definability of arithmetic operations in Pascal triangle modulo an integer divisible by two primes. *Grazer Mathematische Berichte*, **318**, 53–62.

Maurin, F. (1997). The theory of integer multiplication with order restricted to primes is decidable. *Journal of Symbolic Logic*, **62**, 123–130.

Rabin, M. O. (1969). Decidability of second-order theories and automata on infinite trees. *Transactions of the American Mathematical Society*, **141**, 1–35.

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

Speranski, S. O. (2013). A note on definability in fragments of arithmetic with free unary predicates. *Archive for Mathematical Logic*, **52**, 507–516.

Speranski, S. O. (2016). Quantifying over events in probability logic: an introduction. *Mathematical Structures in Computer Science*. DOI: 10.1017/S0960129516000189