Notre Dame Journal of Formal Logic
Volume 30, Number 1, Winter 1989

The Elementary Theory of the Natural Lattice Is Finitely Axiomatizable

PATRICK CEGIELSKI

Introduction It is well known that the set of positive integers with the divisibility relation is a lattice, indeed the prototype of lattices. Here we call it the *natural lattice*. What are the differences between this lattice and other lattices? What are the particular properties (in the language of lattices, defined below) of this lattice? How should it be characterized?

Some linear orders have been studied (the natural order of the positive integers by Dedekind in [5], the orders of rationals and of reals by Cantor in [2], see also [9]). But no characterizations exist for particular lattices.

A mathematical characterization exists for $(\mathbb{N}^*,/)$. It is a partial order with a least member, 1, a denumerable set of atoms (the prime numbers), each member x has a *p-successor* for each atom p (the product $p \cdot x$), and the following *multi-induction principle*: a subset A of $\mathbb{N}^*$ which contains 1, and is such that if x belongs to A then $p \cdot x$ belongs to A for all atoms p, is $\mathbb{N}^*$. But this characterization is not in the hierarchy of logical languages (first-order, second-order, . . .). (In particular, this characterization is not expressible in a second-order language because of the denumerability of the set of atoms).

The logical language of the theory of lattices is naturally the first-order language of partial order, with only a binary predicate, denoted by $\leq$. Our aim is to characterize (i.e., to axiomatize) the first-order theory *DIV* of the structure $(\mathbb{N}^*,/)$. *DIV* is consistent, complete, but not $\aleph_0$-categorical (the standard model is not the only countable model). This theory is decidable (stated by Skolem in [13], but proved first by Mostowski in [12]), thus recursively axiomatizable. But the computational complexity of the axiomatization given by this method is very awkward. We show that this theory is finitely axiomatizable, giving an explicit finite axiomatization. This fact seems prominent because relatively few theories of structures are finitely axiomatizable. The theory of addition and the theory of multiplication are not (see [3]).

Received May 19, 1986; revised January 19, 1987

1 The axiomatization We present the axiomatization in two parts. In the second part axioms are stated in the first-order language with the binary predicate $\leq$ (which represents / for the standard model) and immediate extensions by definitions. In the first part we present the axioms informally and give reasons for their choice. The axiomatization cannot be a mere translation of a natural characterization. After obvious axioms we add, one by one, first-order properties which can complete the theory, while trying to verify that it is complete (roughly by the method of elimination of quantifiers).

We hope to arrive at a simple and natural axiomatization and to eliminate the axioms introduced solely in order to have elimination of quantifiers.

1.1 Comments $(\mathbb{N}^*, /)$ is a lattice (Axioms A1 to A5, Pierce's definition). We don't say that the lattice is distributive because this follows from other axioms. The lattice has a least element (A6). *Warning*: This element is denoted by 0 because the order relation is denoted by $\leq$, but this element is obviously 1 in the standard model.

Any element x of the standard model is the join of the primary numbers (i.e., powers of a prime number, join irreducible in the theory of lattices) less than x (A7). We say that a *lattice* is *pre-F-decomposable* iff it satisfies this condition A7. This name is used because A7 is a condition for decomposability by fibers. The lattices shown in Figure 1 and 2 are not pre-F-decomposable.

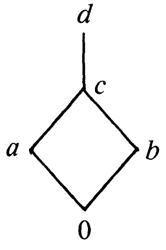

Figure 1.

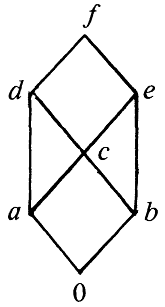

Figure 2.

An element of the standard model is characterized by its valuations (for any prime p, the p-valuation of x is the greatest p-primary number p^{α} which divides x; it is not the usual valuation, but we cannot define α in this language). For a given p, the set of p-primary numbers is a *fiber* (an equivalence class for comparability of join-irreducibles in a general lattice). A *lattice* is *fibered* iff it determines fibers (A8).

If $(F_i)_{i \in I}$ is the set of fibers of a fibered pre-F-decomposable lattice $(E, \leq)$ and x an element of E, then x determines a cut on any fiber F_i (the set of elements of this fiber less than x). This cut does not necessarily have a greatest element (cf. Section 1.3), but this holds in general for *lattices decomposable by fibers* (A9).

Such a lattice is (modulo an isomorphism) a part of $\prod_{i \in I} F_i$. Then $VAL(x, \alpha)$ says α is a join-irreducible, the greatest element less than x in a fiber.

In the standard model if $VAL(x, \alpha)$, $VAL(y, \beta)$ and α and β belong to the same fiber then we have: $VAL(x \vee y,\ \alpha \vee \beta)$ and $VAL(x \wedge y,\ \alpha \wedge \beta)$. But this is false in the lattice (shown in Figure 3) decomposable by fibers: $e = a \vee b$, $VAL(a, a)$, $VAL(b, 0)$, $VAL(e, c)$ but $c \neq 0 \vee a$. Then we add an axiom of regularity (A10). The formulation of this axiom is difficult because fibers have no canonical representatives.

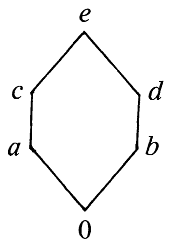

Figure 3.

This kind of formulation is simpler if the lattice is atomic (A11, i.e., any integer has a prime divisor in the standard model). But we have given the general definition of an F-decomposable lattice because this new notion seems to us very interesting, and regular F-decomposable lattices exist which are not atomic; for example, $(\mathbb{R}^+)^I \cup \mathbb{N}^I$ with functional order (i.e., $f \leq g$ iff $\forall x \in I\, f(x) \leq g(x)$).

The next step is to express that the set of atoms is infinite. It is generally impossible by a first-order formula, but here the elements x we are interested in have *finite supports* (in the standard model, only a finite number of prime integers divide x). Thus we can say: for any x there exists an atom a not less than x (A12). The axiom A12 means more than "to have an infinite set of atoms" because if E is an infinite set then $(\mathcal{P}(E), \subseteq)$ is an atomic regular F-decomposable lattice with an infinite set of atoms but which does not verify Axiom A12.

We can say that any element x has a support (A13, in the standard model the set of prime numbers which divide x, or the product of those elements because we cannot speak of the set). We shall see in Section 1.3 that this axiom is independent. Axiom A12 shows that supports are *pseudo-finite.*

An element of such a lattice is a (total) map f over an infinite set I which at i assigns an element of a chain F_i with a least element. The element f has a pseudo-finite support (the set of i such that $f(i) \neq 0$). In the standard model the set of these mappings also satisfies the following stability properties:

(1) The restriction of such a mapping to the support (of another element) is such a mapping (A14).

(2) Fibers are discrete (A15) and those mappings are *incrementable*, i.e., we can add 1 at any nonnull valuation (A16).
(3) Given such mappings f and g, there exists a mapping h whose support is the set of i such that $f(i) \leq g(i)$ (A17).

1.2 The axioms

A1 (Reflexivity) $\forall x(x \leq x)$.

A2 (Antisymmetry) $\forall x,y((x \leq y \;\&\; y \leq x) \to x = y)$.

A3 (Transitivity) $\forall x,y,z((x \leq y \;\&\; y \leq z) \to x \leq z)$.

A4 (G.L.B.) $\forall x \forall y \exists z(z \leq x \;\&\; z \leq y \;\&\; \forall t\ ((t \leq x \;\&\; t \leq y) \to t \leq z))$. (This z, which is unique by A2, is denoted by $x \wedge y$.)

A5 (L.U.B.) $\forall x \forall y \exists z(x \leq z \;\&\; y \leq z \;\&\; \forall t\ ((x \leq t \;\&\; y \leq t) \to z \leq t))$. (This z, which is unique, is denoted by $x \vee y$.)

A6 (Least element) $\exists x \forall y(x \leq y)$. (This element is denoted by 0.)

Definition 1 An element x of a lattice is *join-irreducible* iff it satisfies: $\forall a,b$ $(x = a \vee b \to (x = a$ or $x = b))$.

This is denoted by $SI(x)$ (or $SI^*(x)$ if x is not zero).

A7 (Pre-F-decomposability) $\forall x,y(\forall z((SI(z) \;\&\; z \leq x) \to z \leq y) \to x \leq y)$.

Proposition 1 *In a pre-F-decomposable lattice an element is characterized by the set of join-irreducible elements less than it:* $\forall x,y\ (x = y \leftrightarrow \forall z(SI(z) \to (z \leq x \leftrightarrow z \leq y)))$.

A8 (Fibered lattice) $\forall x,y,z((SI^*(x) \;\&\; SI^*(y) \;\&\; SI^*(z) \;\&\; ((x \leq z \;\&\; y \leq z)\ or\ (z \leq x \;\&\; z \leq y))) \to (x \leq y\ or\ y \leq x))$.

Proposition 2 *The relation ($x \leq y$ or $y \leq x$) is an equivalence relation on SI^* in a fibered lattice, denoted by $x \sim y$. An equivalence class plus 0 is a fiber (it is a chain with a least element).*

A9 (F-decomposability) $\forall x,a((SI^*(a) \;\&\; a \leq x) \to \exists b(SI(b) \;\&\; b \leq x \;\&\; a \leq b \;\&\; \forall c((SI(c) \;\&\; c \leq x \;\&\; a \leq c) \to c \leq b)))$.

Then b is called a *valuation* of x and we denote this by $VAL(x,b)$.

Proposition 3 *In an F-decomposable lattice we have:*

(1) $\forall x,y(x \leq y \leftrightarrow \forall a(VAL(x,a) \to a \leq y))$.
(2) $\forall x,y(x = y \leftrightarrow \forall a(VAL(x,a) \leftrightarrow VAL(y,a)))$.

A10 (Regularity) $\forall x,y,a,b((VAL(x,a) \;\&\; VAL(y,b) \;\&\; ((a = b = 0\ or\ (a = 0 \;\&\; b \neq 0 \;\&\; \forall c((SI^*(c) \;\&\; b \sim c) \to c \nleq x))$ or $(0 < a \leq b))) \to (VAL(x \wedge y,a) \;\&\; VAL(x \vee y,b)))$.

Proposition 4 *A regular F-decomposable lattice is distributive.*

Proof: For example we show that:

$$\forall x,y,z(x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)).$$

Let a,b,c be members of the same fiber so that: $VAL(x,a)$, $VAL(y,b)$, $VAL(z,c)$ and, for example: $0 < a \leq b \leq c$.

Then, using A10 we have: $VAL(y \vee z,c)$, $VAL(x \wedge (y \vee z),a)$, $VAL(x \wedge y,a)$, $VAL(x \wedge z,a)$, $VAL((x \wedge y) \vee (x \wedge z),a)$. Hence $x \wedge (y \vee z)$ and $(x \wedge y) \vee (x \wedge z)$ have the same valuation in each fiber, and then are equal by Proposition 3.

If a is an atom, i.e., $a \neq 0$ & $\forall x(x \leq a \rightarrow (x = 0$ or $x = a))$, we denote this by $\mathbb{A}(a)$.

A11 (Atomicity) $\forall x(x \neq 0 \rightarrow \exists a(\mathbb{A}(a)\ \&\ a \leq x))$.

Proposition 5 *In a fibered atomic lattice there exists at most one atom dividing a join-irreducible, i.e.:*

$$\forall x(SI^*(x) \rightarrow \exists! a(\mathbb{A}(a)\ \&\ a \leq x)).$$

Consequences: In a fibered atomic lattice we can easily characterize fibers:

(1) x is zero or a join-irreducible greater than the atom a is denoted by $SI(a,x)$.

(2) A fiber is $F_a = \{x/SI(a,x)\}$ for an atom a. F_a is called the *fiber with base a*.

(3) An atomic fibered pre-F-decomposable lattice is F-decomposable iff: $\forall x,a(\mathbb{A}(a) \rightarrow \exists\alpha(SI(a,\alpha)\ \&\ \alpha \leq x\ \&\ \forall\beta((SI(a,\beta)\ \&\ \beta \leq x) \rightarrow \beta \leq \alpha)))$. This α is a valuation of x and is denoted by $V(a,x)$.

(4) An atomic F-decomposable lattice is regular iff: $\forall x,y,a(\mathbb{A}(a) \rightarrow (V(a,x \wedge y) = V(a,x) \wedge V(a,y)\ \&\ V(a,x \vee y) = V(a,x) \vee V(a,y)))$.

A12 (Infinite base) $\forall x(x \neq 0 \rightarrow \exists a(\mathbb{A}(a)\ \&\ a \nleq x))$.

Proposition 6 *A lattice with an infinite base has a (standard) infinite set of atoms.*

A13 (Supportability) $$\forall x \exists s \forall a(\mathbb{A}(a) \rightarrow ((V(a,x) \neq 0 \rightarrow V(a,s) = a)\ \&\ (V(a,x) = 0 \rightarrow V(a,s) = 0))).$$

This s, which is unique, is the support of x and is denoted by $SUPP(x)$.

A14 (Truncability) $$\forall x \forall y \exists z \forall a(\mathbb{A}(a) \rightarrow ((a \nleq x \rightarrow V(a,z) = V(a,y))\ \&\ (a \leq x \rightarrow V(a,z) = 0))).$$

This z, which is unique, is denoted by $\bar{T}(x,y)$ and is called the inverse truncate of y by x.

We then have:

Proposition 7 $$\forall x \forall y \exists z \forall a(\mathbb{A}(a) \rightarrow ((a \leq x \rightarrow V(a,z) = V(a,y))\ \&\ (a \nleq x \rightarrow V(a,z) = 0))).$$

This z, which is unique, is denoted by $T(x,y)$ and is called the direct truncate of y by x.

A15 (Discrete fibers)

(1) $\forall a,x(SI(a,x) \rightarrow \exists y(SI(a,y)\ \&\ x \leq y\ \&\ y \neq x\ \&\ \forall z((SI(a,z)\ \&\ x < z) \rightarrow y \leq z)))$. *This y, which is unique, is denoted by $S_a x$ and is called the a-successor of x.*

(2) $\forall a,x((SI(a,x)\ \&\ x \neq 0) \rightarrow \exists y(SI(a,y)\ \&\ S_a y = x))$. *This y, which is unique, is denoted by $P_a x$ and is called the a-predecessor of x.*

A16 (Incrementability) $\forall x \exists y \forall a(\mathbb{A}(a) \rightarrow ((a \not\leq x \rightarrow V(a,y) = 0)$
$\&\ (a \leq x \rightarrow V(a,y) = S_a V(a,x))))$.

This y, which is unique, is denoted by Ix and is called the increment of x.

A17 (Selection) $\forall x \forall y \exists y \forall a(\mathbb{A}(a) \rightarrow (V(a,z) = 0$ *or a and* $V(a,z) = a \leftrightarrow ((a \leq x$ *or* $a \leq y)\ \&\ V(a,x) \leq V(a,y)))$. *This z, which is unique, is denoted by* $SLCT(x,y)$.

Note: We have $SUPP(x) = SLCT(x,x)$, thus A13 is not necessary.

1.3 Independence of axioms The axioms are independent or, at least, Axiom Ai+1 is not a consequence of Axioms A1 to Ai (although sometimes of Axioms Aj for $j \neq i + 1$). We already showed this for all axioms except A8, A9, A13, and A17. We skip the proof for A8.

Independence of A9: E is a subset of the set of (partial) functions from $\mathbb{N}$ to $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$. f is an element of E iff:

- either f: $I \mapsto \mathbb{N}$ with I finite,
- or f: $I \mapsto \{\infty\}$ with $I = 2^n \cdot 3^m \cdot \mathbb{N}$ (then we say f is an *infinite element*).

The order is the ordinary functional order:

$$f \leq g \leftrightarrow (D_f \subseteq D_g \text{ and } \forall x \in D_f\ f(x) \leq g(x)).$$

$(E,<)$ is a lattice. Join-irreducibles are functions whose domain is a set with one element and whose value is in $\mathbb{N}$ (an infinite element is not a join-irreducible because: $2^n \cdot 3^m \cdot \mathbb{N} = 2^{n+1} \cdot 3^m \cdot \mathbb{N} \vee 2^n \cdot 3^{m+1} \cdot \mathbb{N}$). This lattice is fibered, pre-F-decomposable but not F-decomposable.

Independence of A13: E is the set of mappings from $\mathbb{N}$ to $\mathbb{N}$ with $\{x/f(x) = 1\}$ finite, with functional order. This is an atomic regular F-decomposable lattice. Supports are mappings from $\mathbb{N}$ to $\{0,1\}$ with finite $\{x/f(x) = 1\}$. Then the constant mapping 2 has no support.

Independence of A14: E is the set of subsets A of $\mathbb{N}$ with A finite or $A = 2^n \cdot \mathbb{N} \cup F$ with $n \in \mathbb{N}^*$ and F finite. $(E,\subseteq)$ satisfies A1 to A13 but not A14 because $\bar{T}(\{2\},2 \cdot \mathbb{N})$ is not an element of E.

Independence of A15:

(1) The set $\mathcal{P}_f(I)$ of finite subsets of an infinite set I with inclusion satisfies A1 to A14 but not A15.

(2) The set of mappings f from $\mathbb{N}$ to the subset $\{0\} \cup [1,\infty)$ of $\mathbb{R}$ with finite support, with functional order, satisfies A1 to A14 but not A15.

(3) The set of mappings f from $\mathbb{N}$ to $\omega + \omega$ with finite support, with functional order, satisfies A1 to A14, A15(1) but not A15(2).

Independence of A16: E is the set of mappings f form $\mathbb{N}$ to $\mathbb{N}$ satisfying:

$\forall n \in F$, no condition on $f(n)$,
$\forall n \in (2\cdot\mathbb{N}\backslash 4\cdot\mathbb{N})\backslash F$, 2 divides $f(n)$,
$\forall n \in 4\cdot\mathbb{N}\backslash F$, 3 divides $f(n)$,
otherwise, $f(n) = 0$,

where F is a finite set. E with the functional order satisfies A1 to A15 but not A16.

Independence of A17: E is the set of mappings f from $\mathbb{N}$ to $\omega + (\omega^* + \omega)\cdot\phi$ (a nonstandard denumerable model of ω) satisfying:

$\forall n \in F$, no condition on $f(n)$,
$\text{card}(f[(2\cdot\mathbb{N}\backslash 4\cdot\mathbb{N})\backslash F] \cap \mathbb{N}) \leq 1$,
$\text{card}(f[4\cdot\mathbb{N}\backslash F] \cap \mathbb{N}) \leq 1$,
otherwise, $f(n) = 0$,

where F is a finite set. E with the functional order satisfies A1 to A16, but not A17.

2 The main theorem

Theorem *Lattices satisfying A1 through A17 are the same as lattices elementarily equivalent to* $(\mathbb{N}^*,/)$.

It suffices to prove that the theory with Axioms A1 to A17 (the theory denoted by *DIV*) is complete. We use elimination of quantifiers, taking inspiration from the method of Feferman–Vaught.

2.1 The theory of natural order An axiomatization of the theory of $(\mathbb{N},\leq)$ is well known [10]: the order is total, discrete, with a least element, but without a greatest element, i.e., it satisfies Axioms N1, N2, N3, N5 (= A1, A2, A3, A6) and:

N4 $\forall x,y(x \leq y \textit{ or } y \leq x)$.

N6 $\forall x \exists y(x \leq y \;\&\; y \neq x \;\&\; \forall z((x \leq z \;\&\; z \neq x) \rightarrow y \leq z))$. *This y, which is unique, is called the successor of x and is denoted by Sx.*

N7 $\forall x(x \neq 0 \rightarrow \exists! y(x = Sy))$.

A proof that the theory with Axioms N1 to N7 is complete is in [6], pp. 184–187, but with a slightly different axiomatization. The language $(0,\leq,S)$, without $=$, permits elimination of quantifiers.

2.2 The lattice of finite subsets of a set The theory F of the class of structures $(P_f(I),\subseteq)$ is known [7] to be axiomatized by: the lattice is distributive, relatively complemented, with a least element and is completely atomic, i.e. satisfies Axioms F1, F2, F3, F4, F5, F7, F10 (= A1, A2, A3, A4, A5, A6, A12) and:

F6 $\forall x,y,z \ x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z), x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

F8 $\forall x \forall y \exists z (z \leq x \ \& \ x \leq z \vee y \ \& \ z \wedge y = 0)$. *This* z, *which is unique, is denoted by* $x \backslash y$.

F9 (Characterization by atoms) $\forall x,y (\forall a (\mathbb{A}(a) \rightarrow (a \leq x \leftrightarrow a \leq y)) \rightarrow x = y)$.

This theory is complete. We even have elimination of quantifiers in the language $(\wedge, \backslash, (A_n)_{n \in \mathbb{N}^*})$, without $=$, where A_n is the unary predicate "to have at least n atoms" defined by:

$$\exists a_1, \ldots, a_n \Big(\bigwedge_{1 \leq i < j \leq n} a_i \neq a_j \ \& \bigwedge_{1 \leq i \leq n} (\mathbb{A}(a_i) \ \& \ a_i \leq x) \Big).$$

The author has verified these claims in 1979, in an unpublished work, using Karp's method. The proof is too long to appear here.

2.3 Interpretation of ω *and* F *in* DIV

Definition 1 Let $\mathfrak{A}$ be a model of DIV, A its domain, a an atom of $\mathfrak{A}$ (i.e., $a \in A$ and $\mathfrak{A} \models \mathbb{A}(a)$). We denote by $\mathfrak{A}_a$ the structure $(A_a, \leq)$ where: $A_a = \{x \in A / \mathfrak{A} \models \mathrm{SI}(a,x)\}$ and $\leq$ is the restriction of $\leq$ to A_a.

Proposition 1 $\mathfrak{A}_a$ *is a model of* ω, *the theory with Axioms N1 through N7.*

Definition 2 We denote by $\mathfrak{A}_F$ the structure $(A_F, \leq)$ where A_F is the set of supports, i.e.:

$$A_F = \{x \in A / \mathfrak{A} \models \forall a (\mathbb{A}(a) \rightarrow V(a,x) = a \text{ or } 0)\}.$$

Proposition 2 $\mathfrak{A}_F$ *is a model of* F, *the theory with Axioms F1 through F10.*

Proof: Distributivity follows from Section 1.2, by Proposition 4. We have $x \backslash y = \bar{T}(y,x)$.

2.4 A first elimination of quantifiers

Definition 3 Let $\phi(x_1, \ldots, x_n)$ be a formula of the language $(\leq)$ with its free variables among $x_1, \ldots, x_n$. Then we denote by ϕ^p the formula of the language $(\leq, V(.,.))$, with supplementary free variable p, defined by: $\phi(V(p,x_1), \ldots, V(p,x_n))$.

Proposition 3 *Let $\mathfrak{A}$ be a model of DIV, p an atom of $\mathfrak{A}$, $a_1, \ldots, a_n$ elements of A and $b_i = V(p, a_i)$ for $1 \leq i \leq n$. Then*:

$$\mathfrak{A} \models \phi^p(a_1, \ldots, a_n) \text{ iff } \mathfrak{A}_p \models \phi(b_1, \ldots, b_n).$$

Proof: By induction on the rank of the formula ϕ.

Definition 4 If θ is a formula of the language $(\leq)$ we denote by $A_k(\theta)$ ("there are at least k atoms p whose p-adic valuations satisfy θ") the formula:

$$\exists p_1, \ldots, p_k \left(\bigwedge_{1 \leq i < j \leq k} p_i \neq p_j \;\&\; \bigwedge_{1 \leq i \leq k} (\mathbb{A}(p_i) \;\&\; \theta^{p_i}) \right).$$

Theorem 1 *The language $(A_k(\theta))_{k \in \mathbb{N}, \theta \in Fl(\leq, 0, S)}$ permits elimination of quantifiers for DIV.*

Proof: We show by induction on the rank of the formula that: $DIV \vdash \phi \leftrightarrow \psi$, with ψ a formula of the same language but without quantifiers.

We easily have:

$$\begin{aligned} x \leq y &\leftrightarrow \forall p \in A (V(p,x) \leq V(p,y)) \\ &\leftrightarrow \neg A_1(\neg (x \leq y)). \end{aligned}$$

We must note that $x \leq V(p,y)$ does not occur. Then the main case is $\phi = \exists x\ \psi(x, \vec{y})$, where ψ is:

$$\bigwedge_{1 \leq i \leq m} A_{k_i}(\theta_i(x, \vec{y})) \;\&\; \bigwedge_{m+1 \leq i \leq n} \neg A_{k_i}(\theta_i(x, \vec{y})).$$

Definition 5 *Formulas $(\theta_i(x, \vec{y}))_{1 \leq i \leq n}$* are *independents* iff for $i \neq j$, θ_i & θ_j is contradictory.

We note that $S_k(\theta)$ for $A_k(\theta)$ & $\neg A_{k+1}(\theta)$ (meaning there exist exactly k atoms p such that the p-adic valuations satisfy θ).

Lemma 1 *We can suppose that ψ is of the form: $\bigwedge_{1 \leq i \leq m} A_{k_i}(\theta_i(x, \vec{y}))$ & $\bigwedge_{m+1 \leq i \leq n} S_k(\theta_i(x, \vec{y}))$ & $\bigwedge_{n+1 \leq i \leq q} \neg A_{k_i}(\theta_i(x, \vec{y}))$, with independents θ_i.*

Proof: Begin with equivalences such as: if $k \leq r$ then

$$A_k(\theta) \;\&\; A_r(\theta') \leftrightarrow \bigvee_{n=0}^{k} (S_n(\theta \;\&\; \theta') \;\&\; A_{k-n}(\theta \;\&\; \neg\theta') \;\&\; A_{r-n}(\neg\theta \;\&\; \theta')).$$

Then use the distributive law for $\exists$ and disjunction. There are n formulas θ_i in the input and 2^n in the output.

Remarks: To understand the formula of Lemma 3 it is necessary to note the following facts:

(1) If $\omega \models \theta_i(0,\vec{0})$ for $i \in [n+1,q]$ then $\exists x\psi(x,\vec{y})$ is false because the number of atoms is (standard) infinite.
(2) But we can have: $\omega \models \theta_i(x,\vec{0})$ if $x \neq 0$.
(3) If θ is a sentence, $\omega \models \theta$ is expressible in *DIV* using θ^p, the choice of atom p is irrelevant.

Definition 6 If $\mathfrak{A}$ is a model of *DIV* and $\vec{a} = (a_1,\ldots,a_n)$ is an element of A^n then the *support* of $\vec{a}$ is: $supp(\vec{a})$ = L.U.B. (supp(a_1),...,supp(a_n)), i.e., is the set of atoms dividing at least one a_i.

Lemma 2 *Let $\theta(x_1,\ldots,x_n)$ be a formula of the language $(\leq)$, with free variables among $x_1,\ldots,x_n$, $n \geq 1$, $\mathfrak{A}_n$ a model of DIV and $\vec{a} = (a_1,\ldots,a_n)$ an element of A. Then*: $\exists s,\forall p \in \mathbb{A}(V(p,s) = 1$ *or* p *and* $V(p,s) = p \leftrightarrow (p \leq$ supp$(\vec{a})$ & $\theta^p(\vec{a})))$. *This unique s is denoted by* supp$(\theta(\vec{a}))$. *It is the set of atoms whose valuations satisfy θ.*

Proof:

- If θ is a formula without a quantifier (which is the only case to consider because theory ω admits elimination of quantifiers), θ is a Boolean combination of atomic formulas: $S^kx \leq S^ry$, where negation does not occur because the negation of such a formula is an atomic formula.
- If supp$(\phi(\vec{x}))$ and supp$(\psi(\vec{x}))$ exist, then supp$(\phi(\vec{x}) \vee \psi(\vec{x}))$ and supp$(\phi(\vec{x}) \wedge \psi(\vec{x}))$ exist with: supp$(\phi(\vec{x}) \vee \psi(\vec{x}))$ = supp$(\phi(\vec{x})) \vee$ supp$(\psi(\vec{x}))$ and supp$(\phi(\vec{x}) \wedge \psi(\vec{x}))$ = supp$(\phi(\vec{x})) \wedge$ supp$(\psi(\vec{x}))$. If we have $\phi(\vec{x})$ and $\psi(\vec{y})$ with $\vec{x} \neq \vec{y}$ then expressions are a little more elaborate.
- The problem is to show that supp$(S^kx \leq S^ry)$ exists, with x,y variables or constant 0. Let $a,b \in A$. Then:

$$(1)\ \text{supp}(k \leq r) = \begin{cases} \text{supp}(\vec{a}) & \text{if } k \leq r, \\ 1 & \text{if } k > r. \end{cases}$$

$$(2)\ \text{supp}(S^ka \leq r) = \begin{cases} \text{supp}(a',b') \text{ if } k > r, \\ \text{supp}(a',b') \vee \bar{T}(a,\text{supp}(\vec{a})) \text{ if } k \leq r, \end{cases}$$

with $a' = I^ka$ (i.e., $a' = \underbrace{II\ldots Ia}_{k \text{ times}}$), $b' = I^r(\text{supp}(\vec{a}))$.

$$(3)\ \text{supp}(r \leq S^ka) = \begin{cases} \text{supp}(b',a') \text{ if } k < r, \\ \text{supp}(b',a') \vee \bar{T}(a,\text{supp}(\vec{a})) \text{ if } k \geq r. \end{cases}$$

$$(4)\ \text{supp}(S^ka \leq S^rb) = \begin{cases} \text{supp}(a',b') \text{ if } k > r, \\ \text{supp}(a',b') \vee \bar{T}(a \vee b,\text{supp}(\vec{a})) \text{ if } k \leq r, \end{cases}$$

with $a' = I^ka$, $b' = I^rb$.

Lemma 3 *If we denote* $S_i = \mathrm{supp}(\exists x\theta_i(x,\vec{y}))$ *and* $S = \mathrm{supp}(\vec{y})$ *then we have:*

$$\begin{aligned}
\exists x\phi(x,\vec{y}) \leftrightarrow \Bigg(& \bigwedge_{n+1\le i\le q} \neg\theta_i^p(0,\vec{0}) \\
& \& \bigvee_{\sigma\subset[1,p]} \Bigg(\bigwedge_{i\in\sigma} \exists x\theta_i^p(x,\vec{0}) \\
& \& \exists s_1,\ldots,s_q \Bigg(\bigwedge_{1\le i<j\le q} s_i \cap s_j = \emptyset \\
& \& \bigwedge_{1\le i\le q} s_i \subset S_i \ \& \ s_1 \cup s_2 \cup \ldots \cup s_q = S \\
& \& \bigwedge_{\substack{i\notin\sigma \\ 1\le i\le m}} \mathit{card}\ s_i \ge k_i \ \& \bigwedge_{\substack{i\notin\sigma \\ m+1\le i\le q}} \mathit{card}\ s_i \le k_i \\
& \& \bigwedge_{\substack{i\notin\sigma \\ m+1\le i\le n}} \mathit{card}\ s_i = k_i \ \& \bigwedge_{\substack{i\notin\sigma \\ n+1\le i\le q}} \mathit{card}\ s_i \le k_i \Bigg)\Bigg)\Bigg).
\end{aligned}$$

(The identity $s_1 \cup \ldots \cup s_q = S$ is necessary only if (θ_i) is a complete system, i.e., $\bigvee \theta_i$ is a tautology, if no inclusion is sufficient.)

Proof: Obvious when we have the good expression.

Proof of Theorem 1: Because ω is a complete theory, $\exists x\theta_i^p(x,\vec{0})$ is equivalent to $0 \ne 0$ or to $0 = 0$.

By elimination of quantifiers for the theory F we have only expressions such as: card $(\pm S_1 \cap \ldots \cap \pm S_q \cap \pm S) =$ (respectively, $\ge,\le$) k, i.e., S_k (respectively, $A_k, \neg A_{k+1}$) $(\pm\exists x\theta_1(x,\vec{y})\ \&\ldots)$. Hence there is no quantifier because of elimination of quantifiers for theory ω.

Corollary *Theory DIV is complete.*

Proof: Because any sentence of *DIV* is equivalent to a Boolean combination of sentences $A_k(\theta)$, with θ a sentence of theory ω. We know how to decide sentences of theory ω and $A_k(\theta)$ is true iff θ is true.

2.5 Elimination of quantifiers

Definition 7 We denote by $E_k(x)$ (meaning x has at least k atoms) the following formula:

$$\exists p_1,\ldots,p_k \Bigg(\bigwedge_{1\le i<j\le k} p_i \ne p_j \ \& \bigwedge_{1\le i\le k} (\mathbb{A}(p_i)\ \&\ p_i \le x) \Bigg).$$

Theorem 2 *The language* $L = (0,I,\mathrm{supp}(\ ,\ ),LUB(\ ,\ ),GLB(\ ,\ ),(E_k)_{k\in\mathbb{N}^*})$ *admits elimination of quantifiers for the theory DIV.*

Proof: It is sufficient to show that a formula $A_k(\theta)$, $k \in \mathbb{N}^*$, where θ is a formula of the language $(\le,S,0)$, is equivalent to a formula without quantifiers in the language L, using Theorem 1.

We can suppose that θ is without quantifiers, because the language $(\le,S,0)$ admits elimination of quantifiers for the theory ω.

Obviously we have:

Lemma 4 $A_k(\theta \vee \theta') \leftrightarrow \bigvee_{r=0}^{k} (A_r(\theta) \;\&\; A_{k-r}(\theta'))$.

Hence we can consider θ as a conjunction of formulas:

$$S^k x \leq S^r y \tag{1}$$

with x,y variables or constant 0.

Let $\theta = \theta_1 \;\&\ldots\&\; \theta_n$.

If θ_i is (1) with x,y variables, set $t_i = \mathrm{supp}(I^k x, I^r y)$.

If θ_i is (1) with, for example, x a variable and $y = 0$, set:

$$t_i = \begin{cases} \mathrm{supp}(I^k x, I^r(\mathrm{supp}(x))) & \text{if } k > r, \\ \mathrm{supp}(I^k x, I^r(\mathrm{supp}(x))) \vee \mathrm{supp}(\vec{x}) & \text{if } k \leq r, \end{cases}$$

where $\mathrm{supp}(x) = \mathrm{supp}(x,x)$, $\mathrm{supp}((x_1,\ldots,x_n)) = \mathrm{LUB}(\mathrm{supp}(x_1),\ldots,\mathrm{supp}(x_n))$.

If θ_i is $S^k 0 \leq S^r 0$ then θ is equivalent to $E_1(0)$ for $k > r$, and is not important for $k \leq r$.

Then: $A_k(\theta) \leftrightarrow E_k(\mathrm{GLB}(t_1,\ldots,t_n))$.

REFERENCES

[1] Birkhoff, G., *Lattice Theory*, Colloquium Publications Vol. 25, American Mathematical Society, Providence, Rhode Island, 1940; 2nd Ed., 1948; 3rd Ed., 1967.

[2] Cantor, G., “Beiträge zur Begründung der transfiniten Mengenlehre,” *Mathematische Annalen*, vol. 46 (1895), pp. 481–512; English translation in *Contributions to the Founding of the Theory of Transfinite Numbers*, 1915, reprinted by Dover, New York, 1955; French translation pp. 343–437 in *Mémoires de la Société des sciences physiques et naturelles de Bordeaux*, Hermann, Paris, 1899.

[3] Cegielski, P., “Théorie élémentaire de la multiplication des entiers naturels,” pp. 44–89 in *Model Theory and Arithmetic*, Lecture Notes in Mathematics 890, ed. C. Berline, K. McAloon, and J.-P. Ressayre, Springer-Verlag, Berlin, Heidelberg, New York, 1981.

[4] Cegielski, P., “La théorie élémentaire de la divisibilité est finiment axiomatisable,” *Comptes Rendus Hebdomadaires des Séances de L'Académie des Sciences, Paris*, 1st Series, vol. 299 (1984), pp. 367–369.

[5] Dedekind, R., *Was sind und was sollen die Zahlen?*, Friedrich Vieweg & Sohn, Braunschweig, 1888; reprinted as pp. 335–391 in *Gasammelte Mathematische Werke*, Vol. III, Friedrich Vieweg & Sohn, Braunschweig, 1932; English translation Dover, New York, 1963; French translation La Bibliothèque d'Ornicar, dif. Seuil, Paris, 1979.

[6] Enderton, H. B., *A Mathematical Introduction to Logic*, Academic Press, New York, 1972.

[7] Ershov, Y. L., “Decidability of the theory of relatively complemented distributive lattices and the theory of filters,” (in Russian), *Algebra i Logika*, vol. 3 (1964), pp. 17–38.

[8] Feferman, S. and R. L. Vaught, "The first order properties of products of algebraic systems," *Fundamenta Mathematicae*, vol. 47 (1959), pp. 57-103.

[9] Huntington, E. V., "The continuum as a type of order: An exposition of the modern theory," *Annals of Mathematics*, 2nd Series, vol. 6 (1904-1905), pp. 151-184, vol. 7 (1905-1906), pp. 15-43; republished as *The Continuum and Other Types of Serial Order*, Harvard University Press, Cambridge, Massachusetts, 1917, 2nd Ed., Dover, New York, 1955.

[10] Langford, C. H., "Some theorems on deducibility," *Annals of Mathematics*, 2nd Series, vol. 28 (1926-1927), pp. 16-40, 459-471.

[11] Michel, P., "Borne supérieure de la complexité de la théorie de ℕ muni de la relation de divisibilité," pp. 242-250 in *Model Theory and Arithmetic*, Lecture Notes in Mathematics 890, ed. C. Berline, K. McAloon, and J.-P. Ressayre, Springer-Verlag, Berlin, Heidelberg, New York, 1981.

[12] Mostowski, A., "On direct products of theories," *The Journal of Symbolic Logic*, vol. 17 (1952), pp. 1-31.

[13] Skolem, T., "Über einige Satzfunktionen in der Arithmetik," (1930), pp. 281-306 (with an English analysis by H. Wang, p. 34) in *Selected Works in Logic*, ed. J. E. Fenstad, Universitetsforlaget, Oslo, 1970; unpublished French translation by Claude Richard.

27, rue Dézobry
93200 Saint-Denis
France