Objectivite reality and mathematical structures

Petr Kůrka

February 6, 2008

1 Introduction

In [1] Z.Neubauer makes distinction between objective, constituted reality of modern science and natural reality of things like rocks, clouds or animals. Objective reality of scientific descriptions and data is based on objectivity of letters and words.

> These twenty-two letter-signs, signs of sites or of the place assignments constitute the fundaments of a reality we shall call the constituted or established reality, because, contrary to natural reality, it does not come-to-be (does not arise through becoming) but rather, it is established by order - through the order of the letters (Z.Neubauer [1], page 13).

An important special case is the objectivity of natural numbers.

> A number is not a name of an amount or of a count but the very numeric position, which is written down. It says it and indicates it at the same time. It does so through its objective reality - the given sequence of numeric signs - the relation of succession. That is why we find knowledge of numbers so easy - much easier than knowledge of the alphabet. We do not need to sort them: numbers are already sorted. There is no need to put them into an ordered line: they themselves form the ordered line: the very paradigm of everything linearly ordered. Neither do we need to look for them: numerals directly show where the corresponding numbers are - and not only indicate it: a number is its where - where we would find just it when looking for it. (Z.Neubauer [1], page 113).

There is a correspondence of this conception of objective reality with the formalistic conception of mathematics known as the Hilbert program. According to formalism, the objectivity of mathematical theorems and proofs is ensured by encoding them as words (strings of letters) of a formalized language. The correctness of proofs can be verified algorithmically, with no reference to the meaning of these theorems and proofs. In "Grundlagen der Mathematik I" [2], Hilbert and Bernays stress the objectivity and reliability of formalized mathematics and argue for the undoubtfulness of properties of natural numbers and words.

> In der Zahlentheorie haben wir ein Ausgangsobjekt und einen Prozeß des Fortschreitens. Beides müssen wir in bestimten Weise anschaulich festlegen. Die besondere Art der Festlegung ist dabei unwesentlich, nur muß die einmal getroffene Wahl für die ganze Theorie beibehalten werden. Wir wählen als Ausgangsding die Ziffer 1 und als Prozeß des Fortschreitens das Anhängen von 1.
>
> Die Dinge, die wir, ausgehend von der Ziffer 1, durch die Anwendung des Fortschreitungsprozesses erhalten, wie z.B.
>
> 1, 11, 1111
>
> sind Figuren von folgender Art: sie beginnen mit 1, sie enden mit 1; auf jede 1, die nicht schon Ende der Figur bildet, folgt eine angehängte 1. Sie werden durch Anwendung des Fortschreitungsprozesses, also durch einen konkret zum Abschluß kommenden *Aufbau* erhalten, und dieser Aufbau läßt sich daher auch durch einen schrittweisen *Abbau* rückgängig machen. (D.Hilbert, P.Bernays [2], page 20-21.)

Objective reality is grounded in objectivity of elements of certain mathematical structures, first of all, in the objectivity of natural numbers as elements of their **ordinal structure** formed by the **successor operation**. An essential property of this structure is that it is **definable**: Each number can be characterized and uniquely described by a property, i.e., by a logical formula which uses only the **successor predicate**. Thus 1 is the only number which is not preceded by any other number, 2 is the only number which is preceded only by 1, etc. For this reason, the ordinal structure of natural numbers is **asymmetric**, i.e., the only automorphism (self-mapping which preserves the successor relation) is the identity.

We treat here the concepts of definability and asymmetricity in the context of relational structures. A relational structure consists of an underlying set and several relations of specified arity. We present three main examples of definable structures. The first is the ordinal, ordered or additive structure of natural numbers, the second is the semigroup of finite words with distinguished letters or with order, and the third is the structure of (hereditarily) finite sets with the binary relation "belongs to".

2 Relational structures

Definition 1 *A* **type** *is a finite sequence* $\mathbf{n} = (n_1, \ldots, n_k)$ *of positive integers. A* **relational structure** *of type* $\mathbf{n}$ *is a system* $\mathcal{M} = (M, R_1, \ldots, R_k)$*, where* M *is a nonempty set (called the* **underlying set** *of* $\mathcal{M}$*), and* $R_i \subseteq M^{n_i}$ *is an* n_i*-ary relation on* M*.*

Here M^n is the set of all ordered n-tuples $(m_1, \ldots, m_n)$ of elements of M. A set $R \subseteq M^n$ is a hypostasied or reified relation between elements of M. A unary relation $R \subseteq M$ is a hypostasied property: it consists of those elements of M which have the property in question. An oriented graph is a structure of type (2), i.e., a pair (M, R), where $R \subseteq M^2$. We refer to elements of M as vertices, to elements of R as arrows (see Figure 1). An algebraic structure with a binary operation is a structure of type (3). If the operation is addition, then the relation consists of all triples $(p, q, p + q)$. In general, an n**-ary operation** on M is an $(n + 1)$-ary relation $R \subseteq M^{n+1}$, such that for each $m_1, \ldots, m_n \in M$ there exists a unique $m \in M$ with $(m_1, \ldots, m_n, m) \in R$. Not all mathematical structures are relational structures. For example, a topological space is a pair (M, τ), where M is the underlying set (of points) and $\tau \subseteq \mathcal{P}(M)$ is a set of open subsets of M.

Definition 2 *Let* $\mathcal{M} = (M, R_1, \ldots, R_k)$ *and* $\mathcal{M}' = (M', R'_1, \ldots, R'_k)$ *be structures of type* $\mathbf{n} = (n_1, \ldots, n_k)$*. An* **isomorphism** $F : \mathcal{M} \to \mathcal{M}'$ *is a bijective maping* $F : M \to M'$ *such that for each* $i \leq k$ *and for each* $(m_1, \ldots, m_{n_i}) \in M^{n_i}$ *we have*

$$(m_1, \ldots, m_{n_i}) \in R_i \iff (F(m_1), \ldots, F(m_{n_i})) \in R'_i$$

A self-isomorphism $F : \mathcal{M} \to \mathcal{M}$ *is called* **automorphism**. *A structure* $\mathcal{M}$ *is* **asymmetric** *if the only automorphism* $F : \mathcal{M} \to \mathcal{M}$ *is the identity.*

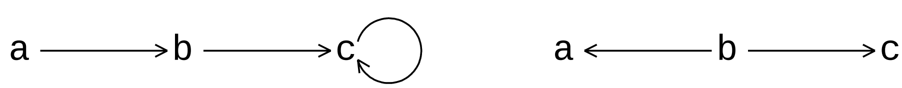

Figure 1: Graphs

Example 1 $\mathcal{M}_1 = (M, R_1)$*, where* $M = \{a, b, c\}$*,* $R_1 = \{(a, b), (b, c), (c, c)\}$ *(Figure 1 left), is a structure of type* (2)*, or a graph.*

It is easy to see that the graph $\mathcal{M}_1$ is asymmetric. Note that R_1 is a unary operation: for each $m \in M$ there exists exactly one $m' \in M$ such that $(m, m') \in R_1$. This means that from each vertex of the graph there leads exactly one arrow.

Example 2 *$\mathcal{M}_2 = (M, R_2)$, where $M = \{a, b, c\}$, $R_2 = \{(b, a), (b, c)\}$ (Figure 1 right), is a graph.*

The graph $\mathcal{M}_2$ is not asymmetric. There exists a nonidentical automorphism $F : \mathcal{M}_2 \to \mathcal{M}_2$ defined by $F(a) = c$, $F(b) = b$, $F(c) = a$.

Example 3 *The binary Boolean algebra is a structure $\mathcal{M}_3 = (M, R_\neg, R_\&)$ of type $(2, 3)$, where $M = \{0, 1\}$, $R_\neg = \{(0, 1), (1, 0)\}$, and*

$$R_\& = \{(0, 0, 0), (0, 1, 0), (1, 0, 0), (1, 1, 1)\}.$$

The structure $\mathcal{M}_3$ is asymmetric. Note that $R_\neg$ is a unary operation and $R_\&$ is a binary operation.

3 Predicate calculus

Given a type $\mathbf{n} = (n_1, \ldots, n_k)$, we have predicate calculus of formulas of type $\mathbf{n}$. For each $i \leq k$ we take a symbol r_i for n_i-ary predicate. We need symbols for variables, symbols for logical connections $\neg$ (negation), & (conjunction), $\vee$ (disjunction), $\Rightarrow$ (implication) $\Leftrightarrow$ (equivalence), symbols $\forall, \exists$ for the general and existential quantifiers and auxiliary symbols like commas and parenthesis. We have **atomic formulas** $r_i(x_1, \ldots, x_{n_i})$, where r_i is a symbol for n_i-ary predicate and $x_1, \ldots, x_{n_i}$ are variables. More complex formulas are formed from atomic formulas by logical connections and quantifiers. In the case of oriented graphs we write atomic formulas as $x \to y$. As an example of a formula consider $(\exists y)(x \to y)$. Here y is a **bound** variable (it is bound by a quantifier) while x is a **free** variable. The formula expresses a property of x, namely that there exists an arrow leading out of x. When we refer to such a formula we denote it as $\varphi(x) \equiv (\exists y)(x \to y)$, with the list of free variables in the parenthesis. A formula is **closed**, if it has no free variables. For example $\psi \equiv (\forall x)(\exists y)(x \to y)$ is a closed formula which means that from each vertex there leads an arrow.

Assume that $\varphi(x_1, \ldots, x_j)$ is a formula of type $\mathbf{n}$ with free variables $x_1, \ldots, x_j$ and that $m_1, \ldots, m_j \in M$ are elements of a structure $\mathcal{M} = (M, \ldots)$ of type $\mathbf{n}$. We write

$$\mathcal{M} \models \varphi[x_1/m_1, \ldots, x_j/m_j],$$

if φ is satisfied in $\mathcal{M}$ by elements $m_1, \ldots, m_j$. This is the Tarski concept of satisfiability (see e.g., Shoenfield [3]). For example, the formula $\varphi(x) \equiv (\exists y)(x \to y)$ is satisfied by every element of the structure $\mathcal{M}_1$ but only by the element b of the structure $\mathcal{M}_2$:

$$\begin{array}{lll} \mathcal{M}_1 \models \varphi[x/a], & \mathcal{M}_1 \models \varphi[x/b], & \mathcal{M}_1 \models \varphi[x/c], \\ \mathcal{M}_2 \not\models \varphi[x/a], & \mathcal{M}_2 \models \varphi[x/b], & \mathcal{M}_2 \not\models \varphi[x/c]. \end{array}$$

When φ is a closed formula, it does not speak about properties of particular elements, but it expresses a property of the structure as a whole. The closed formula $\psi \equiv (\forall x)(\exists y)(x \to y)$ is satisfied in $\mathcal{M}_1$ but not in $\mathcal{M}_2$. We write $\mathcal{M}_1 \models \psi$, and $\mathcal{M}_2 \not\models \psi$.

Definition 3 *An element $m \in M$ of a structure $\mathcal{M} = (M, \ldots)$ is* **definable***, if there exists a formula $\varphi(x)$ with one free variable x, which is satisfied only by m, i.e., $\mathcal{M} \models \varphi[x/m]$ while $\mathcal{M} \not\models \varphi[x/m']$ for each $m' \in M$ different from m. In this case we say that $\varphi(x)$ is a* **defining formula** *of m. We say that $\mathcal{M}$ is a* **definable structure***, if each element of $\mathcal{M}$ is definable.*

Theorem 4 *Every definable structure is asymmetric and either finite or countable.*

Proof: If $F : \mathcal{M} \to \mathcal{M}$ is an automorphism and $\varphi(x)$ a formula with one free variable, then $\mathcal{M} \models \varphi[x/m]$ if and only if $\mathcal{M} \models \varphi[x/F(m)]$. Since φ_m is satisfied only by m, we get $F(m) = m$. The cardinality of all formulas of a fixed type is countable. In uncountable structures (e.g., in structures whose underlying set is the set of real numbers) there is not enough formulas to define all elements.

In structure $\mathcal{M}_2$, neither a nor c are definable (because there exists an automorphism which interchanges them), while b is definable by formulas $(\exists y)(x \to y)$ or $\neg(\exists y)(y \to x)$. We see that an element may have several defining formulas. The structure $\mathcal{M}_1$ is definable. The defining formulas for a, b, c are

$$\begin{aligned} \varphi_a(x) &\equiv \neg(\exists y)(y \to x) \\ \varphi_b(x) &\equiv \neg(\exists y, z)(z \to y \;\&\; y \to x) \\ \varphi_c(x) &\equiv x \to x \end{aligned}$$

A defining formula of an element can be regarded as its **name**. Elements which are not definable are nameless, they cannot be named by any characteristic property. In giving examples of our structures $\mathcal{M}_1$ and $\mathcal{M}_2$ we have taken recourse to the language of set theory using names 'a', 'b', 'c' of some objects of the universum of sets. These are not really elements of the structure, but (arbitrarily chosen) names of these elements. The trick works as long as we use the same names in the list of elements of sets and in the list of ordered pairs of the relation. But we should imagine structures whose elements are not yet named as in Figure 2.

Besides defining elements of a structure we can define further relations between these elements.

Definition 5 *Let $\mathcal{M} = (M, R_1, \ldots, R_k)$ be a structure of type $\mathbf{n} = (n_1, \ldots, n_k)$. A relation $R \subseteq M^p$ is* **definable** *in $\mathcal{M}$, if there exists a formula $\varphi(x_1, \ldots, x_p)$ with p free variables, such that for each $m_1, \ldots, m_p \in M$ we have*

$$(m_1, \ldots, m_p) \in R \iff \mathcal{M} \models \varphi[x_1/m_1, \ldots, x_p/m_p]$$

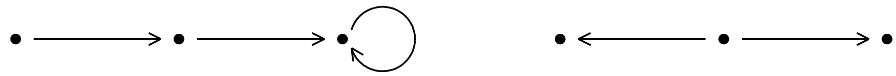

Figure 2: Graphs with nameless vertices

Trivially, each constituting relation $R_1, \ldots, R_k$ of a structure $\mathcal{M} = (M, R_1, \ldots, R_k)$ is definable in $\mathcal{M}$. In the structure $\mathcal{M}_1$ of Example 1, the relation $R = \{(a, c), (b, c), (c, c)\}$ is definable by formula $\varphi(x, y) \equiv (\exists z)(x \to z \;\&\; z \to y)$.

4 Natural numbers

The concepts of asymmetricity and definability apply to infinite structures as well. However, to determine an infinite structure and its properties is not so unproblematic as in the case of finite structures. Usually, infinite structures are conceived as objects whose existence and properties are proved in some version of set theory. We shall consider several structures on the set $\mathbb{N} = \{1, 2, 3, \ldots\}$ of natural numbers.

Natural numbers have at least two basic interpretations which are reflected in the difference between the linguistic categories of ordinal and cardinal numerals. Ordinal numerals refer to "counting in time". We recognize certain events as periodically recurring and distinguish them by ordinal numerals: the first, second and third day. The constituting relation is the relation between a number and its immediate successor. This is in fact a unary **successor operation**. Cardinal numerals, on the other hand, refer to "counting in space". We recognize certain things as objects of the same kind and give their number by a cardinal numeral: one, two or three pebbels. The constituting relations are the sum and product operations: any two numbers can be added or multiplied.

There is a one-to-one correspondence between ordinal and cardinal numerals but there is a difference in the structure which they support: the successor operation in the former case and the sum operation in the latter case. Using this one-to-one correspondence we can conceive natural numbers as possessing both these structures, and some others as well, for example the inequality relation.

Example 4 *The* **ordinal structure** $\mathcal{N}_{\rightarrow} = (\mathbb{N}, R_{\rightarrow})$ **of natural numbers** *is the infinite graph*

$$\bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \cdots$$

The successor relation $R_{\rightarrow}$ is a unary operation: for each $n \in \mathbb{N}$ there is a unique $n' \in \mathbb{N}$ such that $n \to n'$, or $(n, n') \in R_{\rightarrow}$. The ordinal structure is definable and therefore asymmetric. We name by 1 the only element to which there leads no arrow, by 2 the only element to which there leads an arrow only from 1, etc., so

$$R_{\to} = \{(1,2),(2,3),(3,4),(4,5),\ldots\}$$

The defining formulas are

$$\begin{aligned}
\varphi_1(x) &\equiv \neg(\exists y)(y \to x)\\
\varphi_2(x) &\equiv (\forall y)(y \to x \;\Leftrightarrow\; \varphi_1(y))\\
&\equiv (\forall y)(y \to x \;\Leftrightarrow\; \neg(\exists z)(z \to y))\\
\varphi_3(x) &\equiv (\forall y)(y \to x \;\Leftrightarrow\; \varphi_2(y))\\
&\;\vdots
\end{aligned}$$

Example 5 *The* **ordered structure** $\mathcal{N}_< = (\mathbb{N}, R_<)$ **of natural numbers** *consists of the set* $\mathbb{N}$ *of natural numbers and binary order relation*

$$R_< = \{(1,2),(1,3),(2,3),(1,4),(2,4),(3,4),\ldots\}$$

In $\mathcal{N}_<$, the successor and equality relations are definable by formulas

$$\begin{aligned}
x \to y &\equiv (x<y) \;\&\; \neg(\exists z)(x<z \;\&\; z<y)\\
x = y &\equiv \neg(x<y) \;\&\; \neg(y<x)\\
x \le y &\equiv (x<y) \vee (x=y)
\end{aligned}$$

Since the successor relation $R_{\to}$ is definable in $\mathcal{N}_<$, the structure $\mathcal{N}_<$ is definable and asymmetric. Defining formulas for 1 is e.g., $\varphi_1(x) \equiv (\forall y)(x<y)$.

Example 6 *The* **additive structure** $\mathcal{N}_+ = (\mathbb{N}, R_+)$ **of natural numbers** *is of type* (3)*.* R_+ *is the binary operation*

$$R_+ = \{(1,1,2),(1,2,3),(2,1,3),(1,3,4),(2,2,4),\ldots\}$$

In formulas we write the corresponding ternary predicate as $x+y=z$. In $(\mathbb{N}, R_+)$, the order relation is definable by formula $x<y \equiv (\exists z)(x+z=y)$. It follows that $\mathcal{N}_+ = (\mathbb{N}, R_+)$ is definable and asymmetric. Having more structure on $\mathbb{N}$, we get shorter defining formulas: If $\varphi_p(x)$ and $\varphi_q(x)$ are defining formulas for $p, q \in \mathbb{N}$, then we get a defining formula

$$\varphi_{p+q}(x) \equiv (\exists y,z)(x = y+z \;\&\; \varphi_p(y) \;\&\; \varphi_q(z))$$

for $p+q$. In the structure $(\mathbb{N}, R_+, R_\times)$ of natural numbers with addition and multiplication, defining formulas can be based on positional systems (see Section 5).

When we turn to the set of integers $\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$ with the standard successor operation

$$\cdots \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \bullet \longrightarrow \cdots$$

we see that $(\mathbb{Z}, R_\rightarrow)$ is not asymmetric: For any $a \in \mathbb{Z}$ there exists an automorphism $F_a : \mathbb{N} \rightarrow \mathbb{N}$ given by $F_a(x) = x + a$. Therefore $(\mathbb{Z}, R_\rightarrow)$ is not definable and, in fact, no element of $(\mathbb{Z}, R_\rightarrow)$ is definable. The structure $(\mathbb{Z}, R_+)$ is not asymmetric either: there is an automorphism $F(x) = -x$. The only definable element of $(\mathbb{Z}, R_+)$ is zero. Its defining formula is $\varphi_0(x) \equiv (\forall y)(x + y = y)$. However, the structure $(\mathbb{Z}, R_+, R_\rightarrow)$ of type $(3, 2)$ is definable.

5 Letters and words

As names of objects we use finite words (strings of letters) of an alphabet. Denote by A^+ the set of all words of an alphabet A. If $A = \{a, b\}$ is a two-letter alphabet, then the set of words is

$$A^+ = \{a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, aaaa, \ldots\}.$$

Two words can be concatenated, i.e., written one after the other. The concatenation is a binary operation which gives to the set A^+ a structure $(A^+, R_\bullet)$ of type (3) called the **free semigroup** over A. When $A = \{a, b\}$, then the operation of concatenation is

$$R_\bullet = \{(a, a, aa), (a, b, ab), (b, a, ba), (a, aa, aaa), (aa, a, aaa), (b, aa, baa), \ldots\}$$

For $u = u_1 \ldots u_n \in A^+$ we denote by $|u| = n$ its length and by u_i its i-th letter. If A has k letters, then there are exactly k^n words of length n. We write $u \sqsubseteq v$, if u is a **prefix** (initial part) of v, i.e., if $u_i = v_i$ for $i \leq |u|$. This includes also the case that u and v are equal.

Example 7 *If $A = \{1\}$ is a one-letter alphabet, then $A^+ = \{1, 11, 111, 1111, \ldots\}$. The free semigroup $(A^+, R_\bullet)$ is isomorphic to $(\mathbb{N}, R_+)$.*

Thus the free semigroup over a one-letter alphabet is both definable and asymmetric.

If A has at least 2 elements, then $(A^+, R_\bullet)$ is not asymmetric. Any permutation $f : A \rightarrow A$ (e.g. $f(a) = b$, $f(b) = a$) yields an automorphism $F : (A^+, R_\bullet) \rightarrow (A^+, R_\bullet)$ given by $F(u)_i = f(u_i)$. To obtain definability in the case of two or more letters, we have to add some structure. One possibility is to distinguish elements. We say that en element m of a structure is **distinguished**, if the structure contains a unary relation $\{m\}$ (which is subset of M). Any distinguished element is definable.

Example 8 *The* **free semigroup with distinguished letters** *over alphabet $\{a, b\}$ is the structure $\mathcal{M}_{a,b} = (\{a, b\}^+, R_\bullet, \{a\}, \{b\})$ of type $(3, 1, 1)$.*

The structure $\mathcal{M}_{a,b}$ is definable and the elements a and b are distinguished. To distinguish letters just means that we are able to tell them from each other. If r_a is the unary predicate corresponding to the unary relation $\{a\}$, then the defining formula of the letter a is $r_a(x)$. The defining formula of a word ab is $\varphi_{ab}(x) \equiv (\exists y, z)(x = yz \ \& \ r_a(y) \ \& \ r_b(z))$, and the defining formula of a word $u = u_1 u_2 \ldots u_n$ is

$$\varphi_u(x) \equiv (\exists y_1) \cdots (\exists y_n)(x = y_1 \ldots y_n \ \& \ r_{u_1}(y_1) \ \& \ \cdots \ \& \ r_{u_n}(y_n))$$

Another possibility to make the free semigroup definable is to add order. We start with a linearly ordered alphabet $(A, R_<)$. This means that we have a canonical (alphabetical) sequence of letters. We define then the **lexicographic order** on A^+ by

$$u < v \ \Leftrightarrow \ u \sqsubseteq v \text{ or } (\exists i \leq |u|)(u_i < v_i \ \& \ (\forall j < i)(u_j = v_j))$$

This is the order used in dictionaries. If $A = \{a, b\}$ and $a < b$, then the order between words of length at most 3 is

$$a < aa < aaa < aab < ab < aba < abb < b < ba < baa < bab < bb < bba < bbb$$

The structure $(A^+, R_\bullet, R_<)$ is definable since each letter is definable via ordering. Note that $(A^+, R_<)$ is not isomorphic to $(\mathbb{N}, R_<)$, since there is an infinite number of elements between a and b.

Words in alphabets of digits are used as names of natural numbers. In the binary positional system we use the alphabet $A = \{0, 1\}$ with order $0 \prec 1$. Rather than the lexicographic order, we use the **radix** order $R_\prec$ on A^+ defined by

$$u \prec v \ \Leftrightarrow \ (|u| < |v|) \ \vee \ (|u| = |v| \ \& \ (\exists i \leq |u|)(u_i \prec v_i \ \& \ (\forall j < i)(u_j = v_j)))$$

The order between words of length at most three is

$$0 \prec 1 \prec 00 \prec 01 \prec 10 \prec 11 \prec 000 \prec 001 \prec 010 \prec 011 \prec 100 \prec 101 \prec 110 \prec 111$$

The free semigroup with radix order is isomorphic to $(\mathbb{N}, R_<)$. The isomorphism, however, does not give the ususal binary positional system. In this system, 011 is not used as it has the same value 3 as the word 11. For names of natural numbers we use a subset of words which do not begin with 0:

$$\begin{aligned} M &= \{u \in \{0,1\}^+ : \ 0 \not\sqsubseteq u\} \\ &= \{1, 10, 11, 100, 101, 110, 111, 1000, 1001, \ldots\} \end{aligned}$$

The structure $(M, R_\prec)$ is also isomorphic to $(\mathbb{N}, R_<)$. Moreover, the isomorphism assigns to each natural number $x \in \mathbb{N}$ its binary expansion $u = u_1 \ldots u_k$ such that

$$x = 2^{k-1} \cdot u_1 + 2^{k-2} \cdot u_2 + \cdots 2 \cdot u_{k-1} + u_k.$$

6 Hereditarily finite sets

Hereditarily finite sets are finite sets whose elements are finite sets, the elements of their elements are finite sets, etc. Hereditarily finite sets are formed from the empty set in successive stages. At stage 0 we have only the empty set $\emptyset$ with no elements. At stage $n > 0$, we form sets from elements (sets) formed at previous stages. At stage 1 we can form only the set $\{\emptyset\}$ whose unique element is $\emptyset$. At stage 2 we form the set $\{\{\emptyset\}\}$ with unique element $\{\emptyset\}$ and the set $\{\emptyset, \{\emptyset\}\}$ with two elements $\emptyset$ and $\{\emptyset\}$. At the end of stage 2 we have therefore four sets with relation $\in$ (belongs to) given by the graph in Figure 3.

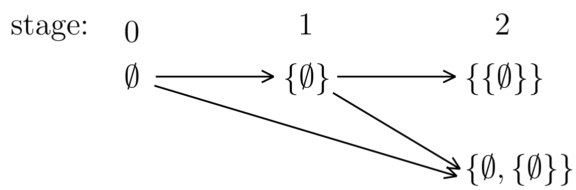

Figure 3: Hereditarily finite sets

At stage 3 we form sets from the four sets $a = \emptyset$, $b = \{\emptyset\}$, $c = \{\{\emptyset\}\}$, and $d = \{\emptyset, \{\emptyset\}\}$. From four elements, 16 sets can be formed: 1 empty set, 4 one-element sets, 6 two-element sets, 4 three-element sets and 1 four-element sets:

$$\begin{array}{l} \emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \\ \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\}, \\ \{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, \{a,b,c,d\}. \end{array}$$

However, among these sets there are also sets $a = \emptyset$, $b = \{a\}$, $c = \{b\}$, $d = \{a, b\}$ formed at previous stages. Thus only 12 new sets are formed at stage 3. The construction continues similarly at higher stages. If k_n is the number of sets formed by stage n, then $k_{n+1} = 2^{k_n}$. Thus we have $k_0 = 1$, $k_1 = 2$, $k_2 = 4$, $k_3 = 16$, $k_4 = 2^{16} = 65536$, $k_5 = 2^{65536} \approx 10^{19728}$, which is already quite a large number. The number of sets formed at stage $n + 1$ is $k_{n+1} - k_n$. The set $\mathbb{F}$ of hereditarily finite sets can be characterized as the smallest set which satisfies the following two properties:

1. $\emptyset \in \mathbb{F}$
2. If $m_1, \ldots, m_n \in \mathbb{F}$, then $\{m_1, \ldots, m_n\} \in \mathbb{F}$.

The structure $(\mathbb{F}, R_\in)$ of hereditarily finite sets is definable. The defining formulas of $\emptyset$, $\{\emptyset\}$, and of a general set $\{m_1, \ldots, m_n\}$ are

$$\begin{array}{rcl} \varphi_\emptyset(x) & \equiv & \neg(\exists y)(y \in x), \\ \varphi_{\{\emptyset\}}(x) & \equiv & (\forall y)(y \in x \;\Leftrightarrow\; \varphi_\emptyset(y)) \\ \varphi_{\{m_1,\ldots,m_n\}}(x) & \equiv & (\forall y)(y \in x \;\Leftrightarrow\; \varphi_{m_1}(y) \vee \cdots \vee \varphi_{m_n}(y)) \end{array}$$

The equality predicate is definable in $(\mathbb{F}, R_\in)$ by

$$x = y \equiv (\forall u)(u \in x \ \Leftrightarrow \ u \in y).$$

Hereditarily finite sets are used as representations of finite mathematical objects, for example as representations of nonnegative integers. The number zero is represented by the empty set $0 := \emptyset$, the number one by one-element set $1 := \{0\}$ and similarly $2 := \{0, 1\}$, $3 := \{0, 1, 2\}$, $4 := \{0, 1, 2, 3\}$, etc. These nonnegative integers satisfy the formula $\mathrm{ord}(x)$ (being an ordinal number)

$$\mathrm{ord}(x) \equiv (\forall u, v)(u \in v \in x \Rightarrow u \in x) \,\&\, (\forall u, v \in x)(u \in v \vee u = v \vee v \in u)$$

In fact, a hereditarily finite set satisfies formula $\mathrm{ord}(x)$ if and only if it is a nonnegative integer. Moreover, the relation $\in$ coincides with the order relation $<$ on nonnegative integers.

Another important new (defined) operation is the binary operation of ordered pair, ordered triple, etc.

$$(a, b) := \{\{a\}, \{a, b\}\}, \ (a, b, c) := ((a, b), c)$$

If a, b are different sets, then the sets (a, b) and (b, a) are different as well. Using the operation of ordered pair, we can represent finite relational structures as elements of the structure $(\mathbb{F}, R_\in)$. For example, the structure $\mathcal{M}_1$ from example 1 can be represented by the set

$$\mathcal{M}_1 = (\{a, b, c\}, \{(a, b), (b, c), (c, c)\})$$

Here a, b, c are arbitrary distinct (hereditarily finite) sets, for example $a = \emptyset$, $b = \{\emptyset\}$, and $c = \{\{\emptyset\}\}$.

7 Constants and terms

In infinite structures like $\mathcal{N}_\to = (\mathbb{N}, R_\to)$ or $(\mathbb{F}, R_\in)$, the naming of objects by defining formulas is not so unproblematic as in finite structures. A defining formula of 1 in $\mathcal{N}_\to$ is $\varphi_1(x) \equiv \neg(\exists y)(y \to x)$, which is equivalent to $(\forall y)\neg(y \to x)$. To verify whether the formula is satisfied for 1, i.e., whether $(\mathbb{N}, R_\to) \models \varphi_1[x/1]$ amounts to verifying $\neg(y \to x)$ for an infinite number of cases $y = 1$, $y = 2$, etc.

A viable alternative is to use in logical formalism **constants** and **function symbols**, and define elements of a structure by **terms**. This is possible when the relational structure in question $\mathcal{M} = (M, R_=, R_2, \ldots)$, contains among its relations the binary **identity relation** $R_= = \{(m, m) : \ m \in M\}$ which consists of all pairs of identical elements. If R_2 is another relation of the structure, which is an n-ary operation, then we write the coresponding atomic formula $r_2(x_1, \ldots, x_n, y)$ as $s_2(x_1, \ldots, x_n) = y$, where s_2 is a function symbol. A term is an expression formed from variables and function symbols. If we have a binary operation with function symbol $+$, then we have e.g., terms $+(x, y)$ or $+(x, +(y, z))$ which are usually written as $x + y$ or $x + (y + z)$. A special case of a function symbol is a constant, which corresponds to a 0-ary operation. A 0-ary operation is just a unary relation $R = \{m\}$ which contains a unique (distinguished) element. The atomic formula $r_m(x)$ is then $x = c_m$, where c_m is the constant (0-ary function symbol) corresponding to the distinguished element m.

Example 9 $\mathcal{N}_1 = (\mathbb{N}, R_=, R_\rightarrow, \{1\})$ *is a structure of type* $(2, 2, 1)$*, where* $R_=$ *is the identity relation,* $R_\rightarrow$ *is the successor relation and* 1 *is a distinguished element.*

In predicate calculus of type $(2, 2, 1)$ we have equality symbol $=$, the successor function symbol s and a constant $|$ (which is something different from the element 1 of the structure). Terms are expressions formed from variables and constants by successive applications of a function symbol s. Examples of terms are x, $s(x)$, $s(s(x))$, $|$, $s(|)$, $s(s(|))$, etc. Terms $|$, $s(|)$ and $s(s(|))$ are **closed**, since they do not contain variables. Atomic formulas are expressions $t_1 = t_2$, where t_1, t_2 are terms. In $\mathcal{N}_1$ we have simple defining formulas

$$\begin{aligned}
\varphi_1(x) &\equiv x = | \\
\varphi_2(x) &\equiv x = s(|) \\
\varphi_3(x) &\equiv x = s(s(|)) \\
&\vdots
\end{aligned}$$

Definition 6 *We say that* $\mathcal{M} = (M, R_1, \ldots)$ *is a* **structure with identity***, if* $R_1 = R_=$ *is the identity relation. We say that a structure with identity is* **term-definable***, if for each element* $m \in M$ *there exists a closed term* t_m*, such that* $\varphi_m(x) \equiv x = t_m$ *is a defining formula of* m*. In this case we say that* t_m *is a* **defining term** *of* m*.*

Thus $\mathcal{N}_1$ is term-definable. In a term-definable structure, we can name elements of the structure by closed terms. This means that the name of an element does not depend on the whole (infinite) structure but only on some finite fragment of it. The names $|$, $s(|)$, $s(s(|))$ of natural numbers depend only on the initial fragment $1 \rightarrow \bullet \rightarrow \bullet$ of the structure $\mathcal{N}_1$ of integers. To obtain a term-definable structure of words, we proceed analogously.

Example 10 *The* **free semigroup with identity and distinguished letters** *over the alphabet* $\{a, b\}$ *is* $\mathcal{M}_{a,b} = (\{a, b\}^+, R_=, R_\bullet, \{a\}, \{b\})$*. The structure is of type* $(2, 3, 1, 1)$ *and is term-definable.*

To define hereditarily finite sets by terms we must add two definable operations of unordered pair and union of two sets:

$$\begin{aligned}
\varphi_{\{\}}(x, y, z) &\equiv (\forall u)(u \in z \Leftrightarrow (u = x \vee u = y)) \\
\varphi_\cup(x, y, z) &\equiv (\forall u)(u \in z \Leftrightarrow (u \in x \vee u \in y))
\end{aligned}$$

8 Names

In conformity to the Hilbert program, terms and formulas are words in the alphabet of the predicate calculus of a given type. Whether we name elements of a structure by defining formulas or defining terms, names are always words. A peculiar situation arises in free semigroups. We can name a word aba by its defining formula $\varphi_{aba}(x) \equiv (\exists y, z, w)(x = yzw \mathbin{\&} r_a(y) \mathbin{\&} r_b(z) \mathbin{\&} r_c(w))$ or by its defining term $\overline{a} \bullet (\overline{b} \bullet \overline{a})$. Here $\overline{a}$ is a constant of the distinguished elelement a and $\bullet$ is the function symbol of concatenation. What we are doing is that we describe a word by a more complex word. The added symbols $\bullet, (,)$ are redundant - they do not carry any information. We can quite well describe a word aba by itself - this is the most economic way. Words are therefore unique in that they are their own names. This holds also for natural numbers when we conceive them as words $1, 11, 111, \ldots$ in a one-letter alphabet $\{1\}$. As for hereditarily finite sets, we can describe them by words in alphabet of four letters $\emptyset$ (empty set), , (comma), $\{$ (left bracket), $\}$ (right bracket). This is a description we have used in Figure 3.

9 Infinite sets

In set theory, the construction of hereditarily finite sets is extended to the construction of general (finite and infinite) sets at stages indexed by infinite ordinal numbers. Ordinal numbers include all nonnegative integers $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$ etc., but continue beyond them. The first infinite ordinal is the set $\omega = \{0, 1, 2, 3, \ldots\}$ of all nonnegative integers. Further ordinal numbers are

$$\begin{aligned}
\omega + 1 &= \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\} \\
\omega + 2 &= (\omega + 1) \cup \{\omega + 1\} = \{0, 1, 2, \ldots, \omega, \omega + 1\} \\
&\vdots \\
2\omega &= \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\} \\
2\omega + 1 &= \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, 2\omega\} \\
&\vdots
\end{aligned}$$

The successive construction of sets is continued as follows. At stage ω we have all hereditarily finite sets constructed at finite stages (see Section 6). At stage $\omega + 1$ we construct all sets from elements constructed by stage ω. Thus we get for example the set ω of nonnegative integers, the set $\mathbb{N} = \omega \setminus \{\emptyset\}$ of positive integers, the set of even positive integers, or the set $\mathbb{F}$ of all hereditarily finite sets. At stage $\omega + 2$ we construct all sets from elements constructed by stage $\omega + 1$. Thus we get some finite sets as a one-element set $\{\omega\}$ (whose element is an infinite set) and also new infinite sets as $\omega + 1$. When this construction process is performed through all stages of all ordinal numbers, the **universum** $\mathbb{V}$ of all sets is obtained. The universum $\mathbb{V}$ cannot be a set. It has the status of a **proper class** in the Gödel-Bernays set theory. The relation

$$\mathbb{E} := \{(x,y) : \ x \in y \in \mathbb{V}\} \subset \mathbb{V} \times \mathbb{V}$$

is also a proper class. It consists of all pairs of sets x, y such that $x \in y$. While there is in Gödel-Bernays set theory no pair $(\mathbb{V}, \mathbb{E})$, there are definable objects of such a "superstructure". We say that a set $m \in \mathbb{V}$ is **definable in** $\mathbb{E}$, if there exists a formula $\varphi(x)$ of set theory (build only from the predicate $\in$), such such that $\varphi(x)$ is satisfied only by m. This means that the formula

$$(\exists x)\varphi(x) \ \& \ (\forall x, y)(\varphi(x) \& \varphi(y) \ \Rightarrow \ x = y)$$

can be proved in the Gödel-Bernays set theory. In this sense, many important infinite sets are definable in $\mathbb{E}$. The unary predicate

$$\operatorname{ord}(x) \equiv (\forall u, v)(u \in v \in x \Rightarrow u \in x) \ \& \ (\forall u, v \in x)(u \in v \vee u = v \vee v \in u)$$

from Section 6 is satisfied exactly for (finite and infinite) ordinal numbers. The formula

$$\varphi_\omega(x) \equiv \operatorname{ord}(x) \ \& \ (\forall u \in x)(u = 0 \vee (\exists v)(u = v \cup \{v\}))$$

says that x is the first infinite ordinal number, so this is a defining formula of the set $\omega = \{0, 1, 2, 3, \ldots\}$ of nonnegative integers. By further constructions we can define the set $\mathbb{N} = \omega \setminus \{0\}$ of natural numbers (positive integers) or the set of odd positive integers.

There are many other subsets of ω which are definable in $\mathbb{E}$, but there are also subsets of ω which are not definable in $\mathbb{E}$. The set $\mathcal{P}(\omega)$ of all subsets of ω is not countable, so there is not enough words to describe all subsets of ω. On the other hand, the set $\mathcal{P}(\omega)$ is definable. The successor operation $S \subset \omega \times \omega$ is a subset of the cartesian product $\omega \times \omega$ of all pairs of nonnegative integers and is definable in $\mathbb{E}$ as well. Similarly, the order and addition operations are definable in $\mathbb{E}$, so structures as $\mathcal{N}_\rightarrow$, $\mathcal{N}_+$ or $\mathcal{N}_1$ are all definable in $\mathbb{E}$.

10 Real numbers

Usually, the system of real numbers is presented as a result of algebraical and topological completions of natural numbers in a sequence of number domains $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. Natural numbers cannot be always subtracted, so we get integers $\mathbb{Z}$ as results of their subtractions. Integers cannot be always divided, so we get rational numbers $\mathbb{Q}$ as their quotients. By topological methods we obtain the set $\mathbb{R}$ of real numbers using Dedekind cuts or Cauchy sequences of rational numbers. The successive constructions of these number domains and of algebraic structures built on them can all be performed within Gödel-Bernays set theory. Thus all these arithmetic structures are definable sets in $\mathbb{E}$.

Having the set $\mathbb{R}$ of real numbers, we get the structures of order, addition, multiplication, etc. Neither the ordered structure $(\mathbb{R}, R_<)$ of real numbers nor the additive structure $(\mathbb{R}, R_+)$ of real numbers are asymmetric for the same reason why the analogous structures of integers $\mathbb{Z}$ are not asymmetric. On the other hand, the ordered ring $\mathcal{R} = (\mathbb{R}, R_<, R_+, R_\times)$ of type $(2, 3, 3)$ is asymmetric. Both 0 and 1 are definable, therefore all rational numbers are definable and algebraic numbers (solutions of algebraic equations with integer coefficients) are definable as well. The defining formula for $\sqrt{2}$ is for example $\varphi_{\sqrt{2}}(x) \equiv (x \times x = 2)\ \&\ (x > 0)$. In fact, a real number is definable in $\mathcal{R}$ if and only if it is algebraic. Transcendent numbers like π or e are not definable in $\mathcal{R}$. However, real numbers are also elements of the universum $\mathbb{V}$ and the class of $\mathbb{E}$-definable real numbers is larger. Of particular interest are algorithmic real numbers.

Definition 7 *A real number x is* **algorithmic***, if there exists an algorithm (a Turing machine) which on input of a natural number n computes the n-th digit of the decimal expansion of x.*

Each algorithmic real number is definable in $\mathbb{E}$ and can be named by the text of the algorithm (or by the code of the Turing machine) which computes its decimal digits. The constructive analysis of A.A.Markov [5] based on the intuitionistic mathematics of Brouwer and Heyting [4] works only with these constructive real numbers. In the study of real functions, constructive analysis is concerned only with functions which can be described by an algorithm, and these algorithmic functions are $\mathbb{E}$-definable as well. Constructive analysis is more intuitive, but its mathematics is more complicated, since the existence of various algorithms must be repeatedly proved.

Classical mathematics, in contrast, assumes the existence of many undefinable objects whose objective reality is questionable. These mathematical "phantoms" are, however, very instrumental in simplifying the theory. The properties of these phantoms are expressed as theorems of set theory. The theorems and their proofs can be written in predicate calculus, and the correctness of these proofs can be (in principle) checked algorithmically. This is the part of the formalistic Hilbert program which survived the negative undecidability and unprovability results of K.Gödel (see e.g., Shoenfield [3]). In this sense, mathematical knowledge about undefinable mathematical phantoms is objective. However, when the actual practice of doing mathematics is considered in its social context, the objectivity of mathematical results may appear more subtle than suggested by this formalistic paradigm - see e.g. De Millo et all [6] or Thurston [7].

Natural numbers, words and hereditarily finite sets are mathematical objects whose objective reality and existence is rooted in structures which envelop them. Of these three kinds of mathematical objects, words are the most easily implemented: in clay, on paper or blackboard, in computer memories as well as in computer keyboards and screens. Maybe it is mostly for this reason, that words are used as names or descriptions of all kinds of finitary mathematical objects.

In particular, words are their own names. Objective reality is objective reality of words.

References

[1] Z.Neubauer: God's Power and Computers' Reason. manuscript.

[2] D.Hilbert, P.Bernays: Grundlagen der Mathematik I. Springer-Verlag, Berlin 1934.

[3] J.R.Shoenfield: Mathematical Logic. Addison-Wesley, 1967.

[4] A.Heyting: Intuitionism: An Introduction. North-Holland, Amsterdam 1971.

[5] A.A.Markov: O logike konstruktivnoj matematiki. Nauka, Moskva 1972.

[6] R.A.De Millo, R.J.Lipton, A.J.Perlis: Social processes and proofs of theorems and programs. in: New directions in the philosophy of mathematics (T. Tymoczko, editor) pp.267-286, Princeton University Press 1998.

[7] W.P.Thurston: On proof and progress in mathematics. in: New directions in the philosophy of mathematics (T. Tymoczko, editor), pp. 337-356, Princeton University Press 1998.