

Ordinals and Sets

– Two Sides of the Same Coin –

Masahiko SATO
Graduate School of Informatics, Kyoto University

Abstract

We introduce a new way of looking at ordinals and sets. Owing to the great success of Zermelo-Fraenkel set theory ZF as a foundational system for describing mathematics, it is now almost taken for granted that the notion of *set* is the most basic notion in mathematics. Indeed, formally speaking, every mathematical object is a set in ZF. In this paper, however, we show that another view of sets is possible. This is done by introducing the notion of *infon*. Intuitively speaking, an infon is a sequence of bits whose length is arbitrary but bounded by an ordinal. Using the notion of infon, which we believe to be more fundamental than that of set, we will show that it is possible to view an infon either as an ordinal or as a set. Thus the totality of infons, so to speak, makes up a coin whose one side consists of ordinals and the other side consists of sets.

1 Introduction

What is a mathematical object? Instead of answering this question directly, modern mathematics provides us with numerous formal systems which we can use to talk about mathematical objects. The characteristic of each formal system is that the system implicitly characterizes the mathematical objects of the system in terms of the axioms of the system. By proving theorems in a formal system, we can establish various relations among mathematical objects, and in this way we can deepen our understanding of mathematical objects. We can also study mathematical objects by metamathematical methods. For example, we can establish the consistency of a formal system either semantically by using model theory or syntactically by using proof theory.

By formalizing the metatheory as well, we see that what we are doing in metamathematics is often simply an *interpretation* of one linguistic system by another. We can also view this as an act of *implementing* the mathematical objects of one system by the mathematical objects of the other. If we can implement one system by another, we may consider that the latter system is more powerful than (or at least as powerful as) the former system, and the latter system is more primitive or concrete than the former. Among various formal systems, ZFC (Zermelo-Fraenkel set theory with the axiom of choice)

is now considered to be the most primitive system for the appropriate reason that virtually all mathematical objects can be implemented as sets. So, from a purely technical point of view, we can answer the very first question we raised at the beginning of this section by saying: ‘A mathematical object is a set.’

In this paper, we will introduce the notion of *infin*¹ and answer the question by saying: ‘A mathematical object is an infon.’ We do this by implementing both ordinals and sets as infons. Intuitively speaking, an infon is a sequence of bits whose length can be transfinite but the length of an infon is always bounded by an ordinal. Therefore, we assume that the notions of ordinal and that of bit are the most basic notions necessary to build up a universe of mathematical objects.

We use ordinals to define infons, and after infons are defined we introduce an important notion of the *length* of an infon. The length of an infon is also an ordinal and we will show how we can well-order all the infons so that infons with shorter length always come before infons with longer length. By using this well-ordering, we will assign a unique ordinal to each infon and will call it the *birthday* of the infon. In this way, we can view an infon as an ordinal by identifying an infon with its birthday.

An infon can also be viewed as a set. Let a be an infon and α be an ordinal. Then we can view a as a set which contains α as its member if and only if the α -th bit of a is 1. Since we already know that each infon can be seen as an ordinal, we can endow a set structure on infons so that each infon is a set whose members are also infons and hence sets.

Another motivation for introducing infons came from our desire to provide a natural framework for doing mathematics formally on a computer (see our [13]). As such a framework should enable us to write formal proofs as naturally as we write proofs informally, we wished to design a formal system in which not only logical reasoning but also computation can be smoothly carried out in it. In order that computation can be done naturally in the system, it is necessary that the system is equipped with basic data structures by which other data structures can be easily implemented in terms of the basic data structures. For such a purpose, we think that infon theory is more adequate than set theory.

In section 2 we introduce infon informally. In section 3 we explain how we can view infons as ordinals, so that we can well-order infons. Infons can also be viewed as sets and we explain this in section 4. After these sections on informal introduction of infons, we give a first-order theory IT (infin theory) which gives an axiomatization of the notion of infon in section 5. The axiomatization is designed so that we can do computation in the formal system more naturally compared to the traditional axiomatization of set theory like ZFC. More precisely, we will introduce the minimization operator μ which can be used to give an explicit name for the smallest infon satisfying a given property. We note that Bourbaki [1] introduced a similar operator τ , but that our μ -operator, which is influenced by Kleene’s μ -operator [9] as well as Hilbert’s ϵ -symbol [7] and Rus-

¹The term ‘infin’ was invented by Keith Devlin in the context of situation theory (see [4, 5]). We borrowed the term here since we think that it is an appropriate name for the entities we introduce in this paper.

sell's ι -term [15], is more concrete than Bourbaki's notation in the sense that our operator is based on the total well-ordering of all the infons. We also show that all the axioms of ZFC are derivable in IT. Section 6 concludes the paper. We have an extra appendix section in which basic properties of IT are listed and proved.

2 Infons

We define infons by assuming that we know ordinals informally. A *bit* is either 0 or 1 and we use each respectively as representing false and true as a boolean value. We will also identify bits with the first two ordinals 0 and 1. Our description of an infon is a generalization of the description of the tape and the head of a Turing machine [14].

Imagine a tape of infinite length, where by infinity we mean absolute infinity which is bigger than any ordinal, and assume that the tape is divided into cells. The tape has the left end but does not have a right end. We assume that each cell of the tape contains a bit, namely, 0 or 1. We also assume that attached with the tape, there is a head which can move and stay at the left end of any cell. In this case we say that the head is looking at the cell just to the right of it, and we say that the cell is the α -th cell of the tape and that the head is at the position α if the cell is the α -th cell counted from the left end. Here we start counting by setting the counter to be 0 initially, so the left most cell becomes the 0-th (not the first) cell of the tape. Given a tape a , we will write a_α for the content of the α -th cell of a . With this notation, a tape a may be informally written as:

$$|_0 a_0 |_1 a_1 |_2 \cdots |_\alpha a_\alpha |_{\alpha+1} \cdots ,$$

where each vertical bar $|_\beta$ designates the left end of the β -th cell of a . We may write a more succinctly as:

$$|a_0|a_1|\cdots|a_\alpha|\cdots ,$$

or even as:

$$a_0a_1\cdots a_\alpha\cdots .$$

Given two bits, they are *equal* if they are both 0 or if they are both 1, and they are *distinct* if one of them is 0 and the other is 1. Given two tapes a and b , they are *equal*, in notation $a = b$, if a_α and b_α are equal bits for all α , and they are *distinct*, in notation $a \neq b$, if a_α and b_α are distinct bits for some α .

We can now define the operation of *cutting a tape at α* as follows. Let a be a tape and α be an ordinal. Then, the result of cutting a at α is a pair of two tapes b and c where b and c are defined as follows. b is the left part of the tape a which is obtained by the cutting appending a blank tape to the right of it. Namely, the content of the β -th cell of b is the same as the content of the β -th cell of a if $\beta < \alpha$ and it is 0 if $\beta \geq \alpha$. b can also be obtained from a by setting the contents of all cells whose positions $\beta \geq \alpha$ to 0. c is the right part of the tape a which is obtained by the cutting. Namely the content of the β -th

cell of c is the content of the $\alpha + \beta$ -th cell of a . We will write $\text{left}(a, \alpha)$ for b and $\text{right}(a, \alpha)$ for c . We say that the cutting of a at α is *safe* if $\text{right}(a, \alpha)$ is 0, namely, if it is a blank tape such that each cell contains 0. We can now define an *infon* as a tape which can be cut safely at some α . We remark that the tape whose cells always contain 1 is not an infon since the tape cannot be cut safely.

With these definitions, we can now define an important notion of the *length* of an infon. Let a be an infon. Then there is an ordinal α for which the cutting of a at α is safe. We define the length of a as the smallest such α and write $|a|$ for it. We will write an infon a of length β informally as:

$$a_0 a_1 \cdots a_\alpha \cdots |_\beta .$$

Moreover, $a_0 a_1 \cdots a_\alpha \cdots |_{\beta+1}$ will also be written as:

$$a_0 a_1 \cdots a_\beta | ,$$

or as:

$$a_0 a_1 \cdots a_\beta$$

where a_β must be 1.

Having defined the length of an infon, we can now define the operation of *appending* an infon b to the right of an infon a , whose result we write $a \hat{=} b$, by stipulating that:

$$(a \hat{=} b)_\gamma \triangleq \begin{cases} a_\gamma & \text{if } \gamma < |a|, \\ b_\beta & \text{if } \gamma = |a| + \beta. \end{cases}$$

It is easy to see that $|a \hat{=} b| = |a| + |b|$. We also see that $(a \hat{=} b) \hat{=} c = a \hat{=} (b \hat{=} c)$.

3 Infons as Ordinals

So far ordinals are used to define infons but they are not infons. In this section we will set up a bijective correspondence between ordinals and infons. This amounts to assign a unique ordinal number to each infon which may be used as the identification number of the infon. We can then simply identify the ID number of an infon with the infon itself, and thereby we may think either an ordinal as an infon or an infon as an ordinal. We must remember, however, that this identification is relative to the bijective correspondence we are going to establish. In the following assignment of ordinals to infons we use sets naively assuming that we can well-order any set.

We define two operations bd and h , where bd will assign a unique ordinal $\text{bd}(a)$ called the *birthday* of a to each infon a and h will assign an ordinal $\text{h}(\alpha)$ called the *height* of α to each ordinal α . The basic idea is to well-order infons according to their lengths so that infons with shorter length will come before infons of longer length.

We first define $\text{h}(\alpha)$ by transfinite induction on α . We need the following two notations for the definition. For each ordinal α , we put $X_\alpha \triangleq \{a \mid |a| = \alpha\}$

and write κ_α for the cardinality of the set X_α . We put $h(0) \triangleq 0$ and for each ordinal $\alpha > 0$ we put:

$$h(\alpha) \triangleq \begin{cases} h(\beta) + \kappa_\beta & \text{if } \alpha = \beta + 1, \\ \sup\{h(\beta) \mid \beta < \alpha\} & \text{if } \alpha \text{ is a limit ordinal,} \end{cases}$$

We can immediately see that $h(\alpha) = 2^{\alpha-1}$ for all finite $\alpha > 0$, $h(\omega) = \omega$ and $h(\alpha) \geq \alpha$ for all α . We will say that an infon is *initial* if it is of the form $1 \cdots |_\alpha$ for some α . We will write $\alpha \uparrow$ for the initial infon $1 \cdots |_\alpha$.

Now, to define $\text{bd}(a)$ for such a that $|a| = \alpha$, we well-order the set X_α so that $1 \cdots |_\alpha$ becomes the least element of X_α and the order-type of the ordering becomes κ_α . It is clear that such a well-ordering is possible. If $a \in X_\alpha$ is the β -th element in X_α with respect to the well-ordering, then we put:

$$\text{bd}(a) \triangleq h(|a|) + \beta.$$

Note that we have $|a| \leq h(|a|) \leq \text{bd}(a)$ so that $|a| \leq \text{bd}(a)$ where $h(|a|) = \text{bd}(a)$ holds iff a is initial.

We thus have a bijective correspondence between infons and ordinals. We will identify an infon a with the ordinal $\text{bd}(a)$ which is the birthday of a . Then, by this identification, we have $\alpha \uparrow = h(\alpha)$, and we can verify that

$$|a| \uparrow \leq a < (|a| + 1) \uparrow$$

and also that if $|a| < |b|$, then $a < b$.

In summary, we can visualize our construction as follows. Let us suppose that each ordinal marks a day on an imaginary time line. We start creating our universe of infons on the 0-th day, and we add exactly one *new* infon on each day. We also assume that there is a cabinet which can contain distinct infons which are well-ordered, and that the cabinet is empty initially. On each day α , we first check if the cabinet is empty or not. If the cabinet is empty, then we well-order all the infons of length $|\alpha|$ so that the order type of the ordering become $\kappa_{|\alpha|}$ and store them in the cabinet keeping the ordering. We then take out the infon $|\alpha| \uparrow$ from the cabinet and make it the infon newly added on the day. If the cabinet is nonempty, then we take out the smallest infon in the cabinet and make it the infon of the day.

4 Infons as Sets

Let a be an infon and β be an ordinal. We say that β is a *member* of a , written $\beta \in a$, if $a_\beta = 1$. Then by the identification we made in the previous section, this definition induces a binary relation on infons. Namely, for infons a and b , we have $b \in a$ if and only if $a_{\text{bd}(b)} = 1$. By the membership relation on infons, we can regard any infon a as a set whose members are exactly those infons b such that $a_b = 1$. In this view, equality of infons can be characterized extensionally since we have:

$$(\forall x. x \in a \Leftrightarrow x \in b) \Rightarrow a = b.$$

Suppose that $b \in a$, that is, $a_b = 1$. Then we have $b < a$ since $b < |a| \leq a$.

With each infon a we can associate a ZFC set $S(a)$ as follows.

$$S(a) \triangleq \{S(b) \mid a_b = 1\}.$$

It is easy to see that $S(a) = S(b)$ iff $a = b$ and that any ZFC set A can be written as $S(a)$ for some infon a by inductive argument on the rank of A . We have moreover $b \in a$ iff $S(b) \in S(a)$ where the latter membership relation is the membership relation on ZFC sets. In this way, we can view any infon as a ZFC set and vice versa.

We have thus established two distinct views of infons as sets. The first one is an *internal* view which is obtained by defining the membership relation as an internal relation on infons. In this view, we can *define* the notion of set within the theory of infons. The second one is an *external* view which identifies an infon a with an external ZFC set $S(a)$.

We remark that, as a set, the infon $\alpha \uparrow$ consists of ordinals $< \alpha$ since we have $\beta \in \alpha \uparrow$ iff $\beta < \alpha$ for all β .

We list below the first 9 infons together with their birthdays and their views as sets. It should be noted that, according to the ordering method of infons described in section 3, infons introduced on days 5, 6, 7 can be any permutation of 3 infons, 011000..., 001000... and 101000.... So, the list below is just one of 6 possible lists of the first 9 infons.

birthday	infon	set
0	000000...	$\{\}$
1	100000...	$\{0\}$
2	110000...	$\{0, 1\}$
3	010000...	$\{1\}$
4	111000...	$\{0, 1, 2\}$
5	011000...	$\{1, 2\}$
6	001000...	$\{2\}$
7	101000...	$\{0, 2\}$
8	111100...	$\{0, 1, 2, 3\}$

5 Infon Theory

We define *Infon Theory*, IT, as a first-order theory. Unlike ordinary first-order theories, IT has neither *implication* nor *negation* as its primitive logical connectives. Instead, these connectives will be introduced as abbreviations. Also in IT, formulas are defined as special terms whose values are either 0 or 1.

We define *terms* and *formulas* inductively as follows. We have two sorts of variables for constructing terms and variables. They are *object variables* and *proposition variables*. We will use Latin letters x, y, z for object variables and p, q, r for proposition variables. Other Latin letters and Greek letters are used as metavariables ranging over terms. When we use a Greek letter our intention

is to view the infon designated by the term as an ordinal. Similarly we use capital Latin letters A, B etc. for sets. We use sans serif Latin letters P, Q etc. as metavariables for formulas, and v as a metavariable ranging over both object variables and proposition variables.

Terms are defined as follows.

1. An object variable is a term.
2. A formula is a term.
3. If α and β are terms, then $\alpha + \beta$ is a term.
4. If x is an object variable and $P(x)$ is a formula, then $\mu x[P(x)]$ is a term.

As a term, a formula denotes 1 (0) if it is true (false, resp.). The term $\mu x[P(x)]$ stands for the smallest ordinal a for which $P(a)$ holds when $\exists x. P(x)$ is true. The term denotes 0 when $\exists x. P(x)$ is false.

Formulas are defined as follows.

1. If p is a proposition variable, then p and \bar{p} are formulas.
2. If a and A are terms, then $a \in A$ and $a \notin A$ are formulas.
3. If P and Q are formulas, then so are $P \wedge Q$ and $P \vee Q$.
4. If v is an object variable or a proposition variable and $P(v)$ is a formula, then $\forall v. P(v)$ and $\exists v. P(v)$ are formulas.

The formula $\alpha \in A$ ($\alpha \notin A$) means that the content of the α -th cell of A is 1 (0, resp.). We remark that \in and \notin are two distinct binary predicate symbols.

With each formula P we associate its *antiformula* P^- as follows.

1. $p^- \triangleq \bar{p}$ and $(\bar{p})^- \triangleq p$.
2. $(a \in A)^- \triangleq a \notin A$ and $(a \notin A)^- \triangleq a \in A$.
3. $(P \wedge Q)^- \triangleq P^- \vee Q^-$ and $(P \vee Q)^- \triangleq P^- \wedge Q^-$.
4. $(\forall v. P(v))^- \triangleq \exists v. (P(v))^-$ and $(\exists v. P(v))^- \triangleq \forall v. (P(v))^-$.

For a closed formula P , we will have P is true iff P^- is false and P is false iff P^- is true. We also see that $(P^-)^-$ is P . In order to stress that P and P^- are antiformulas with each other, we sometimes write P^+ for P .

We introduce some notational conventions.

$$\begin{aligned} P \Rightarrow Q &\triangleq P^- \vee Q^+ \\ P \Leftrightarrow Q &\triangleq (P \Rightarrow Q) \wedge (Q \Rightarrow P) \\ 0 &\triangleq \forall p. p \\ 1 &\triangleq \exists p. p \end{aligned}$$

$$\begin{aligned}
\neg P &\triangleq P \Rightarrow 0 \\
a = b &\triangleq \forall x. x \in a \Leftrightarrow x \in b \\
a \neq b &\triangleq \exists x. x \in a \Leftrightarrow x \notin b \\
A \subseteq B &\triangleq \forall x. x \in A \Rightarrow x \in B
\end{aligned}$$

We assume, as usual, that the binding power of \forall and \exists are weaker than those of \Rightarrow and \Leftrightarrow and that those of \Rightarrow and \Leftrightarrow are weaker than those of \wedge and \vee .

We assume standard natural deduction style inference rules for the *minimal logic* including those for implication. Namely, we have introduction and elimination rules for the logical constants: \Rightarrow , \wedge , \vee , \forall and \exists (see e.g. Prawitz [11]).

There are two points we wish to remark here concerning our logical system. One is that we have two kinds of variables ranging over two distinct domains. The other is about the inference rules for equality.

The *object variables* range over infons, and the *proposition variables* range over truth values 0 and 1 which are the first two infons, namely, the 0th and the 1st infons. Reflecting this, we have the following rules for the universal and existential quantifications over proposition variables with the usual eigen variable conditions.

$$\begin{array}{cccc}
\frac{P(q)}{\forall q. P(q)} & \frac{\forall q. P(q)}{P(Q)} & \frac{P(Q)}{\exists q. P(q)} & \frac{\begin{array}{c} P(q)^1 \\ \vdots \\ R \end{array}}{\exists q. P(q)} \\
& & & 1
\end{array}$$

As for equality, we have the following rules of replacement.

$$\frac{P(a) \quad a = b}{P(b)} \quad \frac{R(P) \quad P = Q}{R(Q)}$$

Note that the following rule is an instance of the replacement rules.

$$\frac{P \quad P = Q}{Q}$$

We also note that we do not have to postulate reflexivity, symmetry and transitivity of the equality relation as axioms as they are all provable only by using logical inference rules.

We also have the following two rules of equality which enable us to compute *truth values* of formulas within the system.

$$\frac{P^+}{P = 1} \quad \frac{P^-}{P = 0}$$

These are all the inference rules of IT.

Before we list the axioms of IT we give some useful theorem schemata which we can obtain by using only logical inference rules. We can prove 1 as follows.

$$\frac{\frac{0^1}{0 \Rightarrow 0}}{\exists p. p} 1$$

We can then see that $1 = 0$ implies contradiction, namely, 0:

$$\frac{\frac{\vdots}{1} \quad 1 = 0^1}{0} \quad (1 = 0) \Rightarrow 0 \quad 1$$

The formula 0, that is $\forall p. p$, is indeed a contradiction since we may infer any formula from 0 by simply applying the \forall -elimination rule:

$$\frac{0}{P}$$

We have

$$P^+ \vee P^-$$

since this formula is $P^- \Rightarrow P^-$ which is provable by the \Rightarrow introduction rule.

We can now see

$$\neg P \Leftrightarrow P^-$$

as follows. The direction \Leftarrow is obvious since $\neg P$ is an abbreviation of $P^- \vee 0$. The other direction is also easy since we can infer P^- from 0. By this theorem, we have the *law of the excluded middle*: $P \vee \neg P$.

We can also prove the following theorems:

$$\begin{aligned} P &\Leftrightarrow P = 1 \\ P = 1 &\Leftrightarrow P^- = 0 \\ P^- = 0 &\Leftrightarrow \neg P^- \\ \neg P^- &\Leftrightarrow \neg\neg P \\ P &\Leftrightarrow \neg\neg P \\ \neg P &\Leftrightarrow P = 0 \\ (P \Leftrightarrow Q) &\Leftrightarrow P = Q \\ \exists p. P(p) &\Leftrightarrow P(0) \vee P(1) \\ \forall p. P(p) &\Leftrightarrow P(0) \wedge P(1) \\ a \neq b &\Leftrightarrow \neg(a = b) \end{aligned}$$

as well as all the theorems of classical second order propositional logic which include all the inhabited types (regarded as IT formulas) of Girard's system F [6]. From the above theorems we see that for any formula P , P is a theorem iff

$\neg P^-$ is a theorem. For example, since $P^+ \vee P^-$ is a theorem, we have another theorem $\neg(P^- \wedge P^+)$.

We add some more notational conventions before we list the axioms of IT. We remark that the last 6 conventions below all introduce abbreviations for terms of the form $\mu z[Q(z)]$ and they will stand for the minimum z with the property $Q(z)$ if $\exists z. Q(z)$ but they will stand for 0 if $\exists z. Q(z)$ does not hold.

$$\begin{aligned}
\alpha \leq \beta &\triangleq \exists x. \alpha + x = \beta \\
\alpha < \beta &\triangleq \alpha \leq \beta \wedge \alpha \neq \beta \\
\forall x \in A. P(x) &\triangleq \forall x. x \in A \Rightarrow P(x) \\
\omega &\triangleq \mu z[0 < z \wedge \forall x. x < z \Rightarrow x + 1 < z] \\
\{x \mid P(x)\} &\triangleq \mu z[\forall x. x \in z \Leftrightarrow P(x)] \\
\{x \in A \mid P(x)\} &\triangleq \{x \mid x \in A \wedge P(x)\} \\
\{f(x) \mid P(x)\} &\triangleq \{y \mid \exists x. y = f(x) \wedge P(x)\} \\
|A| &\triangleq \mu z[\forall x. x \in A \Rightarrow x < z] \\
\alpha \uparrow &\triangleq \{x \mid x < \alpha\}.
\end{aligned}$$

As for axioms and axiom schemata of IT, we have the followings. Correctness of these axioms with respect to the meaning of infons we gave in sections 2 – 4 is easy to verify and we omit the verification here. Since the arguments in sections 2 – 4 can be carried out within ZFC, it follows that IT is consistent relative to ZFC. We will show later in this section that all the axioms of ZFC are derivable in IT. Hence, we will see that ZFC and IT are equiconsistent.

1. $\alpha + \beta = \alpha \Leftrightarrow \beta = 0$.
2. $\beta \neq 0 \Rightarrow \alpha + \beta = |\{\alpha + x \mid x < \beta\}|$.
3. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
4. $\alpha < \beta \vee \alpha = \beta \vee \beta < \alpha$.
5. $\neg(\alpha < \beta \wedge \beta < \alpha + 1)$.
6. $|a| \uparrow \leq a \wedge a < (|a| + 1) \uparrow$.
7. $0 < \omega \wedge (\alpha < \omega \Rightarrow \alpha + 1 < \omega)$.
8. $a \in b \Rightarrow a < b$.
9. $P(a) \Rightarrow P(\mu x[P(x)]) \wedge \mu x[P(x)] \leq a$.
10. $(\forall x. \neg P(x)) \Rightarrow \mu x[P(x)] = 0$.
11. $(\forall x \in a. \exists y. P(x, y)) \Rightarrow \exists z. \forall x \in a. \mu y[P(x, y)] \leq z$.

12. $(\exists z. \forall x. P(x) \Rightarrow x \leq z) \Rightarrow (\exists y. \forall x. x \in y \Leftrightarrow P(x))$.

Axioms 1 – 3 characterizes the addition of infons as ordinals.

Axiom 4 says that the ordering of infons is a total order. Axiom 5 says that there is no infon between an infon α and its successor $\alpha + 1$. Axiom 6 says that any infon of length α is greater than or equal to $\alpha \uparrow$ and strictly less than $(\alpha + 1) \uparrow$.

Axiom 7 characterizes ω as the smallest infon larger than any *finite* infons, where finite infons are obtained from 0 by applying the successor operation finitely many times.

Axiom 8 says that all the elements of a set are created before the set is created.

Axioms 9 and 10 characterize the meaning of the μ -operator. Axiom 9 is also an axiom schema of transfinite induction on ordinals.

Axiom 11 together with Axiom 12 enables us to define a set by replacement. Axiom 12 says that if there is an upper bound for objects satisfying a given property, then the collection of objects satisfying the property forms a set. We can prove the converse of Axiom 12 by using Axiom 8. So, Axiom 12 together with its converse gives us a useful criterion by which we can decide if the collection of objects satisfying a given property forms a set. We will see that this axiom can be used to form big sets like power sets from smaller sets.

As we remarked above, the converse of Axiom 12 holds and so we have the following theorem in IT:

$$(\forall z. \exists x. P(x) \wedge z < x) \Rightarrow \neg(\exists y. \forall x. x \in y \Leftrightarrow P(x))$$

We can use this theorem to show that the collection of objects satisfying a given property does not form a set. For example, consider the property $P(a) \triangleq a \notin a$ which Russell used to derive his paradox. Then by the above theorem we can conclude that there is no set A such that $a \in A$ if and only if $a \notin a$ since $a \notin a$ holds for any infon a . We note that $a \in A$ means that the a -th cell of infon A contains 1, but, on the other hand, there is a tape t such that $t_a = 1$ holds for all ordinals a . However, the tape t is *not* an infon since we cannot cut t safely. In general, for any property $P(a)$, we have a unique tape t such the a -th cell of t contains 1 if and only if $P(a)$ holds. Then, the proposition $\exists z. \forall x. P(x) \Rightarrow x \leq z$ is equivalent to the fact that the tape t can be cut safely at some α . We can thus see that Axiom 12 is a natural formalization of our informal definition of an infon as a tape which can be cut safely.

We now verify that all the axioms of ZFC (see [2]) are derivable in IT. The *Axiom of Extensionality* easily follows from our definition of $a = b$ as an abbreviation of $\forall x. x \in a \Leftrightarrow x \in b$. As we will prove $a \notin 0$ in the Appendix section, the *Axiom of the Null Set* follows from this fact. To prove the *Axiom of Unordered Pairs*, let a and b be infons and consider the infon:

$$\{a, b\} \triangleq \{x \mid x = a \vee x = b\}.$$

This is the desired set since by Axiom 4 we have $a < b \vee a = b \vee b < a$ and in any of three possible cases we can find a z which is \geq both a and b . To verify

the *Axiom of the Sum Set*, we define the *sum set* of A by:

$$\cup A \triangleq \{x \mid \exists y. y \in A \wedge x \in y\}.$$

Let a be an infon and suppose that $\exists y. y \in A \wedge a \in y$. Then we have $a \in b$ for some $b \in A$ and this means that $a < A$ which verifies the axiom.

The *Axiom of Infinity* follows from Axiom 7, and the *Axiom of Replacement* follows from Axioms 11 and 12.

Given a set A we define its power set by:

$$\mathcal{P}(A) \triangleq \{x \mid x \subseteq A\}.$$

To see that this set satisfies the *Axiom of the Power Set*, suppose that $B \subseteq A$. Then we have $|B| \leq |A|$, and by Axiom 6, we have $B < (|B| + 1) \uparrow \leq (|A| + 1) \uparrow$.

To prove the *Axiom of Choice*, let A be a set and suppose that $\exists x. x \in F(\alpha)$ holds for any $\alpha \in A$. Then by putting:

$$f(\alpha) \triangleq \mu x[x \in F(\alpha)] \quad (\alpha \in A),$$

we obtain the desired choice function f . To see the *Axiom of Regularity* (also known as the *Axiom of Foundation* [10]), let A be a nonempty set and consider the infon $a \triangleq \mu x[x \in A]$. Then a is the smallest element of A , and hence no member of a can be a member of A since $b \in a$ implies $b < a$. We have thus verified all the axioms of ZFC.

We now wish to define the notion of *cardinality* in IT. To this end we prepare some more notational conventions.

$$\begin{aligned} \langle a, b \rangle &\triangleq \{\{a\}, \{a, b\}\} \\ \text{Pair}(c) &\triangleq \exists x. \exists y. c = \langle x, y \rangle \\ \pi_1(c) &\triangleq \mu z[\exists y. c = \langle z, y \rangle] \\ \pi_2(c) &\triangleq \mu z[\exists x. c = \langle x, z \rangle] \\ \text{Fun}(f) &\triangleq (\forall z \in f. \text{Pair}(z)) \wedge \forall x \in f. \forall y \in f. \pi_1(x) = \pi_1(y) \Rightarrow \pi_2(x) = \pi_2(y) \\ \text{dom}(f) &\triangleq \{\pi_1(z) \mid z \in f\} \\ \text{ran}(f) &\triangleq \{\pi_2(z) \mid z \in f\} \\ f : A \rightarrow B &\triangleq \text{Fun}(f) \wedge \text{dom}(f) = A \wedge \text{ran}(f) \subseteq B \\ f : A \xrightarrow{1-1} B &\triangleq f : A \rightarrow B \wedge \forall x \in f. \forall y \in f. \pi_1(x) \neq \pi_1(y) \Rightarrow \pi_2(x) \neq \pi_2(y) \\ f : A \xrightarrow{\text{onto}} B &\triangleq f : A \rightarrow B \wedge \text{ran}(f) = B \\ f : A \xrightarrow{\text{bij}} B &\triangleq f : A \xrightarrow{1-1} B \wedge f : A \xrightarrow{\text{onto}} B \\ A \approx B &\triangleq \exists x. x : A \xrightarrow{\text{bij}} B \\ \text{card}(A) &\triangleq \mu z[z \approx A] \end{aligned}$$

In the above, we defined the ordered pair $\langle a, b \rangle$ of two infons a and b by using the standard encoding. Using μ -operator, we can explicitly define the projection operators π_i ($i = 1, 2$) which retrieves the i -th component of a pair. We then defined the notions of a *function*, the *domain* of a function, the *range* of a function and a *bijective function* succinctly using the projection operators. $A \approx B$ means that there is a bijection from A to B , namely, A and B are *equipotent*. Finally $\text{card}(A)$ picks the smallest set from all the sets which are equipotent with A , and we call it the *cardinality* of A . The idea behind our definition of cardinality is the same as that of Bourbaki [1] who uses τ -term.

We conclude this section by noting that we can obtain *Finite Infon Theory*, FIT, simply by replacing the Axiom 7, which asserts the existence of an infinite ordinal, with the following axiom of mathematical induction:

$$P(0) \wedge (\forall x. P(x) \Rightarrow P(x + 1)) \Rightarrow \forall x. P(x).$$

The intended objects of FIT are precisely *finite infons*, namely infons of finite length. As ordinals they are exactly finite ordinals and as sets they are hereditarily finite sets, that is, finite sets all of whose members are hereditarily finite.

6 Conclusion

We must admit that ZFC is a well-designed system in which virtually all of mathematics can be developed. However, if one observes that the notions of natural number, sequence etc. were introduced into mathematics long before the notion of set came to be introduced, then it seems worthwhile to look for an alternative foundational system not based on sets but based on some other more basic and concrete notions. In this paper, we took the notions of ordinal and sequence as such notions, and defined an infon as a transfinite sequence of bits whose length is bounded by an ordinal. We then showed that an infon can be viewed either as an ordinal or as a set.

We can also observe that finite infons, which are simply sequences of bits of finite length, are everywhere in the information society. Two noteworthy examples are internet packets and DNA sequences. We thus see that finite infons are used, as Turing did, to encode finite information, and we believe that it is a natural idea to use transfinite infons to encode transfinite information.

We also emphasized the transfinitary computational treatment of infons as a kind of extension of Turing machines. This is clearly reflected in our choice of atomic formulas, and in IT we have only two kinds of atomic formulas. The first kind atomic formulas are proposition variables p and their antiformalas \bar{p} . The second are formulas of the form $\alpha \in a$ meaning that the content of the α -th cell of a is 1 and formulas of the form $\alpha \notin a$ meaning that the content of the α -th cell of a is 0. Since p ($\alpha \in a$) and \bar{p} ($\alpha \notin a$, resp.) are antiformalas with each other, with each IT formula we could assign its antiformala. In this way we could build up all the formulas without using negation or implication, so that we can interpret all the formulas *positively*. That is, instead of saying that a formula P does *not* hold, we can say that P^- holds.

The term $\mu z[P(z)]$ may be considered as a transfinite generalization of Kleene's μ -operator or as a strong form of Hilbert's ε -symbol. We saw that thanks to the μ -operator we could name sets like ω explicitly within IT whereas in ZFC ω can be introduced only in the meta language.

In section 5 we saw that IT and ZFC are equiconsistent and this means that these two systems have the same power of developing mathematics in them. However, as we have just pointed out above, we think that IT is easier to work directly in it than to do so in ZFC.

IT is a foundational system, just like ZFC, and as such we must accept it directly without appealing to another system. In this respect, our approach is the same as that of Conway [3] who developed a theory of numbers and games using ordinals as fundamental mathematical objects.

Although IT is easier to work within compared to ZFC, it is still inadequate as a basic system for implementing mathematics in it. The reason is that, in modern mathematics, we are mostly concerned with properties of mathematical objects and it is desirable to have a system which can hide implementation details of objects and make them invisible to the users (that is, mathematicians) who use the objects. For example, in IT we implemented the ordered pair $\langle a, b \rangle$ as a set $\{\{a\}, \{a, b\}\}$, but what is needed is that an ordered pair should behave as expected and how it is implemented is not important. We are planning to use IT as a low level language to implement such a higher level language which uses the above mentioned abstract definition of mathematical objects and can be used as a basis for the Natural Framework (NF) [12, 13] for developing mathematical proofs formally on a computer.

The idea and motivation for our design of Natural Framework is similar to Kahn's idea of Natural Semantics [8], but NF put more emphasis on logic than on computation. We hope that we would be able to make logic and computation closer by extending traditional computation which is inherently finitary to transfinite computation on infs.

Appendix: Basic Properties

We establish basic properties of IT in this section.

- $\alpha \leq \alpha$.

Immediate by Axiom 1.

- $\alpha \leq \beta \wedge \beta \leq \gamma \Rightarrow \alpha \leq \gamma$.

Immediate by Axiom 3.

- $\alpha \leq \beta \wedge \beta \leq \alpha \Rightarrow \alpha = \beta$.

Immediate by Axioms 1 and 3.

- $\alpha \leq \beta \Leftrightarrow \alpha < \beta \vee \alpha = \beta$.

To prove \Rightarrow , suppose that $\alpha \leq \beta$. If $\alpha = \beta$, then we are done, and if not, then we have $\alpha < \beta$. To prove \Leftarrow , suppose that $\alpha < \beta \vee \alpha = \beta$. In the first case we have $\alpha \leq \beta$. In the second case we have $\alpha + 0 = \alpha = \beta$. Hence we have $\alpha \leq \beta$.

- $(\forall x. x < \alpha \Rightarrow x < \beta) \Rightarrow \alpha \leq \beta$.

Suppose that $\forall x. x < \alpha \Rightarrow x < \beta$ and $\neg(\alpha \leq \beta)$. Then by Axiom 4 we have $\beta < \alpha$. This implies $\beta < \beta$ which is a contradiction.

- $\alpha \neq 0 \Rightarrow \alpha = |\{x \mid x < \alpha\}|$.

Let us write γ for $|\{x \mid x < \alpha\}|$. Then we have $\forall x. x < \alpha \Rightarrow x < \gamma$ so that we have $\alpha \leq \gamma$. On the other hand, since $\forall x. x < \alpha \Rightarrow x < \alpha$, we have $\gamma \leq \alpha$. Hence $\alpha = \gamma$.

- $0 + \alpha = \alpha$.

Suppose otherwise, and let α be the smallest ordinal such that $0 + \alpha \neq \alpha$. By 1 we see that α is nonempty and can be written as $\alpha = |\{x \mid x < \alpha\}|$, so that by 2 we have $0 + \alpha = |\{0 + x \mid x < \alpha\}| = |\{x \mid x < \alpha\}| = \alpha$. This is a contradiction.

- $0 \leq \alpha$.

Immediate from the above theorem.

- $\neg(\alpha < 0)$.

Suppose that $\alpha < 0$. Then by the above theorem, we have $\alpha < \alpha$ which is a contradiction.

- $\alpha \neq 0 \Leftrightarrow 0 < \alpha$.

Suppose that $\alpha \neq 0$. Then we have $0 < \alpha$ since $0 + \alpha = \alpha$. Next, suppose that $0 < \alpha$ and moreover $\alpha = 0$. Then we have $0 < 0$ which is a contradiction.

- $\alpha < 1 \Rightarrow \alpha = 0$.

Suppose that $\alpha < 1$ and suppose moreover that $\alpha \neq 0$. Then, by the previous theorem, we have $0 < \alpha < 1 = 0 + 1$ contradicting Axiom 5.

- $\alpha < \beta \Leftrightarrow \alpha + 1 \leq \beta$.

Suppose that $\alpha < \beta$. Then $\alpha + x = \beta$ for some $x \neq 0$, that is, $1 \leq x$. So, we have $x = 1 + y$ for some y . Hence $(\alpha + 1) + y = \beta$, that is, $\alpha + 1 \leq \beta$. Next, suppose that $\alpha + 1 \leq \beta$. Then we have $\alpha + (1 + x) = \beta$ for some x . Now, if $\alpha = \beta$, then we have $0 = 1 + x \geq 1 > 0$, which is a contradiction.

- $\alpha + \beta = 0 \Rightarrow \alpha = 0 \wedge \beta = 0$.

We first prove $\alpha + \beta = 0 \Rightarrow \beta = 0$ by showing its contraposition: $\beta \neq 0 \Rightarrow \alpha + \beta \neq 0$. Suppose that $\beta \neq 0$. Then we have $\alpha < \alpha + \beta$. Since $0 \leq \alpha$, we have $0 < \alpha + \beta$, that is, $\alpha + \beta \neq 0$. We have thus seen that $\beta = 0$. Then, $\alpha = \alpha + \beta = 0$.

- $\beta < \gamma \Rightarrow \alpha + \beta < \alpha + \gamma$.

Suppose that $\beta < \gamma$. Then we have $\gamma = \beta + x$ for some $x \neq 0$. Hence $\alpha + \gamma = \alpha + (\beta + x) = (\alpha + \beta) + x$, that is, $\alpha + \beta < \alpha + \gamma$.

- $\alpha + \beta = \alpha + \gamma \Rightarrow \beta = \gamma$.

This follows from the above theorem by using Axiom 4.

- $a \in A \Rightarrow a < |A|$.

Suppose that $a \in A$. By Axiom 8 we have $\forall x. x \in A \Rightarrow x < A$. This means that $\exists z. \forall x. x \in A \Rightarrow x < z$. So, by Axiom 9, we have $a < |A|$.

- $|A| \leq A$.

We have $\exists z. \forall x. x \in A \Rightarrow x < z$ as in the previous theorem. So, by Axiom 9, we have $|A| \leq A$.

- $|0| = 0$.

By Axiom 6 we have $|0| \leq 0$, so that we have $|0| = 0$ since $0 < 0$ is impossible.

- $|a| = 0 \Leftrightarrow a = 0$.

Suppose that $a \neq 0$. Then we have some x such that $x \in a$. Hence $0 \leq x < |a|$. This proves \Rightarrow -part of the theorem. The \Leftarrow -part follows from the previous theorem.

- $a \notin 0$.

Suppose that $a \in 0$. Then we have $a < |0| = 0$, which is a contradiction.

- $a = 0 \Leftrightarrow \forall x. x \notin a$

Immediate by the definition of $=$ and by the previous theorem.

- $|a| < |b| \Rightarrow a < b$.

Suppose that $|a| < |b|$. Then we have $|a| + 1 \leq |b|$, so that $(|a| + 1) \uparrow \leq |b| \uparrow$. On the other hand, by Axiom 6 we have $a < (|a| + 1) \uparrow \leq |b| \uparrow \leq b$. This implies $a < b$.

- $a \in 1 \Leftrightarrow a = 0$.

Suppose that $a \in 1$. Then by Axiom 8 we have $a < 0$, and this implies $a = 0$. Now, we see that 1 is a nonempty set since $1 \neq 0$. Hence we have some x such that $x \in 1$, but this x must be 0 by the above argument. This proves the \Leftarrow -part of the theorem.

We need some more notational conventions to continue our list of theorems.

$$\begin{aligned}\alpha - \beta &\triangleq \mu z[\alpha = \beta + z]. \\ a_\alpha &\triangleq \alpha \in a. \\ a \hat{\wedge} b &\triangleq \mu z[\forall \alpha. (\alpha < |a| \Rightarrow z_\alpha = a_\alpha) \wedge (z_{|a|+\alpha} = b_\alpha)].\end{aligned}$$

We can prove the following properties whose proofs we omit.

- $\beta \leq \alpha \Rightarrow \alpha = \beta + (\alpha - \beta)$.
- $\alpha < |A| \Rightarrow \exists x. \alpha \leq x \wedge x < |A| \wedge x \in A$.
- $(\alpha < |a| \Rightarrow (a \hat{\wedge} b)_\alpha = a_\alpha) \wedge ((a \hat{\wedge} b)_{|a|+\alpha} = b_\alpha)$.
- $|a \hat{\wedge} b| = |a| + |b|$.
- $|\alpha \uparrow| = \alpha$.
- $\exists x. P(x) \Leftrightarrow P(0) \vee \mu x[P(x)] \neq 0$.
- $\forall x. P(x) \Leftrightarrow P(0) \wedge \mu x[\neg P(x)] = 0$.

References

- [1] Nicolas Bourbaki, *Elements of Mathematics, Theory of Sets*, Hermann and Addison-Wesley, 1968.
- [2] Paul J. Cohen, *Set Theory and the Continuum Hypothesis*, Benjamin, 1966.
- [3] John Horton Conway, *On Numbers and Games*, second edition, A K Peters, 2000.
- [4] Keith Devlin, *Logic and Information*, Cambridge University Press, 1991.
- [5] Keith Devlin, Jon Barwise's papers on natural language semantics, *Bull. Symbolic Logic*, **10**, pp. 54 – 85, 2004.
- [6] Jean-Yves Girard, Paul Taylor and Yves Lafont, *Proofs and Types*, Cambridge University Press, 1989.
- [7] David Hilbert and Paul Bernays, *Grundlagen der Mathematik*, vol. **1**, Springer, 1934.
- [8] Gilles Kahn, Natural Semantics, *STACS 87*, Lecture Notes in Computer Science **247**, pp. 22 – 39, 1987.

- [9] Stephen C. Kleene, General recursive functions of natural numbers, *Math. Ann.*, **112**, pp. 727 – 742, 1936.
- [10] Kenneth Kunen, *Set Theory – An Introduction to Independence Proofs*, North-Holland, 1980.
- [11] Dag Prawitz, *Natural Deduction*, Dover, 2006.
- [12] Masahiko Sato, Theory of judgments and derivations, in Arikawa, S. and Shinohara, A. eds., *Progress in Discovery Science*, Lecture Notes in Artificial Intelligence **2281**, pp. 78 – 122, Springer, 2002.
- [13] Masahiko Sato, A framework for checking proofs naturally, *Int. J. of Intelligent Information Systems*, to appear.
- [14] Alan M. Turing, On Computable Numbers, with an Application to the Entscheidungsproblem, *Proc. London Math. Soc.*, **42**, pp. 230 – 265, 1937.
- [15] Alfred North Whitehead and Bertrand Russell, *Principia mathematica*, vol. **1**, Cambridge University Press, 1910.