Notre Dame Journal of Formal Logic
Volume VIII, Number 4, October 1967

AN ELEMENTARY CONSTRUCTION OF THE NATURAL NUMBERS

FRANCIS J. TYTUS

I. *Introduction* This paper presents a set-theoretic construction of the natural numbers which employs, besides standard set-theoretic operations, only The Axiom of Choice and the existence of an infinite set.

The following notation will be used. A set of sets will be called a *family*. Set-theoretic inclusion will be represented by $\subseteq$, and strict inclusion by $\subset$. The power-set of a set S will be represented by $\mathsf{P}(S)$. If f is a function defined on a set S, then $f(T)$ will represent the set of images under f of the elements of T, for each subset T of S. In particular $f(\phi) = \phi$, where ϕ is the void set. If $\mathcal{J}$ is a family of subsets of a set S, then $\bigcap \mathcal{J}$ will represent the intersection of the members of $\mathcal{J}$. In particular, $\bigcap \phi = \phi$. The difference of sets S and T will be represented by $S \backslash T$.

The following definitions would be used. The pair $<S,g>$, where S is a set and g is a function on S, is called a *Peano System* if the following three conditions are satisfied:

(i) g is one-to-one,
(ii) g does not map S into S,
(iii) If T is a subset of S such that
$T \cap [S \backslash g(S)] \neq \phi$ and $g(T) \subseteq T$, then $T = S$.

We wish to construct a Peano System.

A *choice function* on a set S is a function which assigns to each non-void subset T of S an element of T. The *Axiom of Choice* states that a choice function may be defined on any set.

A set S will be called *finite* if and only if every one-to-one mapping in S maps S onto S. S will be called *infinite* if it is not finite. The following propositions give some properties of finite sets which will be used in the sequel.

Proposition 1: *If S is a finite set and T is a subset of S, then T is finite.*

Proof: If f is a one-to-one function in T, then the mapping g in S defined by:

Received October 12, 1966

$$g(x) = \begin{cases} f(x), & x \text{ in } T, \\ x, & x \text{ in } S\backslash T, \end{cases}$$

is one-to-one, and hence maps S onto S. Clearly $f(T) = g(T) = T$. Q.E.D.

Proposition 2: *If S and T are sets of the same cardinality, and S is finite, then T is finite.*

Proof: Let f be a one-to-one function from S onto T. If h is a one-to-one function in T, then the composite function $f^{-1} \circ h \circ f$ is a one-to-one mapping in S, so we have $(f^{-1} \circ h \circ f)(S) = S$. Consequently:

$$\begin{aligned} h(T) &= h(f(S)) \\ &= (f \circ f^{-1} \circ h \circ f)(S) \\ &= f[(f^{-1} \circ \mathrm{h} \circ f)(S)] \\ &= f(S) \\ &= T. \end{aligned}$$

Q.E.D.

Proposition 3: *If T is a finite subset of a set S, and x is in $S\backslash T$, then $T \cup \{x\}$ is finite.*

Proof: Let $U = T \cup \{x\}$, and suppose that f is a one-to-one mapping from U into U. We wish to show that y is in the range of f, where y is an arbitrary element of U. Clearly $U\backslash\{y\}$ has the same cardinality as T, and hence is finite. If y is not in $f(U\backslash\{y\})$, then $f(U\backslash\{y\}) \subseteq U\backslash\{y\}$, and the restriction of f to $U\backslash\{y\}$ is a one-to-one mapping in $U\backslash\{y\}$. Consequently we have $f(U\backslash\{y\}) = U\backslash\{y\}$, since $U\backslash\{y\}$ is finite, and we must have $f(y) = y$, because f is one-to-one. Q.E.D.

II. *Construction of a Peano System* For an arbitrary set S, let f be a choice function on S, by the Axiom of Choice, and let g be the function on $\mathsf{P}(S)$ defined by:

$$g(T) = \begin{cases} T\backslash\{f(T)\}, & T \neq \phi, \\ \phi, & T = \phi. \end{cases}$$

Now let Γ be the family of all sub-families $\mathscr{A}$ of $\mathsf{P}(S)$ such that S is in $\mathscr{A}$ and $g(\mathscr{A}) \subseteq \mathscr{A}$. $\mathsf{P}(S)$ is in Γ, so Γ is non-void. Finally, let $\mathscr{V} = \bigcap \Gamma$. It is clear that $\mathscr{V}$ is in Γ, and that if $\mathscr{A}$ is a sub-family of $\mathscr{V}$ which is also in Γ, then $\mathscr{A} = \mathscr{V}$.

We wish to show that when S is infinite the pair $<\mathscr{V}, g|\mathscr{V}>$ is a Peano System, where $g|\mathscr{V}$ is the restriction of g to $\mathscr{V}$. First of all we note that if $S = \phi$, then S is in $\mathscr{V}\backslash g(\mathscr{V})$, and $<\mathscr{V}, g|\mathscr{V}>$ satisfies condition (ii) of the definition of a Peano System.

Proposition 4: $\mathscr{V} = \{S\} \cup g(\mathscr{V})$.

Proof: Let $\mathscr{A} = \{S\} \cup g(\mathscr{V})$. Clearly $\mathscr{A}$ is both a subset of $\mathscr{V}$ and a member of Γ, so $\mathscr{A} = \mathscr{V}$. Q.E.D.

It follows from Proposition 4 that $<\mathscr{V}, g|\mathscr{V}>$ satisfies condition (iii) of the definition of a Peano System: if $\mathscr{A}$ is a sub-family of $\mathscr{V}$ such that

$\mathscr{S} \cap [\mathscr{V} \backslash g(\mathscr{V})] \neq \phi$ and $g(\mathscr{S}) \subseteq \mathscr{S}$, then by Proposition 4 S is in $\mathscr{S}$, and consequently $\mathscr{S}$ is in Γ, so $\mathscr{S} = \mathscr{V}$. Hence to show that $<\mathscr{V}, g|\mathscr{V}>$ is a Peano System, it remains only to show that $g|\mathscr{V}$ is one-to-one, when S is infinite.

Theorem 1: *If V, W are in $\mathscr{V}$, then either $V \supseteq W$ or $g(W) \supseteq V$.*

Proof: We will prove Theorem 1 in two steps:

Lemma 1: *Suppose, for a fixed W in $\mathscr{V}$, that $V \supset W$ implies $g(V) \supseteq W$, for each V in $\mathscr{V}$. Then $V \supseteq W$ or $g(W) \supseteq V$, for each V in $\mathscr{V}$.*

Proof: Let $\mathscr{S}$ be the family of all V in $\mathscr{V}$ such that $V \supseteq W$ or $g(W) \supseteq V$. We wish to show that $\mathscr{S}$ is in Γ, and hence that $\mathscr{S} = \mathscr{V}$. Clearly S is in $\mathscr{S}$. Suppose that V is in $\mathscr{S}$. We wish to show that $g(V)$ is in $\mathscr{S}$. If $V \supset W$, then $g(V) \supseteq W$, and $g(V)$ is in $\mathscr{S}$. Otherwise $V = W$ or $g(W) \supseteq V$, and in either of these cases we have $g(W) \supseteq g(V)$, so $g(V)$ is again in $\mathscr{S}$. Q.E.D.

Lemma 2: *If W is a fixed element of $\mathscr{V}$, then $V \supset W$ implies $g(V) \supseteq W$, for every V in $\mathscr{V}$.*

Proof: Let $\mathscr{S}$ be the family of all W in $\mathscr{V}$ such that $V \supset W$ implies $g(V) \supseteq W$, for each V in $\mathscr{V}$. We again wish to show that $\mathscr{S}$ is in Γ. S is clearly in $\mathscr{S}$. Suppose that W is in $\mathscr{S}$. We need to show that $g(W)$ is in $\mathscr{S}$. Suppose that $V \supset g(W)$, where V is in $\mathscr{V}$. Then $g(W) \not\supseteq V$, so, by Lemma 1, we have $V \supseteq W$. If $V = W$, then $g(V) = g(W)$, and if $V \supset W$ we have $g(V) \supseteq W \supseteq g(W)$. Q.E.D.

Definition: *Let $I_V = \{W \in \mathscr{V} | W \supseteq V\}$, for each V in $\mathscr{V}$.*

Corollary 1: *$I_{g(V)} = I_V \cup \{g(V)\}$, for each V in $\mathscr{V}$.*

Corollary 2: *The restriction $g|\mathscr{V} \backslash \{\phi\}$ of g to $\mathscr{V} \backslash \{\phi\}$ is one-to-one.*

Proof: Suppose that V, W are distinct elements of $\mathscr{V} \backslash \{\phi\}$. Then either $V \supset W$ or $g(W) \supseteq V$. In the first case we have $W \not\supseteq V$, so $g(V) \supseteq W \supset g(W)$. In the second case we have $g(V) \supseteq V \supset g(V)$. Hence $g(V) \neq g(W)$. Q.E.D.

It follows from Corollary 2 that in order to show that $<\mathscr{V}, g|\mathscr{V}>$ is a Peano System we need only demonstrate that ϕ is not in $\mathscr{V}$, when S in infinite.

Proposition 5: *I_V is finite, for every V in $\mathscr{V}$.*

Proof: Let $\mathscr{S}$ be the Family of all V in $\mathscr{V}$ such that I_V is finite. We wish to show that $\mathscr{S}$ is in Γ. S in $\mathscr{S}$, because $I_S = \{S\}$, which is finite. If V is in $\mathscr{S}$, then $I_{g(V)} = I_V \cup \{U(V)\}$, and I_V is finite, so $I_{g(V)}$ is finite by Proposition 3, and $g(V)$ is in $\mathscr{S}$. Q.E.D.

Corollary: *If ϕ is in $\mathscr{V}$, then $\mathscr{V} = I_\phi$ is finite.*

Proposition 6: *The restriction $f|\mathscr{V} \backslash \{\phi\}$ of f to $\mathscr{V} \backslash \{\phi\}$ is a one-to-one mapping.*

Proof: Suppose that $f(V) = f(W)$, where V, W are in $\mathscr{V} \backslash \{\phi\}$. From the definition of g it follows that $g(V) \not\supseteq W$ and $g(W) \not\supseteq V$, so by Theorem 1 we have $W \not\supseteq V$ and $V \not\supseteq W$. Hence $V = W$. Q.E.D.

Proposition 7: *If* ϕ *is in* $\mathcal{V}$, *then* $f(\mathcal{V}\setminus\{\phi\}) = S$.

Proof: We use a contrapositive argument. Suppose that there is some x in $S/f(\mathcal{V}\setminus\{\phi\})$. Let $\mathcal{J}$ be the family of all V in $\mathcal{V}$ such that x is in V. Clearly S is in $\mathcal{J}$, and if V is in $\mathcal{J}$ it follows that $g(V)$ is in $\mathcal{J}$, since by assumption $f(V) \neq x$ when $V \neq \phi$. Consequently $\mathcal{J}$ is in Γ, so $\mathcal{J} = \mathcal{V}$. Hence ϕ is not in $\mathcal{V}$, which is a contradiction. Q.E.D.

Theorem 2: *If* S *is infinite, then* ϕ *is not in* $\mathcal{V}$.

Proof: We again use a contrapositive argument. Suppose that ϕ is in $\mathcal{V}$. Then, by the corollary to Proposition 5, $\mathcal{V}$ is finite. Consequently $\mathcal{V}\setminus\{\phi\}$ is finite, by Proposition 1. Now the restriction $f|\mathcal{V}\setminus\{\phi\}$ of f to $\mathcal{V}\setminus\{\phi\}$ is a one-to-one mapping from $\mathcal{V}\setminus\{\phi\}$ onto S, by Propositions 6 and 7. Hence it follows from Proposition 2 that S is finite, which is a contradiction. Q.E.D.

Columbus, Ohio