Publ. RIMS, Kyoto Univ.
12 (1977), 577-708

A Foundation of Finite Mathematics[1]

By

Moto-o TAKAHASHI*

Contents

Introduction

The purpose of this article is to study the foundation of finite mathematics from the viewpoint of hereditarily finite sets. (Roughly speaking,

Communicated by S. Takasu, February 21, 1975.

* Department of Mathematics, University of Tsukuba, Ibaraki 300-31, Japan.

[1] This work was supported by the Sakkokai Foundation.

finite mathematics is that part of mathematics which does not depend on the existence of the actual infinity.)

We shall give a formal system for this theory and develop its syntax and semantics in some extent. We shall also study the relationship between this theory and the theory of primitive recursive arithmetic, and prove that they are essentially equivalent to each other. (To be more exact, the latter can be conservatively embedded into the former.)

Relation to the so-called "effectivity in number theory" will also be discussed.

When one considers finite mathematics, the following problems would be basic:

1°. What are finitary objects?

2°. What are finitary operations (and methods)?

3°. What are finitary proofs?

Philosophers may consider these problems philosophically. But let us consider them mathematically here. We seek mathematical formulations of the above three kinds of things. Here mathematical formulation is of course to give exact mathematical definition of what is seemingly mathematical, by abstraction and idealization.

1°. What are finitary objects?

Natural numbers, symbols, finite sets and sequences of such things etc., are usually regarded as finitary objects. But it would be too complex and inconvenient to treat all of them in different types. It would be a reasonable mathematical way to choose some basic type of objects and represent others by these.

Natural numbers or finite sequences of some symbols are usually taken as basic, and it is well-known that other objects are represented by them via Gödel numbers or a kind of coding.

So there would be nothing more to say about the possibility of mathematical formulation of finitary objects. We shall however adopt hereditarily finite sets (for the definition see Section 1) as basic finitary objects in this article, because of their fine structure.

2°. What are finitary operations?

Finitary operations may operate on infinite objects (such as sets of natural numbers). But here we confine ourselves to consider only those finitary operations which operate on finitary objects.

Finitary operations, which are also called algorithm, are finite methods by which any given finitary objects (of a specified kind) are transformed to other finitary objects.

It is well-known that the mathematical formulation of this concept were achieved in 1930's by Herbrand–Gödel, Church, Turing and Post, almost independently. (See e.g. Davis [1].)

When natural numbers are taken as basic, finitary operations are defined to be recursive functions. (Church's thesis). When hereditarily finite sets are taken as basic, they are defined to be Σ_1-definable functions. (See below.)

3°. What are finitary proofs?

Among various kinds of mathematical proofs, finitary (finistic, effective or constructive) proofs have been distinguished often since late 19th century.

Some mathematicians take these finitary proofs as the only mathematically true proofs. Some accepts other proofs but less authentically than finitary proofs. And some others are indifferent to such descrimination.

In this article we would like to give a mathematical formulation of finitary proofs in a fairly strong sense (we call them *strict finitary proofs*). That is to say, we will define them to be formal proofs in the formal system FCS we are going to present.

Our formulation of finitary proofs excludes the use of double induction unless it is reducible to the primitive induction (see below). Strictly speaking, the double induction here means the double induction applied to effective (i.e., Σ_1) predicates and is equivalent to simple induction applied to Π_2-predicates and also to transfinite induction of ω^2-type applied to Σ_1-predicates. (Primitive induction is the simple induction applied to effective (i.e., Σ_1-) predicates. We cannot further confine it to that applied only to decidable (i.e., Δ_1) predicates without assuming other elementary functions than the one we shall adopt, for we need our primitive induction to prove the existence of the values of primitive recursive functions.)

We do not think double induction (or equivalently, simple induction applied to Π_2-formula) to be a strictly finitary method of proof. For, suppose we want to prove $\forall z \forall x \exists y A(z, x, y)$, where A is a decidable predicate, by proving

(i) $\forall x \exists y A(0, x, y)$

and

(ii) $\forall x \exists y A(n, x, y) \longrightarrow \forall x \exists y A(n+1, x, y)$.

Then the assumption $\forall x \exists y A(n, x, y)$ in (ii) is very infinistic, because it assumes, *for every* x, the existence of y such that $A(n, x, y)$. In some cases this assumption may be used for only a few values of x to prove the conclusion of (ii) so that the proof may be reduced to simple induction (applied to Σ_1-predicate). But it is not the case in general. From this observation one thinks natural to exclude such a proof from the scope of finitary proofs. Our formulation will coincide with this intuition.

As we show later, almost all theorems in elementary number theory such as fundamental theorem of arithmetic, Fermat's small theorem, quadratic law of reciprocity etc., can be proved strictly finitarily (in the above sense).

As for theorems on logic, Gentzen's Hauptsatz for LK is proved using double induction. So the proof itself is not strictly finitarily. However this theorem can be proved strictly finitarily (and hence in FCS) by a combined use of Herbrand's theorem and Ackermann's consistency theorem, both of which can be proved strictly finitarily.

Incidentally it would be interesting to ask whether Fermat's conjecture (or other unsolved problems in number theory) can be proved in FCS. It may be possible that the conjecture itself is true but not provable in FCS.

Finally, it should be noted that it is not our intention of this article to conclude that finite mathematics is the only mathematics, because we believe that infinite mathematics exists as its own right.

Acknowledgement

I would like to express my thanks to Professor K. Gödel and Professor G. Takeuti for valuable discussions about finite mathematics.

1. Informal Theory of Hereditarily Finite Sets

For each natural number n, let R_n be defined as follows:

$R_0 = \emptyset$ (the empty set), and $R_{n+1} = P(R_n)$ (P for the power set operation). Then we put $R_\omega = \bigcup_n R_n$. Elements of R_ω are called hereditarily finite sets. The R_n's have the following properties:

1.1. $R_n \subseteq R_{n+1}$,

1.2. R_n is finite,

1.3. R_n is transitive, that is, $x \in R_n$ and $y \in x$ imply $y \in R_n$.

From these we see that R_ω consists precisely of finite subsets of R_ω. That is,

1.4. $u \in R_\omega \Leftrightarrow u \subseteq R_\omega$ and u is finite.

Indeed R_ω is the least set satisfying this condition, that is:

1.5. If X is a set such that X contains every finite subset of X, then $R_\omega \subseteq X$.

1.6. There is no infinite descending sequence such that $R_\omega \ni a_1 \ni a_2 \ni a_3 \ni \cdots$.

1.7. The structure $(R_\omega, \in)$ is a model of Zermelo–Fraenkel axiom system for set theory except the axiom of infinity, and is called Ackermann's model.

This comes easily from the facts that

(i) The power set of a finite set is finite,

(ii) the union of a finite set of finite sets is finite, and

(iii) The range of a finite function (i.e., a function whose domain is a finite set) is finite.

On account of 1.7, we can develop a finite set theory. For example, an ordered pair (and more generally, an n-tuple) is defined by

$$\langle a, b\rangle=\{\{a\}, \{a, b\}\}.$$

$$(\langle a_1,\dots, a_n\rangle=\langle a_1, \langle a_2,\dots, a_n\rangle\rangle.)$$

A finite relation is defined to be a set in R_ω such that every element of it is a pair. A finite function f is a single-valued finite relation ($\langle u, w\rangle$, $\langle v, w\rangle\in f\Rightarrow u=v$). The domain and the range of f are:

$$\mathrm{dom}(f)=\{w|\exists u\langle u, w\rangle\in f\} \text{ and } \mathrm{rang}(f)=\{u|\exists w\langle u, w\rangle\in f\}.$$

Both of these are elements of R_ω whenever f is, etc.

Now we define a binary operation $\#$ on R_ω as follows: for $a, b\in R_\omega$, $a\# b=a\cup\{b\}$, that is, $a\# b$ is the set a added by a single element b. This extremely primitive operation will be taken as basic in our formal theory of hereditarily finite sets below.

Now, R_ω is generated from 0 by this $\#$ operation,*) that is,

1.8. If X is a set such that $0\in X$ and that $a, b\in X$ imply $a\# b\in X$,

then $R_\omega\subseteq X$. Indeed we can show by induction that $R_n\subseteq X$, using the fact that

$$\{a_1,\dots, a_m\}=(\cdots(0\# a_1)\#\cdots)\# a_m).$$

1.8 will be taken as an induction principle in our formal theory (named primitive induction).

Let N denote the set of all natural numbers: $N=\{0, 1, 2,\dots\}$. Let D be the bijection from N onto $P_\omega(N)$ (the set of all finite subsets of N) defined by

1.9. $D(n)(=D_n)=\{n_1,\dots, n_k\}$,

where $n_1,\dots, n_k$ are distinct and $n=2^{n_1}+2^{n_2}+\cdots+2^{n_k}$, i.e., the right-

*) From now on the empty set $\emptyset$ is identified with 0.

hand side is the binary expansion of n. Then a bijection t from N onto R_ω is defined by induction thus;

1.10. $t(n)(=n^t)=\{t(i)|i\in D_n\}$.

This function is well defined, since if $i\in D_n$ then $i<n$. This function is really 1–1 onto, as can easily be shown by induction. It gives a canonical 1–1 coding of h.f. (hereditarily finite) sets into natural numbers. By definition we have

1.11. $x^t\in y^t \Leftrightarrow x\in D_y$, for any $x, y\in N$.

The predicate $\lambda x, y(x\in D_y)$ is primitive recursive. Also the function $\lambda x, y\cdot t^{-1}(x^t \# y^t)$ is primitive recursive. Since the function t and its inverse t^{-1} are very simple and to be effectively calculable, it is natural that relations on R_ω and functions on R_ω to R_ω are defined to be primitive (general) recursive iff they are so when they are transferred into relations on N and functions on N to N via t. For instance, if $R(a, b)$ is a relation on R_ω, then R is primitive recursive iff the relation R' defined by $R'(x, y)\Leftrightarrow R(x^t, y^t)$ is primitive recursive, and if $f(a)$ is a function on R_ω to R_ω, then f is general recursive iff the function f' on N to N defined by $f'(x)=t^{-1}(f(x^t))$ is general recursive.

According to the above, natural numbers are regarded as hereditarily finite sets (via t operation). In spite of it, this coding of natural numbers (into R_ω) might be somewhat unnatural and hard to treat. It would rather be preferable to define natural numbers (in the theory of hereditarily finite sets) as von Neumann ordinals (since we only treat finite sets, we have only *finite* von Neumann ordinals). Thus a h.f. set is a natural number (in symbol Nat(x)) iff x is transitive and every element of x is transitive. (This definition of von Neumann ordinals is due to Shoenfield [1].) Thus natural numbers are regarded as a special kind of h.f. sets. Starting from this definition elementary number theory can be developed.

Finite sequences (of h.f. sets) are a special kind of finite functions (defined as above and which itself is a h.f. set) i.e., a function whose domain is a natural number i.e. the set of natural numbers less than it).

Thus, formulas (of a finitary logic) may be expressed by h.f. sets, as finite sequences of certain symbols, where these symbols are in turn preassumed to be special h.f. sets.

But they can also be coded by the method of cumulative construction. For example, formulas of the usual propositional calculus are defined in the theory of h.f. sets as follows:

(i) $\langle 0, n\rangle$ is a formula;
(ii) if A is a formula, then $\langle 1, A\rangle$ is a formula;
(iii) if A and B are formulas, then $\langle 2, A, B\rangle$ is a formula;
(iv) the only formulas are obtained by (i)–(iii).

Intuitively, $\langle 0, n\rangle$ stands for the n^{th} propositional variable, $\langle 1, A\rangle$ for $\neg A$, $\langle 2, A, B\rangle$ for $A \vee B$. Then $A \wedge B$ is, as usual, defined to be $\neg(\neg A \vee \neg B)$, i.e., $\langle 1, \langle 2, \langle 1, A\rangle, \langle 1, B\rangle\rangle\rangle$. Note that the usual convention for using and abbreviating parentheses is naturally accepted in this case.

Moreover, the notion of formal proofs (in a finitary logic), in whichever style it is formulated, can be reformulated in the theory of h.f. sets in an obvious way. Thus the theory of a finitary logic can be subsumed into the theory of h.f. sets.

A composition is a set with repetition. For instance, in a composition $(ppqpq)$, which is the same as $(pqpqp)$, p occurs three times and q occurs twice, provided p and q are different. Thus a composition is represented by the function whose domain is the set of objects that occur at least once in this composition and whose value at an object is the number of occurrences of the object in the composition. In particular a finite composition of h.f. sets is coded by a h.f. sets:

$$\mathrm{Cb}(f) \Leftrightarrow \{f \text{ is a finite function}\} \wedge \forall x \in \mathrm{rang}(f)(\mathrm{Nat}(x) \wedge x \neq 0).$$

Suppose f is a finite composition of natural numbers. Then we can refer to the sum Σf and the product Πf (as natural number). If $n = \Pi f$, then f is said to be a factorization of n. In addition, if f is composed of prime numbers, then f is said to be a prime factorization of n. In this framework we can state the fundamental theorem of elementary arithmetic as follows; if n is a positive natural number, then there exists one and only one prime factorization (in the above sense) of it. This formulation of the fundamental theorem is much more natural than other formulations of it, as in Skolem [1] (in which only the existence-part of the theorem is formulated) and in Goodstein [4] (in which the uniqueness-part of the theorem is not formulated as a single theorem but a metatheorem (including function variables)), etc.

Moreover, within the theory of h.f. sets, we can go beyond natural numbers to integers, rational numbers, algebraic numbers (integers), polynomials with coefficients from objects already defined, and so on, in an obvious way. (Although the classification method does not apply since it must make use of infinite sets, a finite counterpart of it is readily available.) One can then develop elementary theories of such objects (e.g. such algebraic theory of numbers as Kronecker programmed (e.g. Weyl [1], Reid [1]).

Remark. Primitive recursive relations and functions on R_ω have been characterized e.g. by Rödding [1] (finite) set-theoretically and by Gandy etc., with such definition schemata as Kleene's. General recursive relations and functions are characterized as Δ_1-definable one e.g. by the author [2]. These characterizations are all semantical. Any characterization of general recursive functions is inevitably semantical and non-constructive on account of Gödel's consistency (i.e., the second incompleteness) theorem. Indeed, given a kind of syntactical standpoints (or even any of formalizable theories, e.g. ZF set theory), we can construct a general recursive function which cannot be proved to be general recursive within the system. To prove this let T be a formula in the given system, say S, which defines general recursive functions e.g. the one like T-predicate of Kleene. General recursive functions (say, of one variable) are then defined in the system S by the predicate

$$\mathrm{Gr}(d) \Leftrightarrow \forall x \exists y\, T(d, x, y),$$

which says that computation always halts. (All the variables are assumed to range over natural numbers.) Let

$$P_0, P_1, P_2, \ldots$$

be an enumeration of formal proofs in S. Let g be defined by

$$g(n)=\begin{cases} U(\mu yT((n)_1,\ n,\ y))+1, & \text{if } P_{(n)_0} \text{ is a proof of} \\ & \forall x\exists yT((n)_1,\ x,\ y), \\ 0, & \text{otherwise.} \end{cases}$$

(Notations are as in Kleene [1].)
g is clearly general recursive. But if it were proved to be general recursive in S, in other words, if there were a number e such that e represents the general recursive function g and $\vdash_S \mathrm{Gr}(e)$, then there would be a proof of P_p of $\forall x\exists y\, T(e,\ x,\ y)$ and so letting $n=2^p3^e$, we would have $g(n)=U(\mu yT(e,\ n,\ y))+1=g(n)+1$, a contradiction.

On the other hand, primitive recursive functions are characterized by an effective method. In this paper we shall characterize them in a formal system named FCS. Roughly speaking it takes the following form: $\{\varphi_e | \vdash_{\mathrm{FCS}} \forall x\exists y\, T(e,\ x,\ y)\}$ is just the set of all primitive recursive functions, where φ_e is the function with Gödel number e.

2. Formal Theory of Hereditarily Finite Sets, Introduction

In the monograph of P. J. Cohen [1], page 23, a formal system, named Z_2, of hereditarily finite sets is presented. His system is equivalent to the usual axiom system for Zermelo–Fraenkel set theory excluding the axiom of infinity and including, instead of it, an axiomschema of mathematical induction on (von Neumann) ordinals.

It is also equivalent to the following simpler system which is composed of the axioms;

(i) extensionality: $\forall x\forall y(\forall z(z\in x\rightarrow z\in y)\rightarrow\forall u(x\in u\rightarrow y\in u))$,

(ii) empty set: $\exists x\forall y\neg y\in x$,

(or rather, using the constant 0, $\forall y\neg y\in 0$),

(iii) addition: $\forall x\forall y\exists z\forall u(u\in z\rightleftarrows u\in x\vee u=y)$,

(or rather, using the function symbol $\#$,
$\forall x\forall y\forall u(u\in x\# y\rightleftarrows u\in x\vee u=y)$), and the axiomschema;

(iv) induction: $\varphi(0)\wedge\forall x\forall y(\varphi(x)\wedge\varphi(y)\rightarrow\varphi(x\# y))\rightarrow\forall x\varphi(x)$,
where φ is a formula of set theory (possibly with constants 0 and $\#$). The meaning of these axioms is clear on account of preceding chapter.

Such axioms as sum-set, power-set, and replacement-schema are derivable from this system. In the proof of it the last induction principle plays an essential role.

As is indicated in Cohen [1], these systems are essentially equivalent to the first order arithmetic and also, as indicated in Jensen–Karp [1], they have a technical advantage of "ease of coding", as we have occasionally seen in preceding chapter.

So far, it has tacitly been assumed that the underlying formal logic upon which each theory is constructed is the first order classical predicate calculus. But evidently, the same things as mentioned above are true with the first order intuitionistic predicate calculus.

However, we seek a formal theory of hereditarily finite sets with more restrictive and effective kind of axioms. One of the motivations to this direction is the so-called Σ_1-restricted replacement schema that appeared in the theory of admissible sets in Kripke [1] and Platek [1]. As most of elementary effective part of set theory can be developed with this weak replacement schema, it would be natural to consider that most of elementary number theory and finite mathematics could be developed with Σ_1-induction principle, i.e., (iv) above with φ restricted to Σ_1-formulas, keeping (i)–(iii) unchanged. Also from the viewpoint of effectivity preference in finite mathematics, it would be desirable to take as the underlying logic the first-order intuitionistic predicate calculus instead of the classical one.

Let us call this modified system FS. FS still contains any first-order formulas as meaningful, e.g. we can speak of provability of these formulas. But most of notions that actually appears in the elementary development of number theory and of h.f. sets are recursive, or at least recursively enumerable. Thus, by the characterization of general recursive predicates mentioned in preceding chapter, these notions are expressed by Σ_1-formulas in the sense of Lévy [1]. For example, the relation $z=x\cup y$ is expressed by a restricted formula: $\forall u\in x(u\in z)\wedge\forall u\in y(u\in z)\wedge\forall u\in z(u\in x\vee u\in y)$. Then, the existence of the union of two sets is described as a Σ_1-formula: $\exists z(z=x\cup y)$ (see section 5), with free variables x, y as symbols expressing arbitrary h.f. sets. Indeed, most of theorems proved in elementary number theory are of this form. For more examples, the notions (and theorems) introduced in the informal theory in previous chapter are all of this form.

From these observations we see it would be interesting to formulate a formal theory which contains, from the outset, only Σ_1-formulas. These motivations have led us to formulate the formal system FCS (for finite combinatorial set theory), which will be presented hereafter.

3. The Formal System FCS

3.1. Formal symbols of FCS.

3.1.1. Countable lists of free variables and of bound variables. Usually, $a, b, c, d, a_1, b_1, c_1, d_1$, etc. shall stand for free variables and $x, y, z, u, s_1, y_1, z_1, u_1$, etc. stand for bound variables. The set of free variables is denoted by $\mathbb{F}$ and the set of bound variables by $\mathbf{B}$.

3.1.2. A function symbol $\#$ (of two variables) and a constant 0.

3.1.3. A binary predicate symbol $\in$.

3.1.4. Logical symbols: $\neg, \vee, \wedge, \rightarrow, \forall, \exists$.

3.2. Terms are defined by the following inductive definition. (The extremal clause i.e., the least set condition, will always be omitted in each inductive definition hereafter.)

(i) 0 is a term;

(ii) Free variables are terms;

(iii) If s and t are terms, then $\#st$ is a term.

3.3. Semi-terms are defined as follows:

(i) 0 is a semi-term;

(ii) Variables (both free and bound) are semi-terms;

(iii) If s and t are semi-terms, then $\#st$ is a semi-term.

3.4. Restricted semi-formulas (abbreviated RF′) are defined as follows:

(i) If s and t are semi-terms, then $\in st$ is an RF′;

(ii) If φ is an RF′, so is $\neg\varphi$;

(iii) If φ and ψ are RF′'s, so are $\vee\varphi\psi$, $\wedge\varphi\psi$ and $\rightarrow\varphi\psi$;

(iv) If x is a bound variable, t a semi-term and φ an RF′, then $\exists x\in t\varphi$ and $\forall x\in t\varphi$ are RF′'s.

3.5. Σ-semi-formulas (abbreviated $\sum$F′) are defined as follows:

(i) RF′'s are $\sum$F′'s;

(ii) If A and B are $\sum$F′'s, so are $\vee AB$ and $\wedge AB$.

(iii) If φ is an RF′ and B is a $\sum$F′, then $\to\varphi B$ is a $\sum$F′;

(iv) If x is a bound variable, t a semi-term and A a $\sum$F′, then $\exists x\in tA$ and $\forall x\in tA$ are $\sum$F′'s;

(v) If x is a bound variable and A is a $\sum$F′, then $\exists xA$ is a $\sum$F′.

r, s, t etc. will stand for semi-terms, φ, ψ, χ etc. for restricted semi-formulas and A, B, C etc. for Σ-semi-formulas.

Note that $\neg A$ is not a $\sum$F′ in general.

3.6. To each semi-term and to each Σ-semi-formula, a finite set of variables is assigned as follows:

(0) $V(0)=\varphi$

(i) $V(w)=\{w\}$, if w is a variable,

(ii) $V(\# st)=V(s)\cup V(t)$,

(iii) $V(\neg\varphi)=V(\varphi)$,

(iv) $V(\vee AB)=V(\wedge AB)=V(A)\cup V(B)$,

(v) $V(\to\varphi B)=V(\varphi)\cup V(B)$,

(vi) $V(\exists x\in tA)=V(\forall x\in tA)=(V(A)-\{x\})\cup V(t)$,

(vii) $V(\exists xA)=V(A)-\{x\}$.

The assignment V is well-defined on account of the uniqueness of construction of the so-called Polish notation. Note that every RF′ is $\sum$F′ and hence the cases (i)–(vii) of this definition cover all cases.

If a variable is in $V(s)$ or $V(A)$, then we say the variable occurs free in s or in A, respectively.

3.7. A restricted semi-formula φ is called a restricted formula (abbreviated RF) if $V(\varphi)\cap\mathbf{B}=\emptyset$, and a Σ-semi-formula A is called a Σ-formula (abbreviated $\sum$F) if $V(A)\cap\mathbf{B}=\emptyset$.

Thus a RF′($\sum$F′) is a RF($\sum$F) iff the bound variables occurring in it are actually bound by quantifiers in it.

3.8. Let r be a term, v a (free or bound) variable, s a semi-term and A a $\sum$F′. Then a semi-term $s(r/v)$ and a $\sum$F′, $A(r/v)$ are defined by the induction on s and on A as follows:

(i) $0(r/v)\asymp 0$,

(ii) $v(r/v)\asymp r$,

(iii) $w(r/v)\asymp w$, if w is a variable other than v,

(iv) $(\# st)(r/v)\asymp \#^\frown s(r/v)^\frown t(r/v)$,

(v) $(\in st)(r/v)\asymp \in^\frown s(r/v)^\frown t(r/v)$,

(vi) $(\neg\varphi)(r/v)\asymp \neg^\frown\varphi(r/v)$,

(vii) $(\vee AB)(r/v)\asymp \vee^\frown A(r/v)^\frown B(r/v)$,

(viii) $(\wedge AB)(r/v)\asymp \wedge^\frown A(r/v)^\frown B(r/v)$

(ix) $(\rightharpoonup\varphi B)(r/v)\asymp \rightharpoonup^\frown\varphi(r/v)^\frown B(r/v)$,

(x) $(\exists x\in tA)(r/v)\asymp \exists x\in^\frown t(r/v)^\frown A$, if x is v,
$\asymp \exists x\in^\frown t(r/v)^\frown A(r/v)$, if x is not v,

(xi) $(\forall x\in tA)(r/v)\asymp \forall x\in^\frown t(r/v)^\frown A$, if x is v,
$\asymp \forall x\in^\frown t(r/v)^\frown A(r/v)$, if x is not v,

(xii) $(\exists xA)(r/v)\asymp \exists xA$, if x is v,
$\asymp \exists x^\frown A(r/v)$, if x is not v.

In this definition, $\asymp$ denotes symbolic identity and $^\frown$ denotes concatenation.

$s(r/v)$ and $A(r/v)$ are thus the results of replacing each free occurrence of v in s and A by r. We could more generally define the simulatneous substitution $A(r_1,\dots, r_n/v_1,\dots, v_n)$ in the similar way.

In spite of the presence of the above rigorous definition and notation of substitution we shall often use it conventionally.

3.9. Convention.

We adopt the following conventions.

$\# st$, $\in st$, $\vee AB$, $\wedge AB$, $\rightharpoonup\varphi B$ are usually written $s\# t$, $s\in t$, $A\vee B$, $A\wedge B$, $\varphi\rightharpoonup B$, respectively. Moreover, $\varphi\rightleftharpoons\psi$ is an abbreviation of $(\varphi\rightharpoonup\psi)\wedge(\psi\rightharpoonup\varphi)$. These symbols $\#$, $\in$, $\neg$, $\vee$, $\wedge$, $\rightharpoonup$, $\rightleftharpoons$ then become operations on (restricted or Σ-) formulas. So the usual convention on parentheses is naturally accepted.

3.10. The inference rules of FCS are as follows. (FCS does not contain any axiom.) We shall express them in the following charts as in Gentzen's system NJ. The exact meaning of them will be explained after that. In the following, r, s, t stand for terms, φ, ψ for RF's, A, B C for $\sum$F's and D for $\sum$F$'$ with $V(D)\cap\mathbf{B}\subseteq\{x\}$. Moreover, $r\subseteq s$ stands for $\forall x_1\in r(x_1\in s)$ and $r=s$ for $r\subseteq s\wedge s\subseteq r$.

$$\text{(i)}\ \frac{r\in 0}{A}(0\text{E}) \qquad \text{(ii)}\ \frac{r\in s}{r\in s\# t}(\#\text{I}1) \qquad \text{(iii)}\ \frac{r=t}{r\in s\# t}(\#\text{I}2)$$

$$\text{(iv)}\ \frac{r\in s\# t \quad \begin{array}{c} r\in s \\ \vdots \\ A \end{array} \quad \begin{array}{c} r=t \\ \vdots \\ A \end{array}}{A}(\#\text{E}) \qquad \text{(v)}\ \frac{\begin{array}{c} \psi \\ \vdots \\ \varphi \end{array} \quad \begin{array}{c} \psi \\ \vdots \\ \neg\varphi \end{array}}{\neg\psi}(\neg\text{I}) \qquad \text{(vi)}\ \frac{\varphi \quad \neg\varphi}{A}(\neg\text{E})$$

$$\text{(vii)}\ \frac{A}{A\vee B}(\vee\text{I}1) \qquad \text{(viii)}\ \frac{B}{A\vee B}(\vee\text{I}2) \qquad \text{(ix)}\ \frac{A\vee B \quad \begin{array}{c} A \\ \vdots \\ C \end{array} \quad \begin{array}{c} B \\ \vdots \\ C \end{array}}{C}(\vee\text{E})$$

$$\text{(x)}\ \frac{A \quad B}{A\wedge B}(\wedge\text{I}) \qquad \text{(xi)}\ \frac{A\wedge B}{A}(\wedge\text{E}1) \qquad \text{(xii)}\ \frac{A\wedge B}{B}(\wedge\text{E}2)$$

$$\text{(xiii)}\ \frac{\begin{array}{c} \varphi \\ \vdots \\ B \end{array}}{\varphi\rightharpoonup B}(\rightharpoonup\text{I}) \qquad \text{(xiv)}\ \frac{\varphi\rightharpoonup B \quad \varphi}{B}(\rightharpoonup\text{E}) \qquad \text{(xv)}\ \frac{s\in r \quad D(s/x)}{\exists x\in rD}(\text{b}\exists\text{I})$$

$$\text{(xvi)}\ \frac{\exists x\in rD \qquad \begin{array}{c} a\in r \quad D(a/x) \\ \ddots \quad \cdot^{\cdot^{\cdot}} \\ A \end{array}}{A}(\text{b}\exists\text{E}) \qquad \text{(xvii)}\ \frac{\begin{array}{c} a\in r \\ \vdots \\ D(a/x) \end{array}}{\forall x\in rD}(\text{b}\forall\text{I})$$

$$\text{(xiii)}\ \frac{\forall x\in rD \quad s\in r}{D(s/x)}(\text{b}\forall\text{E}) \qquad \text{(xix)}\ \frac{D(s/x)}{\exists xD}(\exists\text{I})$$

$$\text{(xx)}\ \frac{\exists xD \qquad \begin{array}{c} D(a/x) \\ \vdots \\ B \end{array}}{B}(\exists\text{E}) \qquad \text{(xxi)}\ \frac{D(0/x) \qquad \begin{array}{c} D(a/x) \quad D(b/x) \\ \ddots \quad \cdot^{\cdot^{\cdot}} \\ D(a\# b/x) \end{array}}{D(s/x)}(\text{PI})$$

The last inference rule is also called the inference of primitive induction.

3.11. What we wish to define precisely is the notion of derivation and that of derivability. We define the notion $P\colon\Gamma\vdash A$ (to be read, P is a derivation of A from Γ), where Γ stands for a finite set of $\sum$F's, A a $\sum$F and P a finite object as defined inductively as follows. (r, s,

t, φ, ψ, A, B, C, D are the same as above.) Clauses (i)–(xxi) correspond to the above inference rules.

(0) If $A\in\Gamma$, then $A\colon \Gamma\vdash A$. (This means intuitively that A standing alone is a proof of A from Γ provided $A\in\Gamma$.)

(i) If P: $\Gamma\vdash r\in 0$, then $\dfrac{P}{A}$: $\Gamma\vdash A$.

(ii) If P: $\Gamma\vdash r\in s$, then $\dfrac{P}{r\in s\#t}$: $\Gamma\vdash r\in s\#t$.

(iii) If P: $\Gamma\vdash r=t$, then $\dfrac{P}{r\in s\#t}$: $\Gamma\vdash r\in s\#t$.

(iv) If P: $\Gamma\vdash r\in s\#t$, Q: $\Gamma\cup\{r\in s\}\vdash A$ and R: $\Gamma\cup\{r=t\}\vdash A$, then $\dfrac{P\quad Q\quad R}{A}$: $\Gamma\vdash A$.

(v) If P: $\Gamma\cup\{\psi\}\vdash\varphi$ and Q: $\Gamma\cup\{\psi\}\vdash\neg\varphi$, then $\dfrac{P\quad Q}{\neg\varphi}$: $\Gamma\vdash\neg\varphi$.

(vi) If P: $\Gamma\vdash\varphi$ and Q: $\Gamma\vdash\neg\varphi$, then $\dfrac{P\quad Q}{A}$: $\Gamma\vdash A$.

(vii) If P: $\Gamma\vdash A$, then $\dfrac{P}{A\vee B}$: $\Gamma\vdash A\vee B$.

(viii) If P: $\Gamma\vdash B$, then $\dfrac{P}{A\vee B}$: $\Gamma\vdash A\vee B$.

(ix) If P: $\Gamma\vdash A\vee B$, Q: $\Gamma\cup\{A\}\vdash C$ and R: $\Gamma\cup\{B\}\vdash C$, then $\dfrac{P\quad R\quad Q}{C}$: $\Gamma\vdash C$.

(x) If P: $\Gamma\vdash A$ and Q: $\Gamma\vdash B$, then $\dfrac{P\quad Q}{A\wedge B}$: $\Gamma\vdash A\wedge B$;

(xi) If P: $\Gamma\vdash A\wedge B$, then $\dfrac{P}{A}$: $\Gamma\vdash A$.

(xii) If P: $\Gamma\vdash A\wedge B$, then $\dfrac{P}{B}$: $\Gamma\vdash B$.

(xiii) If P: $\Gamma\cup\{\varphi\}\vdash B$, then $\dfrac{P}{\varphi\rightarrow B}$: $\Gamma\vdash\varphi\rightarrow B$.

(xiv) If P: $\Gamma\vdash\varphi\rightarrow B$, and Q: $\Gamma\vdash\varphi$, then $\dfrac{P\quad Q}{B}$: $\Gamma\vdash B$;

(xv) If P: $\Gamma\vdash s\in r$ and Q: $\Gamma\vdash D(s/x)$, then $\dfrac{P\quad Q}{\exists x\in rD}$: $\Gamma\vdash\exists x\in rD$;

(xvi) If $P\colon \Gamma\vdash\exists x\in rD$ and $Q\colon \Gamma\cup\{a\in r,\ D(a/x)\}\vdash A$, then $\dfrac{P\quad Q}{A}$: $\Gamma\vdash A$, provided none of r, A, D, Γ contain the free variable a, i.e., $a\notin V(r)\cup V(A)\cup V(D)\cup V(\Gamma)$, where $V(\Gamma)=\cup\{V(C)|C\in\Gamma\}$;

(xvii) If $P\colon \Gamma\cup\{a\in r\}\vdash D(a/x)$, then $\dfrac{P}{\forall x\in rD}$: $\Gamma\vdash\forall x\in rD$, provided

$a \notin V(r) \cup V(D) \cup V(\Gamma)$.

(xviii) If $P\colon \Gamma \vdash \forall x \in r D$ and $Q\colon \Gamma \vdash s \in r$, then $\dfrac{P \quad Q}{D(s/x)}\colon \Gamma \vdash D(s/x)$.

(xix) If $P\colon \Gamma \vdash D(s/x)$, then $\dfrac{P}{\exists x D}\colon \Gamma \vdash \exists x D$.

(xx) If $P\colon \Gamma \vdash \exists x D$ and $Q\colon \Gamma \cup \{D(a/x)\} \vdash B$, then $\dfrac{P \quad Q}{B}\colon \Gamma \vdash B$, provided $a \notin V(D) \cup V(B) \cup V(\Gamma)$.

(xxi) If $P\colon \Gamma \vdash D(0/x)$ and $Q\colon \Gamma \cup \{D(a/x), D(b/x)\} \vdash D(a \# b/x)$, then $\dfrac{P \quad Q}{D(r/x)}\colon \Gamma \vdash D(r/x)$, provided a and b are distinct free variables and $a, b \notin V(\Gamma) \cup V(D)$.

3.12. Suppose $P\colon \Gamma \vdash A$. If Γ is empty, then we simply write $P\colon \vdash A$ and say P is a derivation (or a proof) of A.

Also we write $\Gamma \vdash A$ and say A is derivable from Γ if there exists a P such that $P\colon \Gamma \vdash A$. If in addition Γ is empty we simply write $\vdash A$ and say A is derivable or provable or a formal theorem (of FCS). This notion of derivability $\Gamma \vdash A$ could be defined also by omitting the P-part of the definition of $P\colon \Gamma \vdash A$. So we can prove some theorems by the induction on $\Gamma \vdash A$, which we shall use without reference.

$A \dashv\vdash B$ stands for $A \vdash B$ and $B \vdash A$. Moreover, expressions such as $A, \Gamma \vdash B$ or $\Gamma, A \vdash B$ abbreviate $\{A\} \cup \Gamma \vdash B$.

This completes the description of the system FCS.

4. Syntax of FCS; Basic Theorems and Metatheorems

In this and subsequent sections we shall develop the syntax of the system FCS and prove various formal theorems and metatheorems about the system. (Strictly speaking, formal theorem A is a metatheorem $\vdash A$.) Formal theorems are designated by **T1**, **T2**, etc., while metatheorems are designated by **Theorem 1**, **Theorem 2**, etc. It is tacitly assumed that in the following the different syntactical variables a, b, c etc., for variables occurring in the same context express different variables.

Theorem 4.1.

(i) *If* $\vdash A$, *then* $\vdash A(t/a)$.

(ii) *If* $\Gamma \vdash A$, *then* $\Gamma(t/a) \vdash A(t/a)$.

(iii) *If* $\Gamma \subseteq \Pi$ *and* $\Gamma \vdash A$, *then* $\Pi \vdash A$.

(iv) *If* $\Gamma \vdash A$ *and* $\Pi \vdash B$ *for each* $B \in \Gamma$, *then* $\Pi \vdash A$.

(v) *If* $\Gamma \vdash A$ *and* $\{A\} \cup \varDelta \vdash B$, *then* $\Gamma \cup \varDelta \vdash B$.

Outline of proof. First we prove (ii). For this we define a modified notion $\Gamma \vdash_n A$, where n is a natural number. The definition of it is obtained from the definition of $\Gamma \vdash A$ by attaching the subscript n to $\vdash$ in the consequence of each clause and subscripts k, l, m etc., to $\vdash$ in the hypotheses and adding hypothesis $k<n$, $l<n$, $m<n$ etc., in each clause. For example, (i) becomes

(i)′ if $A \in \Gamma$, then $A: \Gamma \vdash_n A$ (for each n), and (x) becomes:

(x)′ If $P: \Gamma \vdash_k A \vee B$, $Q: \Gamma \cup \{A\} \vdash_l C$, $R: \Gamma \cup \{B\} \vdash_m C$ and $k<n$, $l<n$, $m<n$, then $\dfrac{P \quad Q \quad R}{C}: \Gamma \vdash_n C$.

Then it is obvious that $\Gamma \vdash A$ iff $\Gamma \vdash_n A$ for some n. Then prove

4.1.1. If $\Gamma \vdash_n A$, then $\Gamma(t/a) \vdash_n A(t/a)$,

by the induction on n. The trouble with quantification can then be overcome by changing variables twice or more using induction hypothesis. For further detail see the proof of Theorem 2.1 in Takahashi [3]. (ii) is an immediate consequence of 4.1.1. (i) is a special case of (ii). (iii) and (iv) can be proved by the induction on $\Gamma \vdash A$, making use of (ii) in case of quantification. (v) is an immediate corollary of (iv).

q.e.d.

Theorem 4.2. *If A is a* $\sum$F *and at the same time is an instance of tautology of intuitionistic propositional calculus, then* $\vdash A$.

Proof. This theorem is obvious since FCS includes all the inference rules of the intuitionistic propositional calculus NJ of Gentzen [1].

q.e.d.

T.4.3. (i) $a \subseteq a$.

(ii) $a \subseteq b \wedge b \subseteq c \rightharpoonup a \subseteq c$.

(iii) $a = a$.

(iv) $a = b \rightharpoonup b = a$.

(v) $a = b \wedge b = c \rightharpoonup a = c$.

(vi) $a=b \wedge c \in a \rightharpoonup c \in b.$

(vii) $a \subseteq b \rightharpoonup a \# c \subseteq b \# c.$

(viii) $a=b \rightharpoonup a \# c = b \# c.$

(ix) $a=b \rightharpoonup c \# a = c \# b.$

(x) $a=b \wedge a \in c \rightharpoonup b \in c.$

Outline of proof of T4.3.
(i) is just $\forall x_1 \in a(x_1 \in a)$. It is provable as follows:

$$b \in a \vdash b \in a \qquad \text{by (identity)}$$

$$\vdash \forall x_1 \in a(x_1 \in a) \quad \text{by} \quad (\text{b}\forall\text{I}).$$

(ii) is $\forall x_1 \in a(x_1 \in b) \vee \forall x_1 \in b(x_1 \in c) \rightharpoonup \forall x_1 \in a(x_1 \in c)$.
We have easily

$$d \in a,\ a \subseteq b \wedge b \subseteq c \vdash \forall x_1 \in a(x_1 \in b) \qquad (\text{id and } \wedge\text{E1})$$

and

$$d \in a,\ a \subseteq b \wedge b \subseteq c \vdash d \in a \qquad (\text{id})$$

Hence

$$d \in a,\ a \subseteq b \wedge b \subseteq c \vdash d \in b \qquad (\text{b}\forall\text{E})$$

But

$$d \in a,\ a \subseteq b \wedge b \subseteq c \vdash \forall x_1 \in b(x_1 \in c) \qquad (\text{id and } \wedge\text{E2})$$

Hence

$$d \in a,\ a \subseteq b \wedge b \subseteq c \vdash d \in c \qquad (\text{b}\forall\text{E})$$

Hence

$$a \subseteq b \wedge b \subseteq c \vdash \forall x_1 \in a(x_1 \in c) \qquad (\text{b}\forall\text{I})$$

So

$$\vdash a \subseteq b \wedge b \subseteq c \rightharpoonup a \subseteq c.$$

(iii) is obvious from (i) by ($\wedge$I).
(iv) $a \subseteq b \wedge b \subseteq a \rightharpoonup b \subseteq a \wedge a \subseteq b$.

This is an instance of a theorem of intuitionistic propositional calculus, i.e., $A \wedge B \rightharpoonup B \wedge A$ and hence provable in FCS.

(v) $(a \subseteq b \wedge b \subseteq a) \wedge (b \subseteq c \wedge c \subseteq b) \rightharpoonup (a \subseteq c \wedge c \subseteq a)$.

This comes from (ii) and the fact

$$A \wedge B \rightharpoonup C,\ A' \wedge B' \rightharpoonup C' \vdash (A \wedge A') \wedge (B \wedge B') \rightharpoonup (C \wedge C').$$

(vi) It easily follows from $a \subseteq b,\ c \in a \vdash c \in b$.
(vii) By (b$\forall$I) and ($\rightharpoonup$I), it suffices to prove

$$d \in a \# c,\ a \subseteq b \vdash d \in b \# c.$$

By ($\#$E) this comes from

(1) $$d \in a \# c,\ a \subseteq b \vdash d \in a \# c,$$

(2) $$d \in a,\ d \in a \# c,\ a \subseteq b \vdash d \in b \# c,$$

(3) $$d = c,\ d \in a \# c,\ a \subseteq b \vdash d \in b \# c.$$

(1) holds by (id), (2) holds by ($\#$I1) from

$$d \in a,\ d \in a \# c,\ a \subseteq b \vdash d \in b \qquad \text{(b}\forall\text{E)}$$

and (3) holds by ($\#$I2) from

$$d = c,\ d \in a \# c,\ a \subseteq b \vdash d = c \qquad \text{(id)}.$$

(viii) comes easily from (vii).
(ix) It suffices to prove

(4) $$d \in c \# a,\ a = b \vdash d \in c \# b.$$

But it is obvious that

$$d \in c,\ d \in c \# a,\ a = b \vdash d \in c \# b.$$

and also we have

$$d=a,\ d\in c\# a,\ a=b\vdash d\in c\# b,$$

since

$$d=a,\ d\in c\# a,\ a=b\vdash d=b,$$

by (v) and Theorem 4.1 (iii). Thus we have (4).

(x) We make use of (PI), the inference of primitive induction. Let $A(c)$ be the formula $a\in c\rightharpoonup b\in c$.
By (PI), to prove (x) it suffices to prove

(5) $$a=b\vdash a\in 0\rightharpoonup b\in 0$$

and

(6) $$a\in d\rightharpoonup b\in d,\ a\in e\rightharpoonup b\in e,\ a=b\vdash a\in d\# e\rightharpoonup b\in d\# e.$$

(5) follows from $a\in 0,\ a=b\vdash b\in 0$ (0E).
(6) follows (by ($\rightharpoonup$I) and ($\#$E)) from

(7) $$a\in d,\ a\in d\rightharpoonup b\in d,\ a\in e\rightharpoonup b\in e,\ a=b\vdash b\in d\# e$$

and

(8) $$a=e,\ a\in d\rightharpoonup b\in d,\ a\in e\rightharpoonup b\in e,\ a=b\vdash b\in d\# e.$$

(7) comes easily from $a\in d,\ a\in d\rightharpoonup b\in d\vdash b\in d$,
and (8) from $a=e,\ a=b\vdash b=e$ and $b=e\vdash b\in d\# e$. **q.e.d.**

Theorem 4.4.
(i) $a=b\vdash r(a/x)=r(b/x)$,
(ii) $a=b,\ D(a/x)\vdash D(b/x)$,
where $V(r)\cap\mathbf{B}\subseteq\{x\}$ *and* $V(D)\cap\mathbf{B}\subseteq\{x\}$.

Outline of proof. (i). We prove (i) by the induction on the length of r. The induction can easily be carried out using Theorem 4.1 (viii) and (ix) as well as the facts

$$a=b\vdash a=b,$$

$$a=b\vdash v=v,$$

$$a=b\vdash 0=0.$$

(ii). If we prove the theorem for prime formula D, then by the induction on the length of D we can easily prove theorem for all D. Thus it suffices to prove

$$a=b, \quad r(a/x)\in s(a/x)\vdash r(b/x)\in s(b/x)$$

But it is easy to infer it using (i) and **T.4.3** (vi), (x).

Theorem 4.5. *If* $z\notin V(A)$, *then*

(i) $\exists x\exists yA(x, y)\dashv\vdash\exists z\exists x\in z\exists y\in zA(x, y)$,

(ii) $\forall x\in a\exists yA(x, y)\dashv\vdash\exists z\forall x\in a\exists y\in zA(x, y)$,

and more precisely,

(iii) $\forall x\in a\exists yA(x, y)\dashv\vdash\exists z(\forall x\in a\exists y\in zA(x, y)\wedge\forall y\in z\exists x\in aA(x, y))$.

Outline of proof. (i) is obvious from

$$A(a, b)\vdash\exists x\in(0\# a)\# b\exists y\in(0\# a)\# bA(x, y).$$

We prove (iii). Let $B(b, c)$ be the formula

$$\forall x\in b\exists y\in cA(x, y)\wedge\forall y\in c\exists x\in bA(x, y),$$

and $C(b)$ be the formula $b\subseteq a\rightharpoonup\exists zB(b, z)$.

If we prove

(9) $$\forall x\in a\exists yA(x, y)\vdash C(0)$$

and

(10) $$C(d),\ C(e),\ \forall x\in a\exists yA(x, y)\vdash C(d\# e),$$

then by (PI) we have

$$\forall x\in a\exists yA(x, y)\vdash C(a),$$

that is,

$$\forall x\in a\exists yA(x, y)\vdash a\subseteq a\rightharpoonup\exists zB(a, z),$$

from which we have (iii).

(9) is obvious since $\vdash B(0, 0)$.

(10) can be proved thus:

First we can easily have

$$B(b_1, c_1), A(b_2, d) \vdash B(b_1 \# b_2, c_1 \# d).$$

So we have

$$\forall x \in a \exists y A(x, y), b_1 \# b_2 \subseteq a, B(b_1, c_1) \vdash \exists z B(b_1 \# b_2, z).$$

Thus

$$\forall x \in a \exists y A(x, y), b_1 \# b_2 \subseteq a, b_1 \subseteq a \rightharpoonup B(b_1, c_1) \vdash \exists z B(b_1 \# b_2, z).$$

Hence

$$\forall x \in a \exists y A(x, y), C(b_1) \vdash b_1 \# b_2 \subseteq a \rightharpoonup \exists z B(b_1 \# b_2, z).$$

Hence

$$\forall x \in a \exists y A(x, y), C(b_1) \vdash C(b_1 \# b_2).$$

Hence by Theorem 4.1 (iii) we have (10). **q.e.d.**

5. Some Set-Theoretic Operations

In order to treat elementary set-theoretic operations in FCS, we shall make the following observation. Let us consider, for example, the operation of set-theoretic union $\cup$. The fact that $c = a \cup b$ can be expressed in the language of FCS as

$$\forall x \in a(x \in c) \wedge \forall x \in b(x \in c) \wedge \forall x \in c(x \in a \vee x \in b).$$

Let us call this formula $C_\cup(c, a, b)$. Then for fixed a and b, the existence and the uniqueness of c satisfying $C_\cup(c, a, b)$ are expressed by

(1) $$\vdash \exists x C_\cup(x, a, b),$$

and

(2) $$C_\cup(c_1, a, b), C_\cup(c_2, a, b) \vdash c_1 = c_2.$$

They are of course provable in FCS. The uniqueness proof is easy. For the existence proof we make use of the inference of primitive induction on account of the facts

$$a \cup 0 = a \quad \text{and} \quad a \cup (b_1 \# b_2) = (a \cup b_1) \# b_2 .$$

To be more detailed let $A(b)$ be the $\sum$F: $\exists x C_{\cup}(x, a, b)$, which we want to prove. Then by the primitive induction it suffices to prove

$$(3) \qquad \vdash A(0)$$

and

$$(4) \qquad A(b_1), A(b_2) \vdash A(b_1 \# b_2) .$$

(3) follows from $C_{\cup}(a, a, 0)$ and (4) follows from

$$C_{\cup}(c_1, a, b), C_{\cup}(c_2, a, b) \vdash C_{\cup}(c_1 \# b_2, a, b_1 \# b_2) .$$

But these are obvious.

As for the power set operation, the fact "$b = \mathrm{P}(a)$" does not seem at first glance to be able to be expressed by a $\sum$F. (The standard description of it is $\forall x \in b(x \subseteq a) \wedge \forall x(x \subseteq a \rightarrow x \in b)$, which is not a $\sum$F.) But if we notice that a is a finite set, we can easily express "$b = \mathrm{P}(a)$" by a $\sum$F (indeed, by a RF) as follows:

$$\forall x \in b(x \subseteq a) \wedge 0 \in b \wedge \forall x \in b \forall y \in a(x \# y \in b) .$$

Call this formula $C_{\mathrm{P}}(b, a)$. Also in this case

$$\vdash \exists z C_{\mathrm{P}}(z, a) \quad \text{and} \quad C_{\mathrm{P}}(b_1, a), C_{\mathrm{P}}(b_2, a) \vdash b_1 = b_2$$

are provable. Although the uniqueness proof is easy, the existence proof is more complicated than the previous one. We must use the primitive induction twice. The proof is motivated from the following equations:

$$\mathrm{P}(0) (= \{0\}) = 0 \# 0,$$

$$\mathrm{P}(a_1 \# a_2) = \mathrm{P}(a_1) \cup \{x \# a_2 | x \in \mathrm{P}(a_1)\} .$$

Roughly speaking, we first *define* $\mathrm{Q}(c, d) = \{x \# d | x \in c\}$ in FCS by the equations:

$$Q(0,\ d)=0,$$

$$Q(c_1 \# c_2,\ d)(=Q(c_1,\ d) \cup \{c_2 \# d\})=Q(c_1,\ d) \# (c_2 \# d),$$

and then *define* $P(a)$, using the above, by

$$P(0)=0 \# 0$$

$$P(a_1 \# a_2)=P(a_1) \cup Q(P(a_1),\ a_2).$$

More precisely we procced as follows. Let $C_Q(e,\ c,\ d)$ be the RF

$$\forall x \in c(x \# d \in e) \wedge \forall y \in e \exists x \in c(x \# d = y).$$

The existence and the uniqueness condition are:

(5) $\vdash \exists u C_Q(u,\ c,\ d)$ and $C_Q(e_1,\ c,\ d),\ C_Q(e_2,\ c,\ d) \vdash e_1=e_2$.

The former follows, by the primitive induction, from

(i) $C_Q(0,\ 0,\ d)$,

and

(ii) $C_Q(e_1,\ c_1,\ d),\ C_Q(e_2,\ c_2,\ d) \vdash C_Q(e_1 \# (c_2 \# d),\ c_1 \# c_2,\ d)$.

The latter also follows easily.

Now that (5) has been proved, we can prove, using the primitive induction again, the existence and the uniqueness condition thus:

(i) $C_P(0 \# 0,\ 0)$,

(ii) $C_P(b_1,\ a_1),\ C_P(b_2,\ a_2),\ C_Q(e,\ b_1,\ a_2),\ C_U(f,\ b_1,\ e) \vdash C_P(f,\ a_1 \# a_2)$.

Moreover we can prove

T.5.1. $C_P(b,\ a) \vdash c \subseteq a \rightleftharpoons c \in b$.

We need to show

(i) $C_P(b,\ a) \vdash c \subseteq a \rightharpoonup c \in b$,

and

(ii) $C_P(b,\ a) \vdash c \in b \rightharpoonup c \subseteq a$.

(ii) is obvious by the definition of C_P.

(i) follows, by the primitive induction on c for the formula $c \subseteq a \rightharpoonup c \in b$, from

$$C_P(b, a) \vdash 0 \subseteq a \rightharpoonup 0 \in b,$$

and

$$C_P(b, a),\ c_1 \subseteq a \rightharpoonup c_1 \in b \vdash c_1 \# c_2 \subseteq a \rightharpoonup c_1 \# c_2 \in b.$$

Both of these are easily proved.

6. The Existence and the Uniqueness Condition

Now we turn to the general treatment of the existence and the uniqueness condition. Let D be a $\sum$F′ such that $V(A) \cap \mathbf{B} \subseteq \{x\}$. Then $\exists x D$ is a Σ-formula which expresses the existence condition for D. The standard expression for the uniqueness condition for D, that is, $D(a_1/x) \wedge D(a_2/x) \rightharpoonup a_1 = a_2$, is however not a Σ-formula. Instead of it we use the condition

(1) $D(a_1/x),\ D(a_2/x) \vdash a_1 = a_2$,

where a_1 and a_2 are distinct free variables not occurring in D. The existence condition is of course $\vdash \exists x D$. To clarify impression these conditions are abbreviated $\exists ! x D$. If we please, these conditions could be relativized to the assumption Γ.

Remark. We can find a Σ-formula whose derivability is equivalent to (1). Such a formula is obtained as follows.

Let C be a free variable not occurring in D and distinct from a_1 and a_2 (a_1 and a_2 are as above), and let D_c be the RF obtained from D by replacing each occurrence of unbounded quantifier $\exists y$ by bounded quantifier $\exists y \in c$. Then the desired formula is

(2) $D_c(a_1/x) \wedge D_c(a_2/x) \rightharpoonup a_1 = a_2$.

To prove the equivalence mentioned, we make use of the following facts, whose intended meaning might be clear and which will be used later again.

Theorem 6.1. *Let A be a $\sum$F, let c, c_1, c_2 be distinct free variables not occurring in A and let y be a bound variable not occurring in A. Then*

(i) $c_1 \subseteq c_2,\ A_{c_1} \vdash A_{c_2}$.

(ii) $A_c \vdash A$, *(or equivalently,* $\vdash A_c \rightharpoonup A$*)*

(iii) $A \dashv\vdash \exists y A_y$.

We show that the equivalence mentioned above is an easy consequence of this last theorem.

Suppose first that (2) is derivable. Since

$$D(a_1/x) \vdash \exists y_1 D_{y_1}(a_1/x) \quad \text{and} \quad D(a_2/x) \vdash \exists y_2 D_{y_2}(a_2/x),$$

by (iii) of Theorem 6.1, where $y_1,\ y_2 \in \mathbf{B} - V(D)$, we have

$$D(a_1/x),\ D(a_2/x) \vdash \exists y(D_y(a_1/x) \wedge D_y(a_2/x)),$$

by (i) of Theorem 6.1 (Intuitively take y to be $y_1 \cup y_2$, for instance.) From this and the hypothesis we obtain (1).

Suppose next that we have (1). By (ii) of Theorem 6.1 we have

$$D_c(a_1/x) \wedge D_c(a_2/x) \vdash D(a_1/x) \wedge D(a_2/x).$$

From this and the hypothesis we see (2) is derivable.

We now prove Theorem 6.1. (i) and (ii) can be proved by using the induction on the length of formula A on account of the facts

$$c_1 \subseteq c_2,\ \exists x \in c_1 C(x) \vdash \exists x \in c_2 C(x),$$

and

$$\exists x \in c C(x) \vdash \exists x C(x).$$

As for (iii), $\exists y A_y \vdash A$ is an immediate consequence of (ii). We also prove $A \vdash \exists y A_y$ by the induction on A.

1°. If A is a restricted formula, then the assertion is clear since

A_y is just A.

2°. If A is $B \vee C$, then the assertion comes from the fact

$$\exists u B_u \vee \exists v C_v \dashv\vdash \exists y(B_y \vee C_y),$$

as well as the induction hypothesis.

3°. If A is $B \wedge C$, then the assertion comes from the fact

$$\exists u B_u \wedge \exists v C_v \dashv\vdash \exists y(B_y \wedge C_y),$$

(by (i) of Theorem 6.1), as well as the induction hypothesis.

4°. If A is $\exists x \in sB$, then the assertion comes from the fact

$$\exists x \in s \exists y B_y(x) \dashv\vdash \exists y \exists x \in s B_y(x)$$

and the fact that $\exists x \in s(B_y)$ is just $(\exists x \in sB)_y$, as well as the induction hypothesis.

5°. If A is $\exists x B$, then the assertion is proved similarly to the previous case.

6°. If A is $\forall x \in sB$, the assertion is proved as follows. By (ii) of Theorem 4.5,

$$\forall x \in s \exists u B_u(x) \dashv\vdash \exists v \forall x \in s \exists u \in v B_u(x).$$

So if we prove

$$(3) \quad \exists v \forall x \in s \exists u \in v B_u(x) \vdash \exists y \forall x \in s B_y(x),$$

we have the assertion. Let $C_{\cup}(d, c)$ be the formula

$$\forall x \in d \exists y \in c(x \in y) \wedge \forall y \in c \forall x \in y(x \in d).$$

This formula expresses the fact that $d = \cup c = \{u | \exists y \in c(u \in y)\}$. The existence and the uniqueness condition that

$$\vdash \exists z C_{\cup}(z, c) \quad \text{and} \quad C_{\cup}(d_1, c), C_{\cup}(d_2, c) \vdash d_1 = d_2$$

can be proved as in 5. Since

$$C_{\cup}(d, c) \vdash \forall x \in c(x \subseteq d),$$

we have, using (i) of Theorem 6.1,

$$\forall x \in s \exists u \in c B_u(x), \quad C_{\mathrm{U}}(d, c) \vdash \forall x \in s B_d(x).$$

From this and the existence condition for C_{U} we obtain (3). This completes the proof of Theorem 6.1. **q.e.d.**

7. Alternative Versions of Induction Principle

Let Trans(z) ("Trans" for transitive) be the RF′: $\forall x \in z \forall y \in x (y \in z)$. Then we have

T.7.1. $\exists z (a \in z \wedge \mathrm{Trans}(z))$.

Proof. Let $A(a)$ be the $\sum$F to be proved. We prove it by the primitive induction. It suffices to show

(i) $\vdash A(0)$

and

(ii) $A(a_1), A(a_2) \vdash A(a_1 \# a_2)$.

(i) follows from

$$0 \in 0 \# 0 \wedge \mathrm{Trans}(0 \# 0).$$

and (ii) from

$$a_1 \in b_1 \wedge \mathrm{Trans}(b_1),\ a_2 \in b_2 \wedge \mathrm{Trans}(b_2),\ C_{\mathrm{U}}(c, b_1, b_2)$$
$$\vdash a_1 \# a_2 \in c \# (a_1 \# a_2) \wedge \mathrm{Trans}(c \# (a_1 \# a_2)),$$

by (1) in the section 5. **q.e.d.**

The following versions of induction principle hold:

Theorem 7.2. (i) *If* $\forall x \in a A(x), \Gamma \vdash A(a)$, *where* a *occurs neither in* A *nor in* Γ, *then* $\Gamma \vdash A(t)$, *where* t *is any term.*

(ii) *If* $\forall x \in a \forall y \in b A(x, y), \Gamma \vdash A(a, b)$, *where* a *and* b *are distinct free variables occurring neither in* A *nor in* Γ, *then* $\Gamma \vdash A(s, t)$, *where* s *and* t *are terms.*

(iii) *If* $\forall x \in a A(x, b), \forall y \in b A(a, y), \Gamma \vdash A(a, b)$, *with the same restric-*

tion on a, b as above, then $\Gamma \vdash A(s, t)$.

Proof. (i) Suppose that $\forall x \in aA(x), \Gamma \vdash A(a)$, where a occurs neither in A nor in Γ. If we have

(1) $\Gamma \vdash \forall x \in 0A(x)$,

and

(2) $\forall x \in b_1A(x), \forall x \in b_2A(x), \Gamma \vdash \forall x \in b_1 \# b_2A(x)$,

where b_1 and b_2 are *new* free variables, then we shall have

$$\Gamma \vdash \forall x \in t \# tA(x),$$

by the primitive induction and hence have, by (b$\forall$E),

$$\Gamma \vdash A(t),$$

since $\vdash t \in t \# t$.

So it suffices to prove (1) and (2). But (1) is obvious (use (0E) and (b$\forall$I)). In order to obtain (2) it will suffice to show

(3) $c \in b_1 \# b_2, \forall x \in b_1A(x), \forall x \in b_2A(x) \vdash A(c)$.

But obviously, we have

(4) $c \in b_1, \forall x \in b_1A(x), \forall x \in b_2A(x), \Gamma \vdash A(c)$.

Moreover, by hypothesis (using the substitution theorem (Theorem 4.1 (ii))) we have

$$\forall x \in b_2A(x), \Gamma \vdash A(b_2).$$

From this and the equality theorem (Theorem 4.4) we have

(5) $c = b_2, \forall x \in b_1A(x), \forall x \in b_2A(x), \Gamma \vdash A(c)$.

Now (3) follows from (4) and (5) by ($\#$E).

(ii) Suppose that

$$\forall x \in a \forall y \in bA(x, y), \Gamma \vdash A(a, b).$$

We easily have

$$\mathrm{Trans}(c),\ b \in c,\ \forall x \in a \forall z \in c A(x, z),\ \Gamma \vdash \forall x \in a \forall y \in b A(x, y).$$

It follows from the last two facts that

$$\mathrm{Trans}(c),\ b \in c,\ \forall x \in a \forall z \in c A(x, z),\ \Gamma \vdash A(a, b).$$

Hence by (b∀I),

$$\forall x \in a \forall z \in c A(x, z),\ \mathrm{Trans}(c),\ \Gamma \vdash \forall z \in c A(a, z).$$

Then we can make use of (i) of this theorem to show

$$\mathrm{Trans}(c),\ \Gamma \vdash \forall z \in c A(a, z).$$

From this by (b∀E) we have

$$b \in c,\ \mathrm{Trans}(c),\ \Gamma \vdash A(a, b).$$

Now $\Gamma \vdash A(a, b)$ follows from **T.4.3**, by (∃E). Finally, by the substitution theorem we have $\Gamma \vdash A(s, t)$.

(iii) We have

$$b \in c,\ \forall x \in a \forall y \in c A(x, y) \vdash \forall x \in a A(x, b),$$

and

$$b \in c,\ \mathrm{Trans}(c),\ \forall y \in b (y \in c \rightharpoonup A(a, y)) \vdash \forall y \in b A(a, y).$$

Hence by the assumption

$$b \in c,\ \forall x \in a \forall y \in c A(x, y),\ \mathrm{Trans}(c),\ \forall y \in b(y \in c \rightharpoonup A(a, y)),$$
$$\Gamma \vdash A(a, b).$$

Hence

$$\forall x \in a \forall y \in c A(x, y),\ \mathrm{Trans}(c),\ \forall y \in b(y \in c \rightharpoonup A(a, y)),$$
$$\Gamma \vdash b \in c \rightharpoonup A(a, b).$$

By (i) of the theorem we obtain

$$\forall x \in a \forall y \in c A(x, y),\ \mathrm{Trans}(c),\ \Gamma \vdash b \in c \rightharpoonup A(a, b).$$

By (b∀I),

$$\forall x \in a \forall y \in c A(x, y), \text{Trans}(c), \Gamma \vdash \forall y \in c A(a, y).$$

By (i) of theorem again,

$$\text{Trans}(c), \Gamma \vdash \forall y \in c A(a, y).$$

But since $\vdash \exists c(b \in c \wedge \text{Trans}(c))$, we have

$$\Gamma \vdash A(a, b).$$

So we have (iii) by substitution. **q.e.d.**

8. The Law of the Excluded Middle

Let us recall here that the underlying logic for FCS is intuitionistic but not classical, and so the law of the excluded middle cannot be asserted from the outset. It cannot even be stated. (Recall that the negation of Σ-formula is not always a Σ-formula.)

However, as is expected, for restricted formulas this law can be stated of course and does hold!

Theorem 8.1. *For each* RF φ, *we have*

$$\vdash \varphi \vee \neg \varphi.$$

To prove this we shall make use of the following two lemmas.

Lemma 8.1.1. *For* RF's φ *and* ψ *we have*

(i) $\varphi \vee \neg \varphi \vdash \neg \varphi \vee \neg \neg \varphi$,

(ii) $\varphi \vee \neg \varphi, \psi \vee \neg \psi \vdash (\varphi \wedge \psi) \vee \neg(\varphi \wedge \psi)$,

(iii) $\varphi \vee \neg \varphi, \psi \vee \neg \psi \vdash (\varphi \vee \psi) \vee \neg(\varphi \vee \psi)$,

(iv) $\forall x \in a(\varphi(x) \vee \neg \varphi(x)) \vdash \forall x \in a \varphi(x) \vee \neg \forall x \in a \varphi(x)$,

(v) $\forall x \in a(\varphi(x) \vee \neg \varphi(x)) \vdash \exists x \in a \varphi(x) \vee \neg \exists x \in a \varphi(x)$.

Proof. (i)–(iii) are tautologies of the intuitionistic propositional calculus. To obtain (iv) we shall prove

$$\vdash \forall x \in a(\varphi(x) \vee \neg \varphi(x)) \rightarrow (\forall x \in a \varphi(x) \vee \neg \forall x \in a \varphi(x)),$$

by the primitive induction on a. Then we shall readily have (iv). Let

$\chi(a)$ be the formula to be proved. Then it suffices to show

$$(1)\quad \vdash\chi(0) \text{ and } (2)\ \chi(a_1)\vdash\chi(a_1 \# a_2).$$

(1) follows from the fact that $\vdash\forall x\in 0\varphi(x)$, by ($\vee$I1) and ($\neg$I). On the other hand (2) will follow from the following facts

$$(3)\quad \forall x\in a_1\# a_2(\varphi(x)\vee\neg\varphi(x))\dashv\vdash\forall x\in a_1(\varphi(x)\vee\neg\varphi(x))\wedge(\varphi(a_2)\vee\neg\varphi(a_2)),$$

$$(4)\quad \forall x\in a_1\# a_2\varphi(x)\dashv\vdash\forall x\in a_1\varphi(x)\wedge\varphi(a_2).$$

Indeed from (3) we have

$$\forall x\in a_1\# a_2(\varphi(x)\vee\neg\varphi(x)),$$
$$\chi(a_1)\vdash(\forall x\in a_1\varphi(x)\vee\neg\forall x\in a_1\varphi(x))\wedge(\varphi(a_2)\vee\neg\varphi(a_2)).$$

Hence by (ii) of this lemma

$$\forall x\in a_1\# a_2(\varphi(x)\vee\neg\varphi(x)),$$
$$\chi(a_1)\vdash(\forall x\in a_1\varphi(x)\wedge\varphi(a_2))\vee\neg(\forall x\in a_1\varphi(x)\wedge\varphi(a_2)).$$

So by (4) we obtain

$$\forall x\in a_1\# a_2(\varphi(x)\vee\neg\varphi(x)),\ \chi(a_1)\vdash\forall x\in a_1\# a_2\varphi(x)\vee\neg\forall x\in a_1\# a_2\varphi(x),$$

from which (2) surely follows.

As for (v) we can prove it similarly to the previous case.

Lemma 8.1.2. (i) $\vdash a=b\vee a\neq b$.

(ii) $\vdash a\in b\vee a\notin b$.

($a\neq b$ and $a\notin b$ are of course abbreviations of $\neg(a=b)$ and $\neg(a\in b)$ respectively.)

Proof. To prove (i) we utilize the induction principle of Theorem 7.2 (ii). We have only to show

$$\forall x\in a\forall y\in b(x=y\vee x\neq y)\vdash a=b\vee a\neq b.$$

This comes from the fact that

$$a=b\rightleftarrows(\forall x\in a\exists y\in b(x=y)\wedge\forall y\in b\exists x\in a(x=y))$$

with repeated use of the previous lemma. (ii) then follows from (i) and the fact

$$\vdash a \in b \rightleftharpoons \exists z \in b(a = z)$$

together with the previous lemma. **q.e.d.**

Proof of Theorem 8.1. We prove the theorem by the metamathematical induction on the length of φ. But this can easily be carried out using the previous two lemmas. **q.e.d.**

Corollary 8.2. *For restricted formula* $\varphi(a)$, *we have*

(i) $\rightharpoondown \forall x \in a\varphi(x) \rightleftharpoons \exists x \in a \rightharpoondown \varphi(x)$,

(ii) $\rightharpoondown \exists x \in a\varphi(x) \rightleftharpoons \forall x \in a \rightharpoondown \varphi(x)$,

(iii) $\rightharpoondown \rightharpoondown \varphi \rightleftharpoons \varphi$,

(iv) $\varphi \vdash \psi$ *iff* $\rightharpoondown \psi \vdash \rightharpoondown \varphi$.

By the same method as used to prove Lemma 8.1.1, we can prove

Theorem 8.3. (i) $\forall x \in a(A(x) \vee B(x)) \vdash \forall x \in aA(x) \vee \exists x \in aB(x)$.

(ii) $\forall x \in a\forall y \in b(A(x, y) \vee B(x, y)) \vdash \forall x \in a\exists y \in bA(x, y) \vee \exists x \in a\forall y \in bB(x, y)$.

Proof. We shall prove by the primitive induction on b that

$$\forall x \in a(A(x) \vee B(x)) \vdash b \subseteq a \rightharpoonup \forall x \in bA(x) \vee \exists x \in bB(x).$$

Then (i) follows by taking a as b. It suffices to prove

$$\forall x \in a(A(x) \vee B(x)),\ b_1 \subseteq a \rightharpoonup \forall x \in b_1A(x) \vee \exists x \in b_1B(x)$$
$$\vdash b_1 \# b_2 \subseteq a \rightharpoonup \forall x \in b_1 \# b_2A(x) \vee \exists x \in b_1 \# b_2B(x).$$

This follows from

$$b_1 \# b_2 \subseteq a \vdash b_1 \subseteq a \wedge b_2 \in a,$$

$$\forall x \in a(A(x) \vee B(x)),\ b_2 \in a \vdash A(b_2) \vee B(b_2),$$

$$\forall x \in b_1A(x) \vee \exists x \in b_1B(x),\ A(b_2) \vee B(b_2) \vdash \forall x \in b_1 \# b_2A(x)$$

$$\vee \exists x \in b_1 \# b_2 B(x).$$

(ii) can be proved by using (i) twice:

$$\forall x \in a \forall y \in b(A(x, y) \vee B(x, y))$$
$$\vdash \forall x \in a(\exists y \in bA(x, y) \vee \forall y \in bB(x, y))$$
$$\vdash \forall x \in a \exists y \in bA(x, y) \vee \exists x \in a \forall y \in bB(x, y).$$

q.e.d.

9. Δ-Formulas

It would be interesting to consider how one can describe the situation that the law of the excluded middle virtually holds for a Σ-formula A which is not necessarily a restricted formula. We shall do this by the use of pairs of Σ-formulas.

Definition 9.1. A pair (A, B) of Σ-formula is called a Δ-formula (abbreviated ΔF), if

$$\vdash A \vee B \quad \text{and} \quad A \wedge B \vdash \curlywedge,$$

where $\curlywedge$ is an identically false formula, e.g. $0 \in 0$.

Thus, saying that (A, B) is a Δ-formula is that the Σ-formula A has the negation which is provably equivalent of another Σ-formula B.

For example, let φ be a restricted formula. Then both φ and $\neg\varphi$ are Σ-formulas and we have

$$\vdash \varphi \vee \neg\varphi \quad \text{and} \quad \varphi \wedge \neg\varphi \vdash \curlywedge.$$

Hence the pair $(\varphi, \neg\varphi)$ is a Δ-formula. Similarly $(\neg\varphi, \varphi)$ is also a Δ-formula. Moreover we have

Theorem 9.1. (i) *If (A_1, B_1) and (A_2, B_2) are Δ-formulas, then so are (B_1, A_1), $(A_1 \wedge A_2, B_1 \vee B_2)$ and $(A_1 \vee A_2, B_1 \wedge B_2)$, which we shall denote by $\neg(A_1, B_1)$, $(A_1, B_1) \wedge (A_2, B_2)$ and $(A_1, B_1) \vee (A_2, B_2)$ respectively.*

(ii) *Suppose that A and B are $\sum$F''s such that $V(A) \cap \mathbf{B}$, $V(B) \cap \mathbf{B} \subseteq \{x\}$, that $a \notin V(A) \cup V(B)$ and that t is a term. Then if $(A(a/x)$,*

$B(a/x)$) is a ΔF, *so are* $(A(t/x), B(t/x))$, $(\exists x \in tA(x), \forall x \in tB(x))$ *and* $(\forall x \in tA(x), \exists x \in tB(x))$, *which we shall denote* $(A, B)(t/x)$, $\exists x \in t(A, B)$ *and* $\forall x \in t(A, B)$, *respectively.*

Proof. (i) If (A_1, B_1) and (A_2, B_2) are Δ-formulas, we have by definition,

$$\vdash A_1 \vee B_1,\ A_1 \wedge B_1 \vdash \curlywedge,\ \vdash A_2 \vee B_2,\ A_2 \wedge B_2 \vdash \curlywedge.$$

Now the first two results follow from the following tautologies:

$$A_1 \vee B_1 \vdash B_1 \vee A_1,$$

$$B_1 \wedge A_1 \vdash A_1 \wedge B_1,$$

$$A_1 \vee B_1,\ A_2 \vee B_2 \vdash (A_1 \wedge A_2) \vee (B_1 \vee B_2),$$

$$B_1,\ A_1 \wedge A_2 \vdash A_1 \wedge B_1,$$

$$B_2,\ A_1 \wedge A_2 \vdash A_2 \wedge B_2,$$

The last result of (i) follows similarly.

(ii) Suppose that $(A(a), B(a))$ is a ΔF. Then by substitution theorem we easily have that $(A(t), B(t))$ is also a ΔF. To prove that $(\exists x \in tA(x), \forall x \in tB(x))$ is a ΔF, use Theorem 8.3. **q.e.d.**

Definition 9.2. For a ΔF $(A(a), B(a))$, we define $\exists x(A(x), B(x))$ to be the $\sum$F: $\exists x A(x)$.

Theorem 9.2. (i) $A \wedge B \vdash \curlywedge$ *iff* $\neg(A_c \wedge B_c)$, *where c is a free variable occurring neither in A nor in B.*

(ii) *If (A, B) is a* ΔF, *then $A \vdash \curlywedge$ iff $\vdash B$ (and $B \vdash \curlywedge$ iff $\vdash A$).*

(iii) *If (A_1, B_1) and (A_2, B_2) are* ΔF's, *then*

$$A_1 \vdash A_2 \text{ iff } B_2 \vdash B_1,$$

and hence

$$A_1 \dashv\vdash A_2 \text{ iff } B_1 \dashv\vdash B_2,$$

(If the latter is the case we may write $(A_1, B_1) \dashv\vdash (A_2, B_2)$.)

The proof of this theorem is obvious and hence is omitted here.

The notion of Δ-formulas can be generalized to the notion of partition.

Definition 9.3. An n-tuple $(A_1,\ldots, A_n)$ of $\sum$F's is a partition (an n-partition) iff

$$\vdash A_1 \vee \cdots \vee A_n$$

and

$$A_i \wedge A_j \vdash \text{⅄} \qquad \text{for all} \quad i, j=1,\ldots, n;\ i \neq j.$$

Theorem 9.3. *If* $(A_1,\ldots, A_n)$ *is a partition and if* $\{i_1,\ldots, i_k\} \cup \{j_1,\ldots, j_s\} = \{1,\ldots, n\}$, *where* $i_1,\ldots, i_k, j_1,\ldots, j_s$ *are distinct, then*

$$(A_{i_1} \vee \cdots \vee A_{i_k},\ A_{j_1} \vee \cdots \vee A_{j_s})$$

is a ΔF (2-partition).

(ii) *If* $(A_1,\ldots, A_n)$ *and* $(B_1,\ldots, B_m)$ are partitions, then

$$(A_1 \wedge B_1,\ A_1 \wedge B_2,\ldots, A_n \wedge A_m)$$

is a partition.

(iii) *If* $(A_1, B_1),\ldots, (A_n, B_n)$ *are* ΔF'*s, then* $(A_1, B_1 \wedge A_2, B_1 \wedge B_2 \wedge A_3,\ldots, B_1 \wedge B_2 \wedge \cdots \wedge B_{n-1} \wedge A_n, B_1 \wedge B_2 \wedge \cdots \wedge B_{n-1} \wedge B_n)$ *constitutes an* $(n+1)$-*partition.*

10. Expansion by Definition of Predicates

Let (C, D) be a ΔF such that $V(C) \cup V(D) \subseteq \{a_1,\ldots, a_n\}$. Then we can expand the system FCS (or an expansion of FCS) by introducing a new predicate symbol, say **P**, and letting

$$C(a_1,\ldots, a_n) \vdash \mathbf{P}(a_1,\ldots, a_n)$$

and

$$D(a_1,\ldots, a_n) \vdash \neg \mathbf{P}(a_1,\ldots, a_n)$$

as defining postulates. (Then we easily have the converse directions

$$\mathbf{P}(a_1,\dots, a_n) \vdash C(a_1,\dots, a_n)$$

and

$$\neg\mathbf{P}(a_1,\dots, a_n) \vdash D(a_1,\dots, a_n),$$

since (C, D) is a ΔF.)

This kind of expansion can of course be repeated and it is strongly conservative in the sense that (i) each Σ-formula in the expanded language is equivalent to a Σ-formula in the previous language and (ii) the derivability of Σ-formulas in the previous language does not alter through this expansion, i.e., if Γ is a finite set of $\sum$F's in the previous language and A a $\sum$F *in the previous language*, then $\Gamma \vdash A$ in the expanded language, iff $\Gamma \vdash A$ in the previous language. (We say an expansion is conservative if (ii) is satisfied.) Since this kind of expansion is not so standard, we shall outline the proof of this fact below. For convenience' sake we refer to the expanded system as FCS$'$.

We shall first describe FCS$'$ a bit more precisely. Semi-terms and terms of FCS$'$ are the same as those of FCS. RF$'$ in FCS$'$ is defined by adding to the corresponding definition in FCS the following clause:

(v)$_{\mathbf{P}}$ If $t_1,\dots, t_n$ are semi-terms, then $\mathbf{P}t_1\cdots t_n$ is a RF$'$. (Instead of $\mathbf{P}t_1\cdots t_n$ we also write $\mathbf{P}(t_1,\dots, t_n)$.) The definition of $\sum$F$'$ in FCS$'$ is the same as before up to the meaning of RF$'$. Note that according to definition $\neg\mathbf{P}(t_1,\dots, t_n)$ is RF$'$ and hence $\sum$F$'$ in our new sense while $\neg C(t_1,\dots, t_n)$ is neither RF$'$ nor $\sum$F$'$ in our old sense although these two formulas are intuitively equivalent.

Moreover we define

$$V(\mathbf{P}t_1\cdots t_n) = V(t_1) \cup \cdots \cup V(t_n),$$

in addition to the corresponding definition of V in FCS. Then RF and $\sum$F are defined as in FCS. The substitution is defined with

$$\mathbf{P}t_1\cdots t_n(r/v) \asymp \mathbf{P}t_1(r/v)^\frown\cdots{}^\frown t_n(r/v),$$

in addition to the previous cases. The notion of derivation $P\colon \Gamma \vdash A$ is defined as before with the additional clauses:

$(\mathrm{xxii})_{\mathbf{P}}$ If $P\colon \Gamma \vdash C(t_1,\ldots, t_n)$, then $\dfrac{P}{\mathbf{P}(t_1,\ldots, t_n)}\colon \Gamma \vdash \mathbf{P}(t_1, t_n)$,

and

$(\mathrm{xxiii})_{\mathbf{P}}$ If $P\colon \Gamma \vdash D(t_1,\ldots, t_n)$, then $\dfrac{P}{\neg\mathbf{P}(t_1,\ldots, t_n)}\colon \Gamma \vdash \neg\mathbf{P}(t_1,\ldots, t_n)$.

Now we prove

Theorem 10.1. *The expansion from* FCS *to* FCS′ *is conservative.*

Proof. Let $v_0, v_1,\ldots$ be the list of bound variables and let m be such that bound variables occurring in C and D are among $v_0, v_1,\ldots, v_{m-1}$. Then we define $[t]_{+m}$ for each semi-term t in FCS′ by $[0]_{+m}\asymp 0$, $[v_i]_{+m}\asymp v_{i+m}$, $[a]_{+m}\asymp a$ (a: free variable) and $[\# st]_{+m}\asymp \#\frown[s]_{+m}\frown[t]_{+m}$.

We first assign to each RF′ φ in FCS′, a pair of $\sum$F′ in FCS, $\langle\varphi\rangle=([\varphi]_+, [\varphi]_-)$ as follows:

1°. $\langle \in st\rangle=(\in\frown[s]_{+m}\frown[t]_{+m}, \neg\in\frown[s]_{+m}\frown[t]_{+m})$,
2°. $\langle \mathbf{P}t_1\cdots t_n\rangle=(C([t_1]_{+m},\ldots, [t_n]_{+m}), D([t_1]_{+m},\ldots, [t_n]_{+m}{}^{*}))$,
3°. $\langle\neg\varphi\rangle=([\varphi]_-, [\varphi]_+)$,
4°. $\langle \vee\varphi\psi\rangle=(\vee\frown[\varphi]_+\frown[\psi]_+, \wedge\frown[\varphi]_-\frown[\psi]_-)$,
5°. $\langle \wedge\varphi\psi\rangle=(\wedge\frown[\varphi]_+\frown[\psi]_+, \vee\frown[\varphi]_-\frown[\psi]_-)$,
6°. $\langle\exists v_i\in t\varphi\rangle=(\exists v_{i+m}\in\frown[t]_{+m}\frown[\varphi]_+, \forall v_{i+m}\in\frown[t]_{+m}\frown[\varphi]_-)$,
7°. $\langle\forall v_i\in t\varphi\rangle=(\forall v_{i+m}\in\frown[t]_{+m}\frown[\varphi]_+, \exists v_{i+m}\in\frown[t]_{+m}\frown[\varphi]_-)$.

Then it can easily be seen by Theorem 9.1 that if φ is an RF in FCS′, then

$\langle\varphi\rangle$ is a ΔF in FCS.

Next we assign to each $\sum$F′, A in FCS′ a $\sum$F′, $\langle\langle A\rangle\rangle$ as follows:

1°. $\langle\langle\varphi\rangle\rangle\asymp[\varphi]_+$, for RF′,
2°. $\langle\langle \vee AB\rangle\rangle\asymp\vee\langle\langle A\rangle\rangle\langle\langle B\rangle\rangle$,
3°. $\langle\langle \wedge AB\rangle\rangle\asymp\wedge\langle\langle A\rangle\rangle\langle\langle B\rangle\rangle$,
4°. $\langle\langle\neg\varphi B\rangle\rangle\asymp\neg\frown[\varphi]_-\frown\langle\langle B\rangle\rangle$,

* The substitution operation must be generalized.

5°. $\langle\langle \exists v_i \in t A \rangle\rangle \asymp \exists v_{i+m} \in {}^\frown [t]_{+m} {}^\frown \langle\langle A \rangle\rangle$,

6°. $\langle\langle \forall v_i \in t A \rangle\rangle \asymp \forall v_{i+m} \in {}^\frown [t]_{+m} {}^\frown \langle\langle A \rangle\rangle$,

7°. $\langle\langle \exists v_i A \rangle\rangle \asymp \exists v_{i+m} {}^\frown \langle\langle A \rangle\rangle$.

As is expected, $\langle\langle A \rangle\rangle$ does not contain any of bound variables $v_0, \ldots, v_{m-1}$.

Now we observe that

(1) $A \dashv\vdash \langle\langle A \rangle\rangle$,

by the induction on A. This shows that each $\sum$F in FCS′ is equivalent to a $\sum$F in FCS. Moreover we can show that

(2) If $\Gamma \vdash A$ in FCS′, then $\langle\langle \Gamma \rangle\rangle \vdash \langle\langle A \rangle\rangle$ in FCS, (where $\langle\langle \Gamma \rangle\rangle = \{\langle\langle A \rangle\rangle | A \in \Gamma\}$) by the induction on $\Gamma \vdash A$. Then, in particular, letting Γ be empty and A be in FCS, we have that if $\vdash A$ in FCS′, then $\vdash A$ in FCS, since $\langle\langle A \rangle\rangle$ is, in this case, obtained from A merely by some change of variables. Since another direction is obvious we conclude that the expansion under consideration is conservative. **q.e.d.**

Remark. Note that all the metatheorems proved so far are valid in an expansion of this kind.

Remark. Of course we could also consider conservative expansion by the definition of a Σ-predicate (i.e., a predicate defined by a $\sum$F).

11. Expansion by Definition of Function

We can also expand our system FCS by introducing function symbols. In general, when we have

$$\vdash \exists ! x D(x, a_1, \ldots, a_n),$$

where D is a $\sum$F′ in FCS (or an expansion of FCS) such that $V(D) \subseteq \{x, a_1, \ldots, a_n\}$, we introduce a new function symbol, say f, of n variables and adopt

$$D(f(a_1, \ldots, a_n), a_1, \ldots, a_n)$$

as the defining postulate for f.

Through this expansion such syntactical notions as Σ-formula, derivability are naturally changed. Although how they are to be changed is almost apparent, we explain it briefly. First the definition of terms is so changed that the following clause $(\mathrm{iv})_f$ is added to the previous ones:

$(\mathrm{iv})_f$ If $t_1, \ldots, t_n$ are terms, then $ft_1 \cdots t_n$ is a term.

Similarly for semi-terms. The definition of RF' and $\sum$F' are not changed up to the meaning of semi-terms, and the definition of derivability is not changed up to the meaning of RF and $\sum$F.

This kind of expansion (called an expansion by definition of function) can also be repeated. It is conservative, too. We omit the detail of proof of it since it is standard and somewhat similar to the proof of Theorem 10.1. We only note here that e.g. $\forall x \in f(t) \cdot (\cdots)$ is equivalent to

$$\exists y(y = f(t) \wedge \forall x \in y(\cdots)).$$

Theorem 11.1. *An expansion by definition of function is conservative.*

Theorem 11.2. If $\exists ! x D(x, a_1, \ldots, a_n)$ and if $(A(x), B(x))$ is a ΔF, then

$$(\exists x(A(x) \wedge D(x, a_1, \ldots, a_n)), \exists x(B(x) \wedge D(x, a_1, \ldots, a_n)))$$

is a ΔF. In particular

$$(D(0, a_1, \ldots, a_n), \exists x(x \neq 0 \wedge D(x, a_1, \ldots, a_n)))$$

is a ΔF.

Proof is omitted.

12. Finite Set Theory

We have already defined the set-theoretic notions such as "Trans(a)" and operations such as "$a \cup b$". In this section we shall define many other such notions and operations and develop a rudimentary part of finite set theory, in our system. In order to indicate expansions, we shall only give the defining postulates of new concepts. They will be listed as "**D.12.1**", "**D.13.2**", etc. There will also be a kind of meta-definitions which provide a uniform method of giving (infinitely many) defining postulates. They will be distinguished as "**Definition**".

D.12.1. (i) $c=\{a, b\}\rightleftharpoons c=(0\#a)\#b$,
(ii) $c=\langle a, b\rangle\rightleftharpoons c=(0\#(0\#a))\#((0\#a)\#b)$.

These are justified by the fact that $\vdash\exists! y(y=t)$, where t does not contain y.

As usual we have

T.12.1. (i) $d\in\{a, b\}\rightleftharpoons d=a\vee d=b$,
(ii) $\langle a, b\rangle=\{\{a, a\}, \{a, b\}\}$,
(iii) $\langle a, b\rangle=\langle c, d\rangle\rightharpoonup a=c\wedge b=d$.

More generally we define

Definition 12.2. (i) $c=\langle a_1\rangle\rightleftharpoons c=a_1$,
(ii) *for* $n\geq 1$, $c=\langle a_1, a_2,\dots, a_{n+1}\rangle\rightleftharpoons c=\langle a_1,\langle a_2,\dots, a_{n+1}\rangle\rangle$.

From **T.12.1** follows

Theorem 12.2. $\langle a_1,\dots, a_n\rangle=\langle b_1,\dots, b_n\rangle\rightharpoonup a_1=b_1\wedge\cdots\wedge a_n=b_n$.

Now we prove the following comprehension theorem:

Theorem 12.3. (i) *Let* $\varphi(b)$ *be an* RF. *Then*

$$\vdash\exists! y(y\subseteq a\wedge\forall x\in a(x\in y\rightleftharpoons\varphi(x))).$$

(ii) *Let* $(A(b), B(b))$ *be a* ΔF. *Then* $\exists! y(y\subseteq a\wedge\forall x\in a((x\in y\rightharpoonup A(x))\wedge(x\notin y\rightharpoonup B(x))))$.

Proof. Since (i) easily follows from (ii), we only treat (ii). Since the uniqueness is obvious we only prove the existence of y. Let $C(a, c)$ be the formula:

$$c\subseteq a\wedge\forall x\in a((x\in c\rightharpoonup A(x))\wedge(x\notin c\rightharpoonup B(x))).$$

By primitive induction we have only to prove

$$(1) \qquad \vdash \exists y C(0, y)$$

and

$$(2) \qquad \exists y C(a, y) \vdash \exists y C(a \# b, y)$$

(1) is obvious since $C(0, 0)$, while (2) follows easily from

$$C(a, c) \wedge A(b) \vdash C(a \# b, c \# b)$$

and

$$C(a, c) \wedge B(b) \vdash C(a \# b, c).$$

q.e.d.

Theorem 12.4. *Suppose $F(b, a_1, \ldots, a_n)$ is a term in an expansion of* FCS *by definition. Then one can define an expansion by definition of function $f(b, a_1, \ldots, a_n)$ such that*

$$(3) \qquad \vdash \forall y \in f(b, a_1, \ldots, a_n) \exists z \in b(y = F(z, a_1, \ldots, a_n))$$
$$\wedge \forall z \in b(F(z, a_1, \ldots, a_n) \in f(b, a_1, \ldots, a_n)).$$

Moreover such a function is essentially unique, i.e., if f_1 and f_2 satisfy (3) *then*

$$\vdash f_1(b, a_1, \ldots, a_n) = f_2(b, a_1, \ldots, a_n).$$

We shall denote f which satisfies (3) *by* F″. (*This can be also considered as replacement theorem.*)

Proof. Prove

$$\vdash \exists ! c \forall y \in c \exists z \in b(y = F(z, a_1, \ldots, a_n)) \wedge \forall z \in b(F(z, a_1, \ldots, a_n) \in c),$$

by the induction on b. Then we can define the function f as required.

q.e.d.

The following is the axiom of foundation in the axiomatic set theory.

T.12.5. (i) $\forall x \in a \exists y \in a \forall z \in a(z \notin y)$,
(ii) $a \notin a$,

(iii) $\neg(a \in b \wedge b \in a)$.

Proof. First we prove

$$\forall y \in a \exists z \in a(z \in y) \vdash b \notin a$$

by the primitive induction on $* \notin a$. Then by reductio ad absurdrem (corollary 8.2 (iv)) we have

$$b \in a \vdash \exists y \in a \forall z \in a(z \notin y),$$

from which (i) follows. (ii) and (iii) follow from (i) by substituting $0 \# a$ and $(0 \# a) \# b$ for a, respectively. **q.e.d.**

Next theorem asserts the existence of sum set.

Theorem 12.6. $\exists ! y(\forall x \in y \exists z \in a(x \in z) \wedge \forall z \in a \forall x \in z(x \in y))$.

Proof. Let $C(b, a)$ be the formula

$$\forall x \in b \exists z \in b(x \in z) \wedge \forall z \in a \forall x \in z(x \in b).$$

We can easily show $\vdash \exists y C(y, a)$, by the primitive induction, from the facts

(4) $$\vdash \exists y C(y, 0) \qquad (\text{for } \vdash C(0, 0)),$$

and

(5) $$\exists y C(y, a) \vdash \exists y C(y, a \# b).$$

(The latter follows from

$$C(c, a) \vdash C(c \cup b, a \# b).)$$

The uniqueness proof is obvious. **q.e.d.**

Thus we have proved in FCS most of the axioms of elementary set theory, i.e., the axiom of power set, pair set, sum set, extensionality, RF-comprehension (or Δ_1-comprehension), Σ_1-replacement and foundation. (But of course we cannot prove the axiom of infinity.)

So we can do most of elementary set-theoretic constructions within

FCS.

D.12.3. (i) $c = \bigcup a \rightleftharpoons \forall x \in c \exists z \in a(x \in z) \wedge \forall z \in a \forall x \in z(x \in c)$,

(ii) $c = a \cap b \rightleftharpoons c \subseteq a \wedge \forall x \in a(x \in c \rightleftharpoons x \in b)$,

(iii) $c = \bigcap a \rightleftharpoons c \subseteq \bigcup a \wedge \forall x \in \bigcup a(x \in c \rightleftharpoons \forall y \in c(x \in y))$,

(iv) $c = a - b \rightleftharpoons c \subseteq a \wedge \forall x \in a(x \in c \rightleftharpoons x \notin b)$.

The definition (i) is justified by **T.12.5.** (ii)–(iv) are justified by Theorem 12.3 of comprehension.

T.12.7. (i) $d \in \bigcup a \rightharpoonup \exists x(d \in x \wedge x \in a)$,

(ii) $d \in b \wedge b \in a \rightharpoonup d \in \bigcup a$,

(iii) $d \in a \cap b \rightleftharpoons d \in a \wedge d \in b$,

(iv) $a \neq 0 \rightharpoonup (d \in \bigcap a \rightleftharpoons \forall x \in a(d \in x))$,

(v) $\bigcap 0 = 0$,

(vi) $d \in a - b \rightleftharpoons d \in a \wedge d \notin b$,

(vii) $a \cup b = \bigcup \{a, b\}$,

(viii) $a \cap b = \bigcap \{a, b\}$.

Proof. Immediate from definition.

D.12.4. (i) $b = \mathrm{dom}(a) \rightleftharpoons$
$b \subseteq \bigcup\bigcup a \wedge \forall x \in \bigcup\bigcup a(x \in b \rightleftharpoons \exists y \in \bigcup\bigcup a(\langle y, x \rangle \in a))$,

(ii) $b = \mathrm{rng}(a) \rightleftharpoons$
$b \subseteq \bigcup\bigcup a \wedge \forall x \in \bigcup\bigcup a(x \in b \rightleftharpoons \exists y \in \bigcup\bigcup a(\langle x, y \rangle \in a))$,

(iii) $c = a \times b \rightleftharpoons c \subseteq \mathrm{PP}(a \cup b) \wedge$
$\forall x \in \mathrm{PP}(a \cup b) \cdot (x \in c \rightleftharpoons \exists y \in a \exists z \in b(x = \langle y, z \rangle))$,

(iv) $b = f \restriction a \rightleftharpoons b = f \cap (\mathrm{rng}(f) \times a)$,

(v) $b = f''a \rightleftharpoons b = \mathrm{rng}(f \restriction a)$,

(vi) $b = f'a \rightleftharpoons b = \bigcup (f''\{a\})$,[*]

(vii) $g = f^{-1} \rightleftharpoons g \subseteq \mathrm{dom}(f) \times \mathrm{rng}(f) \wedge$
$\forall x \in \mathrm{dom}(f) \times \mathrm{rng}(f) \cdot (x \in g \rightleftharpoons \exists y \in \mathrm{dom}(f) \cdot \exists z \in \mathrm{rng}(f) \cdot$
$(x = \langle y, z \rangle \wedge \langle z, y \rangle \in f))$.

(viii) $h = g \circ f \rightleftharpoons h \subseteq \mathrm{rng}(g) \times \mathrm{dom}(f) \wedge$
$\forall x \in \mathrm{rng}(g) \times \mathrm{dom}(f) \cdot (x \in h \rightleftharpoons \exists u \in \mathrm{dom}(f) \cdot \exists v \in \mathrm{rng}(f) \cdot$

[*] This definition differs from Gödel's.

$$\exists w \in \mathrm{rng}(g)(\langle vu\rangle \in f \wedge \langle wv\rangle \in g \wedge x = \langle wu\rangle)) .$$

All the definitions in **D.12.4** are justified by the comprehension theorem.

T.12.8. (i) $\langle bc\rangle \in a \rightharpoonup c \in \mathrm{dom}(a)$,

(ii) $c \in \mathrm{dom}(a) \rightharpoonup \exists y(\langle yc\rangle \in a)$,

(iii) $\langle bc\rangle \in a \rightharpoonup b \in \mathrm{rng}(a)$,

(iv) $b \in \mathrm{rng}(a) \rightharpoonup \exists y(\langle by\rangle \in a)$,

(v) $c = a \times b \rightleftharpoons \forall z \in c \exists x \in a \exists y \in b(z = \langle x, y\rangle)$
$\wedge \forall x \in a \forall y \in b \exists z \in c(z = \langle x, y\rangle)$.

Proof. Obvious from definition. **q.e.d.**

D.12.5. (i) $\mathrm{Rel}(r) \rightleftharpoons \forall x \in r \exists y \in x \exists u \in y \exists v \in y(x = \langle u, v\rangle)$,

(ii) $\mathrm{Fnc}(f) \rightleftharpoons \mathrm{Rel}(f) \wedge \forall u \in \mathrm{dom}(f) \cdot \forall v \in \mathrm{rng}(f) \cdot \forall w \in \mathrm{rng}(f) \cdot$
$(\langle v, u\rangle \in f \wedge \langle w, u\rangle \in f \rightharpoonup v = w)$,

(iii) $f \mathrm{Fn}\, a \rightleftharpoons \mathrm{Fnc}(f) \wedge \mathrm{dom}(f) = a$,

(iv) $[f : a \rightarrow b] \rightleftharpoons f \mathrm{Fn}\, a \wedge \mathrm{rng}(f) \subseteq b$,

(v) $[f : a \xrightarrow{\mathrm{sur}} b] \rightleftharpoons f \mathrm{Fn}\, a \wedge \mathrm{rng}(f) = b$,

(vi) $[f : a \xrightarrow{\mathrm{inj}} b] \rightleftharpoons f \mathrm{Fn}\, a \wedge \mathrm{Fnc}(f^{-1})$,

(vii) $[f : a \xrightarrow{\mathrm{bij}} b] \rightleftharpoons [f : a \xrightarrow{\mathrm{sur}} b] \wedge [f : a \xrightarrow{\mathrm{inj}} b]$,

(viii) $a \sim b = \exists f \in \mathrm{P}(b \times a) \cdot [f : a \xrightarrow{\mathrm{bij}} b]$.

Theorem 12.9. $\mathrm{Rel}(r) \dashv\vdash \forall x \in r \exists u \exists v(x = \langle u, v\rangle)$
$\dashv\vdash r \subseteq \mathrm{rng}(r) \times \mathrm{dom}(r)$.

T.12.10. (i) $\mathrm{Rel}(a \times b)$,

(ii) $c \subseteq a \times b \rightharpoonup \mathrm{Rel}(c) \wedge \mathrm{dom}(c) \subseteq b \wedge \mathrm{rng}(c) \subseteq a$,

(iii) $a \subseteq b \wedge \mathrm{Rel}(b) \rightharpoonup \mathrm{Rel}(a)$,

(iv) $a \neq 0 \rightharpoonup \mathrm{dom}(a \times b) = b$,

(v) $\mathrm{Fnc}(f) \wedge a \in \mathrm{dom}(f) \rightharpoonup f'a \in \mathrm{rng}(a) \wedge \langle f'a, a\rangle \in f$,

(vi) $\mathrm{Fnc}(f) \wedge \langle b, a\rangle \in f \rightharpoonup b = f'a$,

(vii) $f''a \subseteq \mathrm{rng}(f)$,

(viii) $\mathrm{Rel}(f) \rightharpoonup f \restriction \mathrm{dom}(f) = f \wedge f''\mathrm{dom}(f) = \mathrm{rng}(f)$,

(ix) $f \restriction a \subseteq f$,

(x) $f \restriction a = f \restriction (a \cap \mathrm{dom}(f))$,

(xi) $[f: a \xrightarrow{\text{sur}} a] \rightleftharpoons [f: a \xrightarrow{\text{inj}} a]$,

(xii) $\mathrm{Fnc}(f) \wedge g \subseteq f \rightharpoonup \mathrm{Fnc}(g)$,

(xiii) $a \subseteq \mathrm{dom}(f) \rightharpoonup \mathrm{dom}(f \upharpoonright a) = a$,

(xiv) $\mathrm{Fnc}(f) \rightleftharpoons [f: \mathrm{dom}(f) \xrightarrow{\text{sur}} \mathrm{rng}(f)]$,

(xv) $\mathrm{Fnc}(f) \wedge \mathrm{Fnc}(g) \wedge a \subseteq \mathrm{dom}(f) \wedge a \subseteq \mathrm{dom}(g)$
$\wedge \forall x \in a(f'x = g'x) \rightharpoonup f \upharpoonright a = g \upharpoonright a$,

(xvi) $\mathrm{Fnc}(f) \wedge \mathrm{Fnc}(g) \wedge \mathrm{dom}(f) = \mathrm{dom}(g) \wedge$
$\forall x \in \mathrm{dom}(f)(f'x = g'x) \rightharpoonup f = g$,

(xvii) $0 \notin a \rightharpoonup \exists f(f \mathrm{Fn}\, a \wedge \forall x \in a(f'x \in x))$,

(xviii) $(f \circ g) \circ h = f \circ (g \circ h)$,

(xix) $a \sim a$,

(xx) $a \sim b \rightharpoonup b \sim a$,

(xxi) $a \sim b \wedge b \sim c \rightharpoonup a \sim c$,

(xxii) $a \subsetneqq b \rightharpoonup \neg(a \sim b)$.

(xxiii) $\forall f \in c\, \mathrm{Fnc}(f) \wedge \forall f \in c \forall g \in c(f \upharpoonright (\mathrm{dom}(f) \cap \mathrm{dom}(g))$
$= g \upharpoonright (\mathrm{dom}(f) \cap \mathrm{dom}(g)) \rightharpoonup \mathrm{Fnc}(\cup c)$.

Sketch of proof. (xi) can be proved by formalizing the usual method by the induction on (the cardinality of) a. (xvii) can also be obtained by the induction on a. (xxii) is a corollary of (xi). The proofs of others are omitted. **q.e.d.**

Remark. (xvii) of this theorem is the finite choice theorem.

Definition 12.6. (i) $\mathrm{dom}^{(0)}(f) = f$,

(ii) $\mathrm{dom}^{(n+1)}(f) = \mathrm{dom}(\mathrm{dom}^{(n)}(f))$, $(n \geq 0)$

(iii) $\mathrm{dom}_{i+1}(f) = \mathrm{rng}(\mathrm{dom}^{(i)}(f))$, $(i \geq 0)$

(iv) *Let* π *be a permutation on* $\{1, \ldots, n\}$.

Then we define

$$g = \mathrm{Conv}_\pi(f) \rightleftharpoons g \subseteq \mathrm{dom}_{\pi(1)}(f) \times \cdots \times \mathrm{dom}_{\pi(n)}(f) \wedge$$

$$\forall x \in \mathrm{dom}_{\pi(1)}(f) \times \cdots \times \mathrm{dom}_{\pi(n)}(f) \cdot (x \in g \rightleftharpoons$$

$$\exists y_1 \in \mathrm{dom}_1(f) \cdot \cdots \cdot \exists y_n \in \mathrm{dom}_n(f) \cdot (\langle y_1, \ldots, y_n \rangle \in f \wedge$$

$$x = \langle y_{\pi(1)}, \ldots, y_{\pi(n)} \rangle).$$

(v) $y=a_1\times\cdots\times a_n \rightleftharpoons y=((a_1\times a_2)\times\cdots)\times a_n$.

(vi) $\mathrm{Rel}_n(r) \rightleftharpoons r\subseteq \mathrm{dom}_1(r)\times\cdots\times\mathrm{dom}_n(r) \qquad (n\geq 1)$.

(vii) $\mathrm{Fnc}_n(f) \rightleftharpoons \mathrm{Rel}_{n+1}(f)\wedge \mathrm{Fnc}(f)$.

Theorem 12.11. (i) $\mathrm{Rel}_n(r) \dashv\vdash \forall x\in r\exists y_1\cdots\exists y_n(x=\langle y_1,\ldots, y_n\rangle)$,

(ii) $\mathrm{Conv}_{\mathrm{id}}(f)=f\cap(\mathrm{dom}_1(f)\times\cdots\times\mathrm{dom}_n(f))$, where id is the identity map on $\{1, 2,\ldots, n\}$,

(iii) $\mathrm{Conv}_{\pi\circ\sigma}(f)=\mathrm{Conv}_\pi(\mathrm{Conv}_\sigma(f))$,

(iv) $\langle a_1,\ldots, a_n\rangle\in f \rightleftharpoons \langle a_{\pi(1)},\ldots, a_{\pi(n)}\rangle\in \mathrm{Conv}_\pi(f)$,

(v) $\mathrm{Fnc}_n(f)\rightharpoonup\mathrm{Rel}_n(\mathrm{dom}(f))$.

Proof. Obvious.

Definition 12.7. *For each non-negative integer n we define the constant $\bar{n}$ (function of 0 variables) as follows*:

(i) $\bar{0}=0$,

(ii) $\overline{n+1}=\bar{n}\#\bar{n}$.

Moreover for each hereditarily finite set s we define the constant s^* as follows:

(iii) $s^*=(\cdots(0\# s_1^*)=\cdots)\# s_n^*)$,

when $s=\{s_1,\ldots, s_n\}$ and $s_1<s_2<\cdots<s_n$ in the standard ordering.

Theorem 12.12. *Let r and s be h.f. sets*

(i) *if $r\in s$, then $\vdash r^*\in s^*$,*

(ii) *if $r\notin s$, then $\vdash r^*\notin s^*$,*

(iii) *if $r\neq s$, then $\vdash r^*\neq s^*$.*

(Of course, if $r=s$, then $\vdash r^*=s^*$.)

(iv) *if $n<m$, then $\vdash\bar{n}\in\bar{m}$.*

(v) *if $n\geq m$, then $\vdash\bar{n}\notin\bar{m}$.*

Proof. (i) easily follows from the definition of s^* by the inference I# and **T.4.3.**

(ii) follows from (iii) by the fact

(6) If $s=\{s_1,\ldots, s_n\}$, then

$$r^*\in s^*\vdash r^*=s_1^*\vee\cdots\vee r^*=s_n^*.$$

(iii) can be proved by the induction on the maximum of the ranks of r and s, with the use of **T.4.3.** **q.e.d.**

Theorem 12.13.

$$\forall x \in a \exists y A(x, y) \vdash \exists f(f \mathrm{Fn}\, a \wedge \forall x \in a A(x, f'x)).$$

Proof. Prove

$$b \subseteq a \rightarrow \exists f(f \mathrm{Fn}\, b \wedge \forall x \in b A(x, f'x)),$$

by the primitive induction on b, under the assumption $\forall x \in a \exists y A(x, y)$.

q.e.d.

D.12.8. (i) $1 = 0 \# 0$,

(ii) $c = a \oplus b \rightleftarrows c = (\{0\} \times a) \cup (\{1\} \times b)$,

(iii) $c = {}^{b}a \rightleftarrows c \subseteq \mathrm{P}(b \times a) \wedge \forall f \in \mathrm{P}(b \times a) \cdot (f \in c \rightleftarrows [f \colon a \rightarrow b])$,

(iv) $c = a! \rightleftarrows c \subseteq {}^{a}a \wedge \forall f \in {}^{b}a(f \in c \rightleftarrows [f \colon a \xrightarrow{\mathrm{bij}} a])$.

(v) $c = \mathrm{I}(a) \rightleftarrows c\, \mathrm{Fn}\, a \wedge \forall x \in a(c'x = x)$.

T.12.14. (i) $0 \neq 1$,

(ii) $\mathrm{I}(a) \in a! \wedge a! \subseteq {}^{a}a$,

(iii) $0 \in 1$,

(iv) $a \in 1 \rightarrow a = 0$,

(v) $f \in {}^{b}a \rightleftarrows [f \colon a \rightarrow b]$,

(vi) $f \in a! \rightleftarrows [f \colon a \xrightarrow{\mathrm{bij}} a]$,

(vii) $f \in a! \wedge g \in a! \rightarrow f \circ g \in a! \wedge f^{-1} \in a!$
$\wedge f^{-1} \circ f = \mathrm{I}(a) \wedge f \circ f^{-1} = \mathrm{I}(a) \wedge f \circ \mathrm{I}(a) = f \wedge \mathrm{I}(a) \circ f = f$,

(viii) $b \notin a \wedge d \notin c \rightarrow (a \sim c \rightleftarrows a \# b \sim c \# d)$,

(ix) $a \sim b \wedge c \sim d \rightarrow a \oplus c \sim b \oplus d \wedge a \times c \sim b \times d \wedge {}^{c}a \sim {}^{d}b \wedge a! \sim b!$.

Theorem 12.15. $\exists ! f(f \mathrm{Fn}\, a \wedge \forall x \in a(f'x = F(x)))$, *where* $F(x)$ *is any term of a conservative expansion of* FCS *described above.*

Proof. Use primitive induction on a. **q.e.d.**

D.12.9. (i) $\Sigma f = \{\langle i, j \rangle \mid j \in \mathrm{dom}(f) \wedge i \in f'j\}$

(ii) $\Pi f = \{g \colon \mathrm{dom}(g) = \mathrm{dom}(f) \wedge \forall x \in \mathrm{dom}(f)(g'x \in f'x)\}$.

(iii) $\sum_{x \in b} F(x, a_1, \ldots, a_n) = \Sigma F \restriction (b, a_1, \ldots, a_n)$

(iv) $\prod_{x\in b} F(x, a_1,\ldots, a_n)=\Pi F \restriction (b, a_1,\ldots, a_n)$

(v) ${}_aP_b=\{f\colon b \xrightarrow{\text{inj}} a\}$

(vi) ${}_aC_b=\{x\subseteq a\colon x\sim b\}$

T.12.16. (i) $\mathrm{Fnc}(f)\wedge \mathrm{Fnc}(g)\wedge \mathrm{dom}(f)=\mathrm{dom}(g)\wedge$
$\forall i\in \mathrm{dom}(f)(f'i\sim g'i)\rightharpoonup \Sigma f\sim \Sigma g\wedge \Pi f\sim \Pi g,$

(ii) $a\oplus b=\Sigma\{\langle a, 0\rangle, \langle b, 1\rangle\},$

(iii) $a\times b\sim \Pi\{\langle a, 0\rangle, \langle b, 1\rangle\}$

(iv) $\Sigma 0=0\wedge \Pi 0=1$

(v) $\Sigma f=\bigcup\{f'a\times\{a\}|a\in \mathrm{dom}(f)\}$

(vi) $\mathrm{Fnc}(f)\wedge \mathrm{Fnc}(g)\wedge \mathrm{dom}(f)\cap \mathrm{dom}(g)=0$

$$\rightharpoonup \Sigma(f\cup g)=\Sigma f\cup \Sigma g\wedge \Sigma f\cap \Sigma g=0$$

$$\wedge \Sigma(f\cup g)\sim \Sigma f\oplus \Sigma g$$

$$\wedge \Pi(f\cup g)\sim \Pi f\times \Pi g$$

(vii) $\Sigma\{\langle a, j\rangle\}=a\times\{j\}\wedge a\times\{j\}\sim a$

(viii) $\Pi\{\langle a, j\rangle\}\sim a$

(ix) $\sum_{x\in b\cup c} F(x)=\sum_{x\in b} F(x)\cup \sum_{x\in c} F(x)$

(x) $b\cap c=0\rightharpoonup \sum_{x\in b\cup c} F(x)\sim \sum_{x\in b} F(x)\oplus \sum_{x\in c} F(x)$

(xi) $\wedge \prod_{x\in b\cup c} F(x)\sim \prod_{x\in b} F(x)\times \prod_{x\in c} F(x)$

(xii) $\sum_{x\in \Sigma G(y)} F(x)\sim \sum_{y\in c}\Big(\sum_{x\in G(y)} F(x)\Big)$

(xiii) $\prod_{\substack{x\in \Sigma G(y)\\ y\in c}} F(x)\sim \prod_{y\in c}\Big(\prod_{x\in G(y)} F(x)\Big)$

(xiv) $\sum_{x\in b}(F(x)\oplus G(x))\sim \sum_{x\in b} F(x)\oplus \sum_{x\in b} G(x)$

(xv) $\prod_{x\in b}(F(x)\times G(x))\sim \sum_{x\in b} F(x)\times \prod_{x\in b} G(x)$

(xvi) $\sum_{x\in b}\sum_{y\in c} F(x, y)\sim \sum_{<x,y>\in b\times c} F(x, y)$

(xvii) $\prod_{x\in b}\prod_{y\in c} F(x, y)\sim \prod_{<x,y>\in b\times c} F(x, y)$

$\prod_{x\in b}\sum_{y\in c} F(x, y)\sim \sum_{f\in {}^bc}\prod_{x\in b} F(x, f'x)$

T.12.17. *If F is a term of an expansion of* FCS *as mentioned above, then*

(i) $\mathrm{Trans}(w) \vdash \exists ! f(f \mathrm{Fn}\, w \wedge \forall x \in w(f'x = F(f \restriction x)))$.

(ii) *If* $G(f, a_1, \ldots, a_n)$ *is a function (or term) in an expansion of* FCS, *then one can define a function* $F(a_1, \ldots, a_n)$ *such that*

$$\vdash F(a_1, \ldots, a_n) = G(F \restriction (a_1, \ldots, a_n), a_1, \ldots, a_n).$$

($F \restriction$ *is the function obtained from* F *as in Theorem* 12.15.)

Proof. Let

$$V(f, w) \Leftrightarrow \mathrm{Trans}(w) \wedge f \mathrm{Fn}\, w \wedge \forall x \in w(f'x = F(f \restriction x)).$$

Then we first show

(7) $$V(f, w), V(g, w'), a \subseteq w, a \subseteq w' \vdash f \restriction a = g \restriction a.$$

This follows from

(8) $$V(f, w), V(g, w') \vdash a \in w \wedge a \in w' \rightarrow f'a = g'a$$

by using (xv) of **T.12.10**.
(8) is shown by the induction (theorem) on a with the use of **T.12.10** (xv) again.

Next we show that

(9) $$\exists f V(f, \overline{\mathrm{Tc}}(a)),$$

by the induction on a. We have only to prove

(10) $$\forall x \in a \exists g V(g, \overline{\mathrm{Tc}}(x)) \vdash \exists f V(f, \overline{\mathrm{Tc}}(a)).$$

Now by

(11) $$\forall x \in a \exists g V(g, \overline{\mathrm{Tc}}(x)) \vdash$$
$$\exists z(\forall x \in a \exists g \in z V(g, \overline{\mathrm{Tc}}(x)) \wedge \forall g \in z \exists x \in a V(g, \overline{\mathrm{Tc}}(x))).$$

But we easily have

(12) $$\forall x \in a \exists g \in c V(g, \overline{\mathrm{Tc}}(x)) \wedge \forall g \in c \exists x \in a V(g, \overline{\mathrm{Tc}}(x))$$
$$\vdash V(\cup c, \overline{\mathrm{Tc}}(a)).$$

Moreover we have

$$(13)\qquad V(k, \overline{\mathrm{T}}\mathrm{c}(a)) \vdash V(k', \overline{\mathrm{T}}\mathrm{c}(a)),$$

where k' denote $k \cup \{\langle F(k \restriction a), a\rangle\}$.
From (11), (12) and (13) follows (10). Hence we have shown (9). Now

$$\forall x \in w \exists f V(f, \overline{\mathrm{T}}\mathrm{c}(x)),$$

and hence

$$\exists c(\forall x \in w \exists f \in c V(f, \overline{\mathrm{T}}\mathrm{c}(x)) \wedge \forall f \in c \exists x \in w V(F, \overline{\mathrm{T}}\mathrm{c}(x))).$$

By the same way as above we have

$$\forall x \in w \exists f \in c V(f, \overline{\mathrm{T}}\mathrm{c}(x)) \wedge \forall f \in c \exists x \in w V(f, \overline{\mathrm{T}}\mathrm{c}(x)))$$

$$\vdash V(\cup c, w), \text{ and hence}$$

$$\vdash \exists f V(f, w).$$

Uniqueness follows from (7). **q.e.d.**

Elementary theory of finite groups can be formalized in FCS. For instance, the homorphism and the isomorphism theorems are proved in FCS with their usual proofs. For more example, the theorem that every finite abelian group is a direct product of cyclic groups, is usually proved using free abelian group, so that the proof is infinistic. However, this can obviously be avoided and the theorem is proved in FCS.

One could further define in FCS, various algebraic notions such as finite fields, finite lattices, finite partially ordered sets, etc., and develop theories about these notions which do not use the infinite methods. It would be interesting to see how far the extent of these theories will be formalizable in FCS.

13. Natural Numbers and Number Theory

According to the program mentioned in Section 1, natural numbers are here regarded as (finite) von Neumann ordinals.

D.13.1. (i) $\mathrm{Nat}(a)\Leftrightarrow\mathrm{Trans}(a)\wedge\forall x\in a\cdot\mathrm{Trans}(x)$,

(ii) $b=\mathrm{S}(a)\Leftrightarrow b=a\# a$,

(iii) $a<b\Leftrightarrow\mathrm{Nat}(a)\wedge\mathrm{Nat}(b)\wedge a\in b$,

(iv) $b>a\Leftrightarrow a<b$,

(v) $a\leq b\Leftrightarrow\mathrm{Nat}(a)\wedge\mathrm{Nat}(b)\wedge(a\in b\vee a=b)$,

(vi) $b\geq a\Leftrightarrow a\leq b$.

Since $\mathrm{Nat}(a)$ is an RF, we have

T.13.1. $\mathrm{Nat}(a)\vee\neg\mathrm{Nat}(a)$.

Moreover we have

T.13.2. (i) $\mathrm{Nat}(a)\wedge b\in a\to\mathrm{Nat}(b)$,

(ii) $\mathrm{Nat}(0)$,

(iii) $\mathrm{Nat}(a)\to\mathrm{Nat}(\mathrm{S}(a))$,

(iv) $\mathrm{S}(a)=\mathrm{S}(b)\to a=b$,

(v) $\mathrm{Nat}(a)\to a\leq a$,

(vi) $a\leq b\wedge b\leq a\to a=b\wedge\mathrm{Nat}(a)$,

(vii) $a\leq b\wedge b\leq c\to a\leq c$,

(viii) $a<b\wedge b<c\to a<c$,

(ix) $\mathrm{Nat}(a)\wedge\mathrm{Nat}(b)\to a<b\vee a=b\vee b<a$,

(x) $\forall x\in a\cdot\mathrm{Nat}(x)\wedge a\neq 0\to\exists x\in a\forall y\in a(y\leq x)$,

(xi) $\mathrm{Nat}(a)\wedge a\neq 0\to\exists b(\mathrm{Nat}(b)\wedge a=\mathrm{S}(b))$.

Proof. (i) Obviously we have

$$\mathrm{Nat}(a),\quad b\in a\vdash\mathrm{Trans}(b). \tag{1}$$

So, $\mathrm{Nat}(a)$, $b\in a$, $c\in b\vdash c\in a$, and hence

$$\mathrm{Nat}(a),\quad b\in a,\quad c\in b\vdash\mathrm{Trans}(c).$$

Therefore,

$$\mathrm{Nat}(a),\quad b\in a\vdash\forall x\in b\cdot\mathrm{Trans}(x). \tag{2}$$

From (1) and (2) we have (i).

(ii) is immediate.

(iii) It can be easily proved that

$$\text{(3)} \qquad \mathrm{Trans}(a) \vdash \mathrm{Trans}(\mathrm{S}(a)).$$

Moreover, since $c \in \mathrm{S}(a) \vdash c = a \vee c \in a$, we have

$$\mathrm{Nat}(a), \quad c \in \mathrm{S}(a) \vdash \mathrm{Trans}(c).$$

Therefore,

$$\text{(4)} \qquad \mathrm{Nat}(a) \vdash \forall x \in \mathrm{S}(a) \cdot \mathrm{Trans}(x).$$

From (3) and (4) we have (iii).

(iv) Evidently,

$$a \# a = b \# b \vdash a \in b \# b \wedge b \in a \# a.$$

Hence,

$$a \# a = b \# b \vdash (a \in b \wedge a = b) \wedge (b \in a \vee a = b).$$

But, by **T.12.5** (iii), $\vdash \neg(a \in b \wedge b \in a)$. So we must have

$$a \# a = b \# b \vdash a = b.$$

(v) Immediate from definition of $\leq$.

(vi) Use **T.12.5** (iii).

(vii), (viii) Use the fact that $\mathrm{Nat}(c) \vdash \mathrm{Trans}(c)$.

(ix) We use Theorem 7.2 (iii). Let $D(a, b)$ be the formula

$$\mathrm{Nat}(a) \wedge \mathrm{Nat}(b) \rightharpoonup (a \in b \vee a = b \vee b \in a).$$

We have to show

$$\forall x \in a D(x, b), \quad \forall y \in b D(a, y) \vdash D(a, b).$$

On account of (i) of this theorem it is enough to show that

$$\text{(5)} \qquad \mathrm{Nat}(a), \quad \mathrm{Nat}(b), \quad \forall x \in a(x \in b \vee x = b \vee b \in x),$$

$$\forall y \in b(a \in y \vee a = y \vee y \in a) \vdash a \in b \vee a = b \vee b \in a.$$

This can be proved as follows:

$$\mathrm{Nat}(a),\quad c\in a,\quad c=b\vee b\in c\vdash b\in a;$$

$$a\notin b,\quad \mathrm{Nat}(a)\vdash\forall x\in a(x\neq b\wedge b\notin x);$$

$$a\notin b,\quad \mathrm{Nat}(a),\quad \forall x\in a(x\in b\vee x=b\vee b\in x)\vdash\forall x\in a(x\in b),$$

here we used the law of excluded middle for RF's. Similarly,

$$b\notin a,\quad \mathrm{Nat}(b),\quad \forall y\in b(a\in y\vee a=y\vee y\in a)\vdash\forall y\in b(y\in a).$$

Hence,

$$a\notin b,\ b\notin a,\ \mathrm{Nat}(a),\ \mathrm{Nat}(b),\ \forall x\in a(x\in b\vee x=b\vee b\in x),$$

$$\forall y\in b(a\in y\vee a=y\vee y\in a)\vdash a=b,$$

from which (5) follows. (The law of excluded middle is used again.)

(x) By primitive recursion, we can easily show

$$\vdash\forall x\in a\cdot\mathrm{Nat}(x)\wedge a\neq 0\rightharpoonup\exists x\in a\forall y\in a(x\in y\vee x=y),$$

by using (ix).

(xi) In view of (x) and (i), it is sufficient to prove

$$\mathrm{Nat}(a),\quad b\in a,\quad \forall y\in a(y\in b\vee y=b)\vdash a=\mathrm{S}(b).$$

But this is obvious since $\mathrm{Nat}(a)\vdash\mathrm{Trans}(a)$. **q.e.d.**

Theorem 13.3. (*Primitive induction on natural numbers.*)

(i) *If* $\Gamma\vdash A(0)$, *and if* $\mathrm{Nat}(a), A(a), \Gamma\vdash A(S(a))$, *where* a *is a free variable which does not occur in* Γ *or in* $A(x)$, *then* $\mathrm{Nat}(t), \Gamma\vdash A(t)$, *for any term* t;

(ii) (*course-of-values induction*) *if* $\mathrm{Nat}(a), \forall x\in aA(x), \Gamma\vdash A(a)$, *where* a *is a free variable which does not occur in* Γ *or in* $A(x)$, *then* $\mathrm{Nat}(t)$, $\Gamma\vdash A(t)$, *for any term* t.

Proof. We shall prove

$$\Gamma\vdash\mathrm{Nat}(t)\rightharpoonup A(t),$$

by the induction of Theorem 7.2 (i). It suffices to prove

$$\forall x\in a(\mathrm{Nat}(x)\rightharpoonup A(x)),\quad \Gamma\vdash\mathrm{Nat}(a)\rightharpoonup A(a).$$

By the assumption it follows easily that

$$a=0,\quad \forall x\in a(\mathrm{Nat}(x)\rightharpoonup A(x)),\quad \Gamma\vdash \mathrm{Nat}(a)\rightharpoonup A(a).$$

So it suffices to prove

$$a\neq 0,\quad \forall x\in a(\mathrm{Nat}(x)\rightharpoonup A(x)),\quad \Gamma\vdash \mathrm{Nat}(a)\rightharpoonup A(a),$$

since $\vdash a=0\vee a\neq 0$.
Now by assumption

$$\mathrm{Nat}(b),\quad A(b),\quad \Gamma\vdash A(\mathrm{S}(b)).$$

So,

$$a=\mathrm{S}(b),\quad \mathrm{Nat}(a),\quad \mathrm{Nat}(b)\rightharpoonup A(b),\quad \Gamma\vdash A(a),$$

and hence

$$a=\mathrm{S}(b),\quad \mathrm{Nat}(a),\quad \forall x\in a(\mathrm{Nat}(x)\rightharpoonup A(x)),\quad \Gamma\vdash A(a).$$

But by **T.13.2** (xi),

$$\mathrm{Nat}(a),\quad a\neq 0\rightharpoonup \exists x(a=\mathrm{S}(x)).$$

Therefore, we have

$$\forall x\in a(\mathrm{Nat}(x)\rightharpoonup A(x)),\quad \Gamma\vdash \mathrm{Nat}(a)\rightharpoonup A(a).$$

To prove (ii), use (i) with the formula $\forall x\in aA(x)$ instead of A, and then use **T.7.1**. (Another way to obtain (ii) is to apply Theorem 7.2 (i) directly.) **q.e.d.**

By **T.13.2** and Theorem 13.3, we obtain Peano axioms with mathematical induction restricted to $\sum$F's (primitive induction). But the primitive induction is not so weak as might seem at first sight. Indeed, almost all the theorems of elementary number theory are provable with the use of this induction.

Incidentally, we prove some more variants of primitive induction.

Corollary 13.4. *If we have*

$$\mathrm{Nat}(a),\quad A(f(a)),\quad \Gamma\vdash A(a)$$

and

$$a\neq 0,\quad \mathrm{Nat}(a),\quad \Gamma\vdash f(a)<a,$$

where a does not occur in Γ or in $A(x)$, then we have $\Gamma\vdash A(a)$.

Proof. Immediate from Theorem 13.2 (i). **q.e.d.**

Remark. This also holds when $<$ is replaced by some standard ordering isomorphic to ω^2 or even to ω^n. This is shown by Tait [1] and Guard [1], for different (but essentially equivalent) systems.

Next we shall introduce various number theoretic functions and predicates in our system. To do this we wish to extend our system by definitions of these functions and predicates. Since these functions are defined only over natural numbers but not over all h.f. sets, we adopt the convention that these functions take 0 as value for arguments which are not natural numbers. In case of a number theoretic predicate we also adopt the convention that it takes the true value only for natural numbers.

For notational simplicity we introduce the new variables ranging over natural numbers:

$$\lambda,\ \mu,\ \nu,\ \lambda_1,\ \mu_1,\ \nu_1,\dots.$$

For example, $\exists\lambda A(\lambda)$ means $\exists x(\mathrm{Nat}(x)\wedge A(x))$, $\forall\lambda\in yA(\lambda)$ means $\forall x\in y(\mathrm{Nat}(x)\rightarrow A(x))$ and $\forall\lambda<\mu A(\lambda)$ means $\forall x\in\mu A(x)$. Moreover $\vdash A(\lambda_1,\dots,\lambda_n,x_1,\dots,x_m)$ means

$$\vdash\mathrm{Nat}(y_1)\wedge\cdots\wedge\mathrm{Nat}(y_n)\rightarrow A(y_1,\dots,y_n,x_1,\dots,x_m),$$

or what is the same,

$$\mathrm{Nat}(y_1),\dots,\mathrm{Nat}(y_n)\vdash A(y_1,\dots,y_n,x_1,\dots,x_m).$$

Now suppose that

$$(6)\qquad\begin{cases}\exists!\nu D(\nu,\mu_1,\dots,\mu_n)\\ \text{and}\\ D(b,a_1,\dots,a_n)\vdash\mathrm{Nat}(b)\wedge\mathrm{Nat}(a_1)\wedge\cdots\wedge\mathrm{Nat}(a_n).\end{cases}$$

Let $D'(b, a_1,\dots, a_n)$ be

$$D(b, a_1,\dots, a_n) \vee (b=0 \wedge \neg(\mathrm{Nat}(a_1) \wedge \cdots \wedge \mathrm{Nat}(a_n))).$$

Then we easily obtain

$$\exists! y D'(y, a_1,\dots, a_n).$$

So by Section 11, we can introduce a new function symbol, say ρ, such that

$$\vdash D'(\rho(a_1,\dots, a_n), a_1,\dots, a_n).$$

This is characterized by

$$\vdash \mathrm{Nat}(\rho(\mu_1,\dots, \mu_n)) \wedge D(\rho(\mu_1,\dots, \mu_n), \mu_1,\dots, \mu_n)$$

and

$$\neg(\mathrm{Nat}(a_1) \wedge \cdots \wedge \mathrm{Nat}(a_n)) \vdash \rho(a_1,\dots, a_n)=0.$$

This is a general method of introducing number theoretic functions into the system.

However, number theoretic functions are often defined recursively but not explicitly as (6). As is well-known, recursive definitions can be reduced to explicit ones in usual number-theoretic formal system such as first-order number theory. The same is true for our system FCS, which is logically weaker than the first-order number theory. This is stated as follows:

Theorem 13.5. *Suppose* $G(a_1,\dots, a_n)$ *and* $H(b, c, a_1,\dots, a_n)$ *are given function symbols or terms in some expansion of* FCS *by definition. Then one can introduce a function* $F(b, a_1,\dots, a_n)$ *in some expansion of* FCS *by definition, such that*

$$(7) \qquad \begin{cases} \vdash F(0, a_1,\dots, a_n) \\ \vdash F(\mathrm{S}(v), a_1,\dots, a_n)=H(v, F(v, a_1,\dots, a_n), a_1,\dots, a_n) \\ \neg\mathrm{Nat}(b) \vdash F(b, a_1,\dots, a_n)=0. \end{cases}$$

Moreover such an F *is essentially unique in the sense that if both* F

and F' satisfy the above conditions, then

$$\vdash F(b, a_1,\ldots, a_n) = F'(b, a_1,\ldots, a_n).$$

Proof. Let $W(f, b, a_1,\ldots, a_n)$ be the formula

$$\mathrm{Nat}(b) \wedge f\mathrm{Fn}\,\mathrm{S}(b) \wedge f'0 = G(a_1,\ldots, a_n)$$
$$\wedge \forall v < b(f'\mathrm{S}(v) = H(v, f'v, a_1,\ldots, a_n)).$$

We can prove

$$\mathrm{Nat}(b) \rightarrow \exists f W(f, b, a_1,\ldots, a_n)$$

by the induction of Theorem 13.3. Moreover we have

$$b \subseteq c, \quad W(f, b, a_1,\ldots, a_n), \quad W(g, c, a_1,\ldots, a_n) \rightarrow f \subseteq g.$$

Now let $D(c, b, a_1,\ldots, a_n)$ be the formula

$$\exists f(W(f, b, a_1,\ldots, a_n) \wedge c = f'b) \vee (\neg \mathrm{Nat}(b) \wedge c = 0).$$

Then

$$\vdash \exists ! c D(c, b, a_1,\ldots, a_n).$$

So by Section 11, we may introduce a function symbol F such that

$$\vdash D(F(b, a_1,\ldots, a_n), b, a_1,\ldots, a_n).$$

Now it is obvious that F satisfies the required condition. Next suppose F and F' satisfy the condition (7). Then we can prove

$$\mathrm{Nat}(b) \vdash F(b, a_1,\ldots, a_n) = F'(b, a_1,\ldots, a_n)$$

by the induction (by Theorem 13.3) on b, and also

$$\neg \mathrm{Nat}(b) \vdash F(b, a_1,\ldots, a_n) = F'(b, a_1,\ldots, a_n)$$

since $\neg \mathrm{Nat}(b) \vdash F(b, a_1,\ldots, a_n) = 0$ and the same for F'. In view of **T.13.1** we have the uniqueness of F. **q.e.d.**

Example. The addition $\lambda = \mu + \nu$ can be defined explicitly by

$$\exists f(f\,\mathrm{Fn}\,\mathrm{S}(\nu) \wedge f'0=\mu \wedge \forall\xi<\nu(f'\mathrm{S}(\xi)=\mathrm{S}(f'\xi)) \wedge \lambda=f'\nu).$$

(We adopt however another definition of the addition, c.f. **D.13.4**, below.)

In the above theorem, G and H may not be number-theoretic functions (i.e., those functions which take natural numbers as values for natural number arguments and 0 otherwise).

But if both G and H are number-theoretic, then resulting F is also number-theoretic and is the one obtained by the usual primitive recursion. Since other schemata to define primitive recursive functions (i.e., successor, constant, projection and composition) are all at hand in our system, it follows that all the primitive recursive functions are definable in FCS (by Σ-formulas).

Furthermore, each instance of the inference rules of primitive recursive arithmetic (abbreviated PRA) given by Goodstein [2] or Curry [1] is easily provable in FCS. (PRA was first introduced by Skolem [1].) It follows that PRA is embeddable into FCS. We state these results as theorems:

Theorem 13.6. *Every primitive recursive function is definable in* FCS *by a Σ-formula, and every primitive recursive predicate is definable in* FCS *by a Δ-formula.*

Proof. The first part of the theorem was mentioned above. To be more detailed,

$$D(b, a)\Longleftrightarrow(\mathrm{Nat}(a) \wedge b=\mathrm{S}(a)) \vee (\neg\mathrm{Nat}(a) \wedge b=0)$$

defines the successor function,

$$D(b, a_1,\dots, a_n)\Longleftrightarrow b=0$$

defines the identically-0 function,

$$D(b, a_1,\dots, a_n)\Longleftrightarrow b=a_i$$

defines the i-th projection (of n arguments), and

$$D(b, a_1,\dots, a_n)\Longleftrightarrow\exists x_1\cdots\exists x_n(B_1(x_1, a_1,\dots, a_n)$$

$$\wedge \cdots \wedge B_m(x_m, a_1, \ldots, a_n) \wedge C(b, x_1, \ldots, x_m))$$

defines the composition (of the function defined by C and those by B_i's).

The second part of the theorem follows from the first part, since if a primitive recursive predicate P is defined by a primitive recursive function F informally by

$$P(\mu_1, \ldots, \mu_n) \Longleftrightarrow F(\mu_1, \ldots, \mu_n) = 0,$$

and if F is defined by a Σ-formula D of our system:

$$b = F(a_1, \ldots, a_n) \Longleftrightarrow D(b, a_1, \ldots, a_n),$$

then $P(a_1, \ldots, a_n)$ is defined by the Δ-formula $(B(a_1, \ldots, a_n), C(a_1, \ldots, a_n))$, where

$$B(a_1, \ldots, a_n) \Longleftrightarrow \mathrm{Nat}(a_1) \wedge \cdots \wedge \mathrm{Nat}(a_n) \wedge D(0, a_1, \ldots, a_n)$$

and

$$C(a_1, \ldots, a_n) \Longleftrightarrow \mathrm{Nat}(a_1) \wedge \cdots \wedge \mathrm{Nat}(a_n) \rightarrow \exists x (x \neq 0 \wedge D(x, a_1, \ldots, a_n)).$$

That (B, C) is a ΔF would be an easy exercise. **q.e.d.**

Theorem 13.7. *Via the above interpretation, all the equations provable in* PRA *are provable in* FCS.

We omit the detailed proof of it.

We could proceed to develop number theory along the line of PRA (cf. Goodstein [2], Hilbert–Bernays [1]). But we adopt another way, which will turn out to be more natural and simple for our system.

We begin by defining the cardinality of sets:

D.13.2. $C(n, a) \Longleftrightarrow a \sim n \wedge \mathrm{Nat}(n)$.

T.13.8. $\exists ! n\, C(n, a)$.

Proof. By **T.12.9** (xxii), $\nu \subsetneqq \mu \vdash \nu \nsim \mu$. But, as is easily seen, $\nu < \mu \vdash \nu \subsetneqq \mu$. So,

$$\nu < \mu \vdash \nu \nsim \mu.$$

From this with **T.13.2** (ix), it follows that

$$\mu \neq \nu \vdash \mu \nsim \nu.$$

Hence

$$C(\mu, a), \quad C(\nu, a) \vdash \mu = \nu.$$

Uniqueness is proved. Obviously,

$$b \in a \vdash a \# b = a.$$

Hence

$$b \in a, \quad C(n, a) \vdash C(n, a \# b). \tag{8}$$

On the other hand we easily verify that

$$[f : a \xrightarrow{\text{bij}} n], \quad b \notin a \vdash [f \cup \{\langle n, b \rangle\} : a \# b \xrightarrow{\text{bij}} \mathrm{S}(n)].$$

So,

$$C(n, a), \quad b \notin a \vdash C(\mathrm{S}(n), a \# b). \tag{9}$$

Using (8) and (9) with $\vdash b \in a \vee b \notin a$, we have

$$\exists n C(n, a) \vdash \exists n C(n, a \# b).$$

But $\vdash \exists n C(n, 0)$ is clear. So, by the primitive induction we have $\exists n C(n, a)$. **q.e.d.**

By **T.13.8**, we can define $\bar{a}$ by

D.13.3. $C(\bar{a}, a)$.

We are now in a position to define addition, multiplication etc. of natural numbers:

D.13.4. (i) $\mu + \nu = \overline{\overline{\mu \oplus \nu}}$;

(ii) $\mu \cdot \nu = \overline{\overline{\mu \times \nu}}$;

(iii) $\mu^{\nu} = \overline{\overline{{}^{\nu}\mu}}$;

(iv) $\mu! = \overline{\overline{\mu!}}$;

(v) $\mu \dot{-} \nu = \overline{\overline{\mu - \nu}}$;

(vi) $(f)_\nu = \begin{cases} f'\nu, & \textit{if} \quad \nu \in \mathrm{dom}(f), \\ 0, & \textit{otherwise}; \end{cases}$

(vii) $\sum f = \overline{\overline{\Sigma f}}$;

(viii) $\prod f = \overline{\overline{\Pi f}}$;

(ix) $\mu | \nu \Longleftrightarrow \exists \lambda (\mu \times \lambda = \nu)$;

(x) $\lambda = [\mu/\nu] \Longleftrightarrow \exists \xi < \nu (\mu = \lambda \cdot \nu + \xi) \vee (\nu = 0 \wedge \lambda = 0)$;

(xi) $\mathrm{rem}(\mu, \nu) = \mu \dot{-} [\mu/\nu] \cdot \nu$;

(xii) $\binom{\mu}{\nu} = \overline{\overline{{}_\mu C_\nu}}$;

(xiii) $a \equiv b(m) \Longleftrightarrow \mathrm{rem}(a, m) = \mathrm{rem}(b, m)$.

(These definitions should be interpreted as such define functions whose values for natural number arguments are as in their definitions and 0 for other arguments.)

T.13.9. (i) $\lambda + \mu = \mu + \lambda$

(ii) $(\lambda + \mu) + \nu = \lambda + (\mu + \nu)$,

(iii) $\lambda \cdot \mu = \mu \cdot \lambda$,

(iv) $(\lambda \cdot \mu) \cdot \nu = \lambda \cdot (\mu \cdot \nu)$,

(v) $(\lambda + \mu) \cdot \nu = \lambda \cdot \nu + \mu \cdot \nu$,

(vi) $\lambda^{\mu + \nu} = \lambda^\mu \cdot \lambda^\nu$,

(vii) $(\mu \cdot \nu)^\lambda = \mu^\lambda \cdot \nu^\lambda$,

(viii) $\mu + 0 = \mu \wedge \mu + 1 = \mathrm{S}(\mu)$,

(ix) $\mu + (\mathrm{S}\nu) = \mathrm{S}(\mu + \nu)$,

(x) $\mu \cdot 0 = 0 \wedge \mu \cdot 1 = \mu$,

(xi) $\mu \cdot (\mathrm{S}\nu) = \mu \cdot \nu + \mu$,

(xii) $\mu + \nu = \lambda \rightharpoonup \nu = \lambda \dot{-} \mu$,

(xiii) $\mu \cdot \nu = \lambda \wedge \mu \neq 0 \rightharpoonup \nu = [\lambda/\mu]$,

(xiv) $\mu \leq \nu \rightharpoonup \nu = \mu + (\nu \dot{-} \mu)$,

(xv) $\nu < \mu \rightharpoonup \nu \dot{-} \mu = 0$,

(xvi) $\mu | \nu \rightharpoonup \nu = [\nu/\mu] \cdot \mu$,

(xvii) $\nu = [\nu/\mu] \cdot \mu + \mathrm{rem}(\nu, \mu)$,

(xviii) $\nu > 0 \rightharpoonup \nu > \mathrm{rem}(\mu, \nu)$,

(xix) $\nu > 0 \wedge \nu > \mu \rightarrow [\mu/\nu] = 0 \wedge \mathrm{rem}(\mu, \nu) = \mu$,

(xx) $0! = 1$,

(xxi) $(\mathrm{S}\mu)! = (\mathrm{S}\mu) \cdot \mu!$,

(xxii) $\mu! = \prod_{\nu \in \mathrm{S}(\mu) \dot{-} 1} \nu \left(= \prod_{1 \leq \nu \leq \mu} \nu \right)$,

(xxiii) $\overline{\overline{\mathrm{P}(a)}} = 2^{\bar{\bar{a}}}$,

(xxiv) $\sum_{\nu \in \mu} 2^{\nu} \left(= \sum_{\nu < \mu} 2^{\nu} \right) = 2^{\mu} \dot{-} 1$,

(xxv) $\binom{\mu}{\mu} = \binom{\mu}{0} = 1$,

(xxvi) $\binom{\mu + 1}{\nu + 1} = \binom{\mu}{\nu + 1} + \binom{\mu}{\nu}$

(xxvii) $a \equiv a(m) \wedge (a \equiv b(m) \rightarrow b \equiv a(m))$,
$\wedge (a \equiv b(m) \wedge b \equiv c(m) \rightarrow a \equiv c(m))$,

(xxviii) $m \neq 0 \rightarrow (a \equiv 0(m) \rightleftarrows m | a)$.

Proof. For (i)~(xi), use **T.12.14**. For others one can also prove them as usual. **q.e.d.**

Although the above definitions are obvious, the following one is somewhat technical.

D.13.5. (i) $\mathrm{Cb}(f) \Longleftrightarrow \mathrm{Fnc}(f) \wedge \forall x \in \mathrm{rng}(f)(\mathrm{Nat}(x) \wedge x \neq 0)$,

(ii) $h = f \vartriangle g \Longleftrightarrow \mathrm{Fnc}(h) \wedge \mathrm{dom}(h) = \mathrm{dom}(f) \cup \mathrm{dom}(g)$
$\wedge \forall x \in \mathrm{dom}(f) \cap \mathrm{dom}(g) \cdot (h'x = f'x + g'x)$
$\wedge \forall x \in \mathrm{dom}(f) - \mathrm{dom}(g) \cdot (h'x = f'x)$
$\wedge \forall x \in \mathrm{dom}(g) - \mathrm{dom}(f) \cdot (h'x = g'x)$,

(iii) $\| f \| = \sum_{x \in \mathrm{dom}(f)} f'x$,

(iv) $\langle\langle a \rangle\rangle = \{\langle 1, a \rangle\}$,

(v) $h = \Delta(g) \Longleftrightarrow \mathrm{Fnc}(h) \wedge \mathrm{dom}(h) = \cup \{\mathrm{dom}(f) | f \in \mathrm{dom}(g)\}$
$\wedge \forall x \in \mathrm{dom}(h) \cdot (h'x = \sum_{\substack{f \in g \\ x \in \mathrm{dom}(f)}} (f'x) \cdot (g'f))$,

(vi) $h = \overline{\mathrm{rg}}(f) \Longleftrightarrow h \,\mathrm{Fn}\, \mathrm{rng}(f) \wedge \forall x \in \mathrm{dom}(h) \cdot (h'x = \overline{\overline{f^{-1}\{x\}}})$

(vii) $\mathrm{Fcr}(f) \Longleftrightarrow \mathrm{Cb}(f) \wedge \forall x \in \mathrm{dom}(f)(\mathrm{Nat}(x) \wedge x \neq 0)$,

(viii) $\Sigma^* f = \sum_{x \in \mathrm{dom}(f)} (f'x) \cdot x$,

(ix) $\Pi^* f = \prod_{x \in \mathrm{dom}(f)} x^{f'x}$,

(x) $\{\{a\}\} = \{\langle 1, x \rangle | x \in a\}$.

Then we easily obtain

T.13.10. (i) $\mathrm{Cb}(f) \to \mathrm{Nat}(\|f\|)$,

(ii) $\mathrm{Cb}(0) \wedge \|0\| = 0$,

(iii) $\mathrm{Cb}(f) \to f \vartriangle 0 = f$,

(iv) $\mathrm{Cb}(\langle\langle a\rangle\rangle) \wedge \langle\langle a\rangle\rangle = 1$,

(v) $\lambda \neq 0 \to \mathrm{Cb}(\{\langle\lambda, a\rangle\}) \wedge \|\{\langle\lambda, a\rangle\}\| = \lambda$,

(vi) $\mathrm{Cb}(f) \wedge \mathrm{Cb}(g) \to \mathrm{Cg}(f \vartriangle g) \wedge f \vartriangle g = g \vartriangle f \wedge \|f \vartriangle g\| = \|f\| + \|g\|$,

(vii) $\mathrm{Cb}(f) \wedge \mathrm{Cb}(g) \wedge \mathrm{Cb}(h) \to (f \vartriangle g) \vartriangle h = f \vartriangle (g \vartriangle h)$,

(viii) $\mathrm{Cb}(g) \wedge \forall f \in \mathrm{dom}(g) \cdot \mathrm{Cb}(f) \to \mathrm{Cb}(\Delta(g)) \wedge \|\Delta(g)\| = \sum_{f \in \mathrm{dom}(g)} \|f\|^{g'f}$,

(ix) $\mathrm{Cb}(f) \wedge \forall x \in \mathrm{dom}(f) \cdot \mathrm{Nat}(x) \to \mathrm{Nat}(\Sigma^* f) \wedge \mathrm{Nat}(\Pi^* f)$,

(x) $\mathrm{Cb}(f) \wedge \mathrm{Cb}(g) \wedge \forall x \in \mathrm{dom}(f) \cdot \mathrm{Nat}(x)$
$\wedge \forall x \in \mathrm{dom}(g) \cdot \mathrm{Nat}(x) \to \forall x \in \mathrm{dom}(f \vartriangle g) \cdot \mathrm{Nat}(x)$
$\wedge \Sigma^*(f \vartriangle g) = \Sigma^* f + \Sigma^* g \wedge \Pi^*(f \vartriangle g) = (\Pi^* f) \cdot (\Pi^* g)$,

(xi) $\Sigma^* 0 = 0 \wedge \Sigma^* \langle\langle\lambda\rangle\rangle = \lambda \wedge (\mu \neq 0 \to \Sigma^* \{\langle\mu, \lambda\rangle\} = \mu \cdot \lambda)$
$\wedge \Pi^* 0 = 1 \wedge \Pi^* \langle\langle\lambda\rangle\rangle = \lambda \wedge (\mu \neq 0 \to \Pi^* \{\langle\mu, \lambda\rangle\} = \lambda^\mu)$,

(xii) $\mathrm{Cb}(\{\{a\}\}) \wedge \|\{\{a\}\}\| = \bar{\bar{a}}$,

(xiii) $\mathrm{Fnc}(f) \to \overline{\overline{\mathrm{dom}(f)}} = \|\overline{\mathrm{rg}}(f)\|$,

(xiv) $\mathrm{Cb}(f) \wedge f \neq 0 \to \exists p \in \mathrm{dom}(f) \cdot \exists g (\mathrm{Cb}(g) \wedge f = g \vartriangle \langle\langle p\rangle\rangle)$,

(xv) $p_1 \neq p_2 \wedge p_1 \neq p_3 \wedge \cdots \wedge p_{n-1} \neq p_n$
$\wedge \lambda_1 \neq 0 \wedge \cdots \wedge \lambda_n \neq 0 \to \mathrm{Cb}(\{\langle\lambda_1, p_1\rangle, \ldots, \langle\lambda_n, p_n\rangle\})$
$\wedge \Sigma^* \{\langle\lambda_1, p_1\rangle, \ldots, \langle\lambda_n, p_n\rangle\} = \lambda_1 p_1 + \cdots + \lambda_n p_n$
$\wedge \Pi^* \{\langle\lambda_1, p_1\rangle, \ldots, \langle\lambda_n, p_n\rangle\} = p_1^{\lambda_1} \cdots p_n^{\lambda_n}$.

D.13.6. (i) $\mathrm{Prime}(\lambda) \Longleftrightarrow \forall \mu < \lambda \forall \nu < \lambda (\mu \cdot \nu \neq \lambda) \wedge \lambda \neq 0 \wedge \lambda \neq 1$.

(ii) $\mathrm{PFtr}(f) \Longleftrightarrow \mathrm{Ftr}(f) \wedge \forall x \in \mathrm{dom}(f)\, \mathrm{Prime}(x)$.

T.13.11. (*Factorization theorem*).

$$\lambda \neq 0 \to \exists ! f (\mathrm{PFtr}(f) \wedge \lambda = \Pi^* f).$$

Proof. Existence proof is as usual and by course-of-values induction on λ. Of course, we use the fact that

$$\mathrm{Prime}(\lambda) \wedge \neg \mathrm{Prime}(\lambda).$$

It holds since "Prime" is an RF in some conservative expansion of FCS. Then, we proceed as usual:

$$\mathrm{Prime}(\lambda)\rightharpoonup\mathrm{PFtr}(\langle\langle\lambda\rangle\rangle)\wedge\lambda=\Pi^*\langle\langle\lambda\rangle\rangle.$$

$$\lambda=1\rightharpoonup\mathrm{PFtr}(0)\wedge\lambda=\Pi^*0,$$

$$\lambda\neq 0\wedge\lambda\neq 1\wedge\neg\mathrm{Prime}(\lambda)\rightharpoonup\exists\mu<\lambda\exists\nu<\lambda(\lambda=\mu\nu),$$

$$\mathrm{PFtr}(f)\wedge\mathrm{PFtr}(g)\wedge\mu=\Pi^*f$$

$$\wedge\,\nu=\Pi^*g\rightharpoonup\mathrm{PFtr}(f\vartriangle g)\wedge\mu\nu=\Pi^*(f\vartriangle g).$$

From these

$$\forall\mu<\lambda(\mu\neq 0\rightharpoonup\exists f(\mathrm{PFtr}(f)\wedge\mu=\Pi^*f)$$

$$\vdash\lambda\neq 0\rightharpoonup\exists f(\mathrm{PFtr}(f)\wedge\lambda=\Pi^*f),$$

and the course-of-values induction is complete.

To prove the uniqueness we shall follow a simple proof due to T. Takagi [1]. First it is obvious that

$$\mathrm{PFtr}(f)\wedge\lambda=\Pi^*f\rightharpoonup f\subseteq\lambda\times\lambda.$$

In view of this it suffices to prove

$$\lambda\geq 2\rightharpoonup\forall f\in P(\lambda\times\lambda)\cdot\forall g\in P(\lambda\times\lambda)\cdot(\mathrm{PFtr}(f)$$

$$\wedge\,\mathrm{PFtr}(g)\wedge\lambda=\Pi^*f=\Pi^*g\rightharpoonup f=g).$$

Denote this ΣF by $A(\lambda)$. We prove it by course-of-values induction on λ:

$$\forall\mu<\lambda A(\mu)\vdash A(\lambda).$$

Now

$$\mathrm{Cb}(f)\wedge\lambda=\Pi^*f\wedge\lambda\geq 2\vdash f\neq 0\wedge\mathrm{Cb}(f)$$

$$\vdash\exists p\in\mathrm{dom}\,f\exists g(\mathrm{Cb}(g)\wedge f=g\vartriangle\langle\langle p\rangle\rangle).$$

Hence

$$\mathrm{Cb}(f)\wedge\lambda=\Pi^*f\wedge\lambda\geq 2\vdash\exists p\exists f_1(\mathrm{Cb}(g)\wedge\mathrm{Prime}(p)\wedge\lambda=p\cdot\Pi^*f_1).$$

So it suffices to prove

$$\forall\mu<\lambda A(\mu)\wedge\lambda=p\cdot\Pi^*f_1=q\cdot\Pi^*g_1\wedge\mathrm{Cb}(f_1)\wedge\mathrm{Cb}(g_1)$$

$$\wedge\,\mathrm{Prime}(p)\wedge\mathrm{Prime}(q)\vdash\langle\langle p\rangle\rangle\vartriangle f_1=\langle\langle q\rangle\rangle\vartriangle g_1.$$

Denote the left-hand side formula by B.

$$B\wedge p=q\vdash\Pi^*f_1=\Pi^*g_1<\lambda\wedge\mathrm{PFtr}(f_1)\wedge\mathrm{PFtr}(g_1).$$

Hence using $\forall\mu<\lambda A(\mu)$, we have

(10) $$B\wedge p=q\vdash p=q\wedge f_1=g_1\vdash\langle\langle p\rangle\rangle\vartriangle f_1=\langle\langle q\rangle\rangle\vartriangle g_1.$$

On the other hand

$$B\wedge p<q\wedge\mu=(q\dot{-}p)\times\Pi^*g_1\wedge q\dot{-}p=\Pi^*h\wedge\mathrm{PFtr}(h)$$

$$\wedge\,\Pi^*f_1\dot{-}\Pi^*g_1=\Pi^*h'\wedge\mathrm{PFtr}(h')\vdash\mu<\lambda$$

$$\wedge\,\mu=\Pi^*h\cdot\Pi^*g_1=\Pi^*(h\vartriangle g_1)$$

$$\wedge\,\mu=p\cdot(\Pi^*f_1\dot{-}\Pi^*g_1)=p\cdot\Pi^*(h')$$

$$=\Pi^*(\langle\langle p\rangle\rangle\vartriangle h').$$

Let the left-hand side be Γ. Using $\forall\mu<\lambda A(\mu)$ again, we have

$$\Gamma\vdash p\vartriangle h'=h\vartriangle g_1\vdash p\in\mathrm{dom}(h)\vee p\in\mathrm{dom}(g_1).$$

But we can easily show

$$p<q\wedge\mathrm{Prime}(p)\wedge\mathrm{Prime}(q)\wedge q\dot{-}p=\Pi^*h\vdash p\notin\mathrm{dom}(h).$$

Hence

$$\Gamma\vdash p\in\mathrm{dom}(g_1).$$

Hence

(11) $$\Gamma\vdash\exists g_2(\mathrm{Cb}(g_2)\wedge g_1=\langle\langle p\rangle\rangle\vartriangle g_2).$$

Hence

$$\Gamma,\ \mathrm{Cb}(g_2),\ g_1=\langle\langle p\rangle\rangle\vartriangle g_2\vdash\lambda=p\cdot\Pi^*f_1=q\cdot p\cdot\Pi^*g_2$$

$$\vdash\Pi^*f_1=q\cdot\Pi^*g_2=\Pi^*(\langle\langle q\rangle\rangle\vartriangle g_2)\wedge\Pi^*f_1<\lambda.$$

Using $\forall\mu<\lambda A(\mu)$ once more, we obtain

$$\begin{aligned} \Gamma,\ \mathrm{Cb}(g_2),\ g_1=\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}g_2 \vdash f_1 &= \langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}g_2 \\ \vdash\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}f_1 &= \langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}\langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}g_2 \\ &= \langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}g_2 \\ &= \langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}g_1. \end{aligned}$$

Thus

$$\Gamma,\ \exists g_2(\mathrm{Cb}(g_2)\wedge g_1=\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}g_2)\vdash\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}f_1=\langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}g_1.$$

By (11)

$$\Gamma\vdash\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}f_1=\langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}g_1.$$

So by $(\exists E)$

(12) $$B,\ p<q\vdash\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}f_1=\langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}g_1.$$

Similarly

(13) $$B,\ p>q\vdash\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}f_1=\langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}g_1.$$

(11), (12), (13) with **T.13.2** (ix) show

$$B\vdash\langle\langle p\rangle\rangle\mathbin{\scriptstyle\triangle}f_1=\langle\langle q\rangle\rangle\mathbin{\scriptstyle\triangle}g_1,$$

as was to be proved. **q.e.d.**

D.13.7. (i) $\mathrm{Prim}(\lambda,\ \mu)\Leftrightarrow\neg\exists\nu\leq\lambda(1<\nu\wedge\nu|\lambda\wedge\nu|\mu)$

(ii) $\mathrm{GCD}(\lambda,\ \mu)=\nu\Leftrightarrow\nu|\lambda\wedge\nu|\mu<\mathrm{Prim}(\lambda/\nu,\ \mu/\nu)$

(iii) $\mathrm{LCM}(\lambda,\ \mu)=\lambda\mu/\mathrm{GCD}(\lambda,\ \mu)$

T.13.12. (i) $\exists\nu_1\exists\nu_2\exists\nu_3\exists\nu_4\exists\xi(\lambda\nu_1-\mu\nu_2=\xi\wedge\lambda=\nu_3\xi\wedge\mu=\nu_4\xi)$

(ii) $\mathrm{Prim}(\lambda,\ \mu)\rightarrow\exists\nu_1\exists\nu_2(\lambda\nu_1\mathbin{\dot{-}}\mu\nu_2=1)$

(iii) $\mathrm{GCD}(\lambda,\ \mu)|\lambda\wedge\mathrm{GCD}(\lambda,\ \mu)|\mu$

(iv) $\nu|\lambda\wedge\nu|\mu\rightarrow\nu|\mathrm{GCD}(\lambda,\ \mu)$

(v) $\lambda|\mathrm{LCM}(\lambda,\ \mu)\wedge\mu|\mathrm{LCM}(\lambda,\ \mu)$

(vi) $\lambda|\nu\wedge\mu|\nu\rightarrow\mathrm{LCM}(\lambda,\ \mu)|\nu$

Proof is omitted.

Now, Fermat's small theorem:

$$\mathrm{Prim}(p)\wedge\lambda\not\equiv 0\ (\mathrm{mod.}\,p)\to\lambda^{p-1}\equiv 1\ (\mathrm{mod.}\,p),$$

can be proved in FCS with its usual proof (e.g. group theoretic one, since classification of elements of a finite set is available in FCS).

The existence of primitive root congruent modulo a prime:

$$\mathrm{Prim}(p)\to\exists\lambda(\lambda^{p-1}\equiv 1\ (\mathrm{mod.}\,p)\wedge\forall i<p-1\ (\lambda^{i}\not\equiv 1\ (\mathrm{mod.}\,p))),$$

can also be proved by a similar method. The same holds in case of prime power.

Lagrange's theorem:

$$\exists\lambda_1\exists\lambda_2\exists\lambda_3\exists\lambda_4(\mu=\lambda_1^2+\lambda_2^2+\lambda_3^2+\lambda_4^2),$$

as well as other similar results concerning the sum of two or three squares, can be proved in FCS. (e.g. the proofs of these theorems in Landau [1] can be formalized into FCS without difficulty.)

Wilson's theorem and the quadratic law of reciprocity can be proved in FCS, because they can be proved by finite combinatorial methods.

The theory of quadratic diophantine equations and quadratic forms (e.g. of two indeterminates) can be formalized in FCS.

14. Recursion Theorem

We shall prove a form of recursion theorem. Before stating the theorem we shall define the notion of a Σ-formula with Σ-predicate variable X with n argument places, which we shortly call a Σ^+-formula or a $\sum^+$F.

14.1. *Inductive definition of Σ^+-semiformula (abbreviated $\sum^+$F').*

1° *Every* RF' *is a* $\sum^+$F'.

2° *If $t_1,\dots,t_n$ are semi-terms, then $Xt_1\cdots t_n$ is a* $\sum^+$F'.

3° *If A and B are* $\sum^+$F', *then $\vee AB$, $\wedge AB$ are* $\sum^+$F'.

4° *If A is a* $\sum^+$F' *and t is a semi-term, then $\forall x\in tA$, $\exists x\in tA$ and $\exists xA$ are* $\sum^+$F'.

Now that we have defined the notion of Σ^{+}-semiformula, we define Σ^{+}-formulas just the same way as we defined Σ-formulas from Σ-semiformulas. Σ^{+}-formulas contain the predicate variable X only in their positive parts. We shall write also $X(t_1,\dots, t_n)$ instead of $Xt_1\cdots t_n$.

14.2. Let $v_0, v_1,\dots$ are enumeration of *bound* variables. Let m be a non-negative integer.

For a semi-term t or an RF′ φ, we define t_{+m} or φ_{+m} as follows:

1° $0_{+m}\asymp 0$,

2° $(v_i)_{+m}\asymp v_{i+m}$,

3° $a_{+m}\asymp a$, where a is a free variable,

4° $(\# st)_{+m}\asymp \#^\frown s_{+m}{}^\frown t_{+m}$,

5° $(\in st)_{+m}\asymp \in^\frown s_{+m}{}^\frown t_{+m}$,

6° $(\neg\varphi)_{+m}\asymp\neg^\frown\varphi_{+m}$,

7° $(\vee\varphi\psi)_{+m}\asymp\vee^\frown\varphi_{+m}{}^\frown\psi_{+m}$,

8° $(\wedge\varphi\psi)_{+m}\asymp\wedge^\frown\varphi_{+m}{}^\frown\psi_{+m}$,

9° $(\rightharpoonup\varphi\psi)_{+m}\asymp\rightharpoonup^\frown\varphi_{+m}{}^\frown\psi_{+m}$,

10° $(\exists v_i\in t\varphi)_{+m}\asymp\exists v_{i+m}\in^\frown t_{+m}{}^\frown\varphi_{+m}$,

11° $(\forall v_i\in t\varphi)_{+m}\asymp\forall v_{i+m}\in t_{+m}{}^\frown\varphi_{+m}$.

Namely, t_{+m} or φ_{+m} is obtained from t or φ, respectively, by replacing each bound variable v_i by v_{i+m}.

14.3. Next we define the substitution of $\sum$F $C(a_1,\dots, a_n)$ (or rather $\lambda a_1\cdots a_nC(a_1,\dots, a_n)$) for X in a $\sum^{+}$F′ A in the following obvious way (the result of substitution is denoted by $A[C]$): Suppose the bound variables in C are among $v_0,\dots, v_{m-1}$.

1° If φ is an RF′, then $\varphi[C]$ is φ_{+m}.

2° $(Xt_1\cdots t_n)[C]\asymp C(t_1,\dots, t_n)$.

3° $(\vee AB)[C]\asymp\vee^\frown A[C]^\frown B[C]$.

4° $(\wedge AB)[C]\asymp\wedge^\frown A[C]^\frown B[C]$.

5° $(\rightharpoonup\varphi A)[C]\asymp\rightharpoonup^\frown\varphi[C]^\frown A[C]$,

6° $(\forall v_i\in tA)[C]\asymp\forall v_{i+m}\in t_{+m}{}^\frown A[C]$,

7° $(\exists v_i\in tA)[C]\asymp\exists v_{i+m}\in t_{+m}{}^\frown A[C]$,

8° $(\exists v_iA)[C]\asymp\exists v_{i+m}{}^\frown A[C]$.

Moreover we define $A[a]$, where a is a variable, to be

$$A[\lambda b_1 \cdots b_n(\langle b_1, \ldots, b_n\rangle \in a)].$$

Lemma 14.1. (i) *If* $C(a_1, \ldots, a_n)$, $\Gamma \vdash D(a_1, \ldots, a_n)$, *where* $a_1, \ldots, a_n$ *are not in* Γ, *then* $A[C]$, $\Gamma \vdash A[D]$, *in particular*,

(ii) $a \subseteq b$, $A[a] \vdash A[b]$,

(iii) $A[C] \vdash \exists x(\mathrm{Rel}_n(x) \wedge A[x] \wedge \forall y_1 \in \mathrm{Tc}(x) \cdots \forall y_n \in \mathrm{Tc}(x)$

$(\langle y_1, \ldots, y_n\rangle \in x \rightharpoonup C(y_1, \ldots, y_n)))$,

and hence,

(iv) $A[C] \vdash \exists x \exists d(\mathrm{Rel}_n(x) \wedge A_d[x] \wedge \forall y_1 \in \mathrm{Tc}(x) \cdots \forall y_n \in \mathrm{Tc}(x)$

$(\langle y_1, \ldots, y_n\rangle \in x \rightharpoonup C(y_1, \ldots, y_n)))$.

Proof. (i) It is obvious since X occurs in A only in its positive parts. Formally, use the induction on A.

(iii) We also use the induction on A. For the sake of brevity we prove it only for $n=1$, that is,

$$A[C] \vdash \exists x(A[x] \wedge \forall y \in \mathrm{Tc}(x)(y \in x \rightharpoonup C(y))).$$

Let us denote by $A^*(x)$ the formula $A[x] \wedge \forall y \in \mathrm{Tc}(x)\ (y \in x \rightharpoonup C(y))$.

1° If A is an RF, then A does not contain X. So we may take 0 as x. Since in this case $A[C] \asymp A[x] \asymp A$, we easily have

$$A[C] \vdash A[0] \wedge \forall y \in \mathrm{Tc}(0)(y \in 0 \rightharpoonup C(y)).$$

2° A is Xt. Then $A[C]$ is $C(t)$ and $A[x]$ is $t \in x$. The assertion follows from the fact that

$$C(t) \vdash A[\{t\}] \wedge \forall y \in \mathrm{Tc}(\{t\})(y \in \{t\} \rightharpoonup C(y)).$$

3° A is $\vee A_1 A_2$. Then $A[C]$ and $A[x]$ are $\vee {}^\frown A_1[C]^\frown A_2[C]$ and $\vee {}^\frown A_1[x]^\frown A_2[x]$, respectively. By the induction hypothesis we have $\vdash \exists x_1 A_1^*(x_1)$ and $\vdash \exists x_2 A_2^*(x_2)$. From these we easily have the assertion.

4° A is $\wedge A_1 A_2$. Then $A[C]$ is $\wedge {}^\frown A_1[C]^\frown A_2[C]$ and $A[x]$ is $\wedge {}^\frown A_1[x]^\frown A_2[x]$. Using (i) we can easily prove

$$A_1^*(x_1),\ A_2^*(x_2) \vdash (A_1 \wedge A_2)^*(x_1 \cup x_2).$$

So we have the assertion since $\vdash\exists x_1 A_1^*(x_1)$ and $\vdash\exists x_2 A_2^*(x_2)$ by the induction hypothesis.

5° A is $\rightharpoondown\varphi A_2$. Similar to the case 3°.

6° A is $\exists v_i \in t A_1(v_i)$. Then $A[C]$ is $\exists v_{i+m} \in t_{+m} A_1(v_{i+m})[C]$. By the induction hypothesis, we have

$$(A_1(c))[C] \vdash \exists x_1((A_1(c))^*(x_1)).$$

From this the assertion easily follows.

7° A is $\exists v_i A_1(v_i)$. Similar to the last case.

8° A is $\forall v_i \in t A_1(v_i)$. By the induction hypothesis we have

$$(A_1(c))[C] \vdash \exists x_1((A_1(c))^*(x_1)).$$

Hence by (restricted) generalization,

$$\forall v_{i+m} \in t_{+m}(A_1(v_{i+m})[C]) \vdash \forall v_{i+m} \in t_{+m} \exists x_1 (A_1(v_{i+m}))^*(x_1).$$

So by Theorem 4.5 (iii),

$$A[C] \vdash \exists z(\forall v_{i+m} \in t_{+m} \exists x_1 \in z(A_1(v_{i+m}))^*(x_1))$$
$$\wedge \forall x_1 \in z \exists v_{i+m} \in t_{+m}(A_1(v_{i+m}))^*(x_1))).$$

Then

$$A[C],\ \forall v_{i+m} \in t_{+m} \exists x_i \in d(A_1(v_{i+m}))^*(x_1))$$
$$\wedge \forall x_1 \in d \exists v_{i+m} \in t_{+m}(A_1(v_{i+m}))^*(x_1)) \vdash A^*(\cup d).$$

So we have the assertion. (iv) is an immediate consequence of (iii).

q.e.d.

Now we are in a position to prove the following recursion theorem:

Theorem 14.2. *Let* $A(a_1,\dots, a_n)$ *is a* $\sum^+$F. *Then there can be found a* $\sum$F $C(a_1,\dots, a_n)$ *such that*

14.2.1. $(A(a_1,\dots, a_n))[C] \vdash C(a_1,\dots, a_n)$, *and such a* C *is essentially unique in the sense that*

14.2.2. *for any* $\sum$F $D(a_1,\dots, a_n)$, *if*

$$\Gamma,\ (A(a_1,\dots, a_n))[D] \vdash D(a_1,\dots, a_n),$$

where $a_1, \ldots, a_n$ *are distinct free variables not in* Γ, *then*

$$\Gamma,\ C(a_1, \ldots, a_n) \vdash D(a_1, \ldots, a_n),$$

in particular, we have

14.2.3. $(A(a_1, \ldots, a_n))[C] \dashv\vdash C(a_1, \ldots, a_n)$.

14.2.4. *If another* $C_1(a_1, \ldots, a_n)$ *satisfies the conditions* 14.2.1 *and* 14.2.2 *with* C_1 *in place of* C, *then*

14.2.5. $C(a_1, \ldots, a_n) \dashv\vdash C_1(a_1, \ldots, a_n)$.

Proof. The proof of this theorem is a modification of the proof of corresponding theorem in Platek [1] and Takahashi [1]. (Of course some cares are needed because our underlying logic here is intuitionistic.) For notational simplicity, we only prove the case where $n=1$.
Let

$$U_A(w, r) = \{z \in w \mid A_w(z)[r]\}.$$

Formal definition of it is

$$y = U_A(w, r) \Longleftrightarrow y \subseteq w \wedge \forall z \in w(z \in y \rightleftarrows A_w(z)[r]).$$

By Theorem 12.3 it defines a function. U_A is monotonic, i.e.

$$w \subseteq w',\quad r \subseteq r' \vdash U_A(w, r) \subseteq U_A(w', r').$$

Now

$$\mathrm{Trans}(w) \vdash \exists! f(f \mathrm{Fn}\, w \wedge \forall t \in w(f't = U_A(w, \cup(f''t)))).$$

Let $V(f, w)$ be the formula

$$\mathrm{Trans}(w) \wedge f \mathrm{Fn}\, w \wedge \forall t \in w(f't = U_A(w, \cup(f''t))).$$

Then we have the following monotonicities:

$$V(f, w),\quad t \in w,\quad s \in \overline{\mathrm{T}}\mathrm{c}(t) \vdash f's \subseteq f't$$

and

$$V(f, w),\quad V(g, w'),\quad w \subseteq w',\quad t \in w \vdash f't \subseteq g't.$$

The proof is by induction, using the above-mentioned monotonicity of U_A.

Now we put

$$C(a) \Longleftrightarrow \exists f \exists w \exists x \in w(V(f, w) \wedge a \in f'x).$$

We have only to show that the $C(a)$ is the desired $\sum$F. First we prove

$$A(a)[C] \vdash C(a).$$

By Lemma 14.1 (iii)

(1) $$A(a)[C] \vdash \exists u(A_q(a)[u] \wedge \forall y \in uC(y)).$$

Using the theorem of replacement (Theorem 4.5 (ii)) we have

$$\forall y \in uC(y) \vdash \exists k \forall y \in u \exists f \in k \exists w \in k \exists x \in w$$
$$(\mathrm{Trans}(w) \wedge V(f, w) \wedge y \in f'x).$$

From this with the use of the monotonicities and the uniqueness of f, we have

(2) $$\forall y \in uC(y) \vdash \exists f \exists w \forall y \in u \exists x \in w$$
$$(\mathrm{Trans}(w) \wedge V(f, w) \wedge y \in f'x \wedge w \supseteq q \wedge a \in w).$$

We claim

(3) $$\mathrm{Trans}(w), \quad V(f, w), \quad \forall y \in u \exists x \in w(y \in f'x), \quad A_q(a)[u],$$
$$q \subseteq w, \quad a \in w, \quad V(g, w \# w) \vdash a \in g'w.$$

Since $\forall y \in u \exists x \in w(y \in f'x)$, by monotinicity

$$y \in f'x \subseteq g'x.$$

Hence from the assumptions we have $\forall y \in u(y \in \bigcup(g''w))$, i.e., $u \subseteq \bigcup(g''w)$. Since $A_q(a)[u]$, $q \subseteq w \subseteq w \# w$ and $u \subseteq \bigcup(g''w)$, we have $A_w(a)[\bigcup(g''w)]$. Since $a \in w \subseteq w \# w$, by the definition of U_A, $a \in U_A(w \# w, \bigcup(g''w)) = g'w$. This proves (3). Hence on account of (1) and (2), we have

$$A(a)\,[C] \vdash \exists g \exists w(\mathrm{Trans}\,(w) \wedge V(g,\ w \# w) \wedge a \in g'w)\,.$$

From this it follows that

$$A(a)\,[C] \vdash C(a)\,.$$

Next let

$$(4) \qquad \Gamma,\ (A(a))\,[D] \vdash D(a)\,.$$

We claim that

$$(5) \qquad V(f,\ w),\ \Gamma \vdash c \in w \rightharpoonup \forall x \in f'cD(x)\,.$$

In order to prove it by the induction on c, we prove

$$V(f,\ w),\ \Gamma,\ \forall y \in c(y \in w \rightharpoonup \forall x \in f'yD(x)) \vdash c \in w \rightharpoonup \forall x \in f'cD(x)\,.$$

It suffices to prove

$$(6) \qquad V(f,\ w),\ \Gamma,\ c \in w,\ \forall y \in c \forall x \in f'yD(x) \vdash \forall x \in f'cD(x)\,.$$

Now

$$V(f,\ w),\ c \in w,\ \forall y \in c \forall x \in f'yD(x) \vdash \forall y \in \cup\,(f''c) \cdot D(y)\,.$$

Hence

$$V(f,\ w),\ \Gamma,\ c \in w,\ \forall y \in c \forall x \in f'yD(x),\ A_w(a)\,[\cup\, f''c]$$

$$\vdash A_w(a)\,[D] \vdash A(a)\,[D] \vdash D[a]\,.$$

Here we have used the assumption.
On the other hand, by the definition of $f'c$,

$$V(f,\ w),\ c \in w,\ a \in f'c \vdash A_w(a)\,[\cup\, f''c]\,.$$

Thus,

$$V(f,\ w),\ \Gamma,\ c \in w,\ \forall y \in c \forall x \in f'yD(x),\ a \in f'c \vdash D[a]\,.$$

From this, (6) and hence (5) follows.

By (5) we can easily obtain

$$\Gamma,\ C(a)\vdash D(a).$$

This proves 14.2.2. In order to obtain 14.2.3, let $D(a_1,\dots,a_n)$ be $A(a_1,\dots,a_n)[C]$. Then by 14.2.1,

$$D(a_1,\dots,a_n)\vdash C(a_1,\dots,a_n).$$

Hence by Lemma 14.1 (i),

$$A(a_1,\dots,a_n)[D]\vdash A(a_1,\dots,a_n)[C],$$

that is,

$$A(a_1,\dots,a_n)[D]\vdash D(a_1,\dots,a_n).$$

So, by 14.2.2 with Γ empty,

$$C(a_1,\dots,a_n)\vdash D(a_1,\dots,a_n),$$

that is,

$$C(a_1,\dots,a_n)\vdash A(a_1,\dots,a_n)[C].$$

This with 14.2.1 yields 14.2.3. 14.2.4 is obvious from 14.2.1 and 14.2.2.

q.e.d.

Let $A(a_1,\dots,a_n)$ be a $\sum^+$F. Then by Theorem 14.2 we can define a $\sum$F $C(a_1,\dots,a_n)$ satisfying 14.2.1 and 14.2.2. We denote the relation between A and C by

$$C(a_1,\dots,a_n)\overset{\text{ind}}{\Longleftrightarrow}A(a_1,\dots,a_n)[C],$$

and say that C is inductively defined by this equivalence (as its least solution). For instance by the equivalence

$$C(a)\overset{\text{ind}}{\Longleftrightarrow}\forall x\in a\exists y\in xC(y),$$

a $\sum$F $C(a)$ is defined (up to the equivalence).

15. Miscellaneous Development

By Theorem 12.16, we can define

D.15.1. (i) $\mathrm{R}(x) = \bigcup(\mathrm{P}''(\mathrm{R} \restriction (x)))(= \bigcup\{\mathrm{P}\,\mathrm{R}(y) | y \in x\})$.

(ii) $\mathrm{Ra}(x) = \bigcup(\mathrm{S}''(\mathrm{Ra} \restriction (x)))(= \bigcup\{\mathrm{S}''\,\mathrm{Ra}(y) | y \in x\})$.

(iii) $S\,\mathrm{trans}(a) \Longleftrightarrow \mathrm{Trans}(a) \wedge \forall x \in a \forall y \in \mathrm{P}(x)(y \in a)$.

T.15.1. (i) $\mathrm{R}(0) = 0 \wedge \mathrm{Ra}(0) = 0$,

(ii) $\mathrm{Nat}(\mathrm{Ra}(a))$,

(iii) $S\,\mathrm{trans}(\mathrm{R}(a))$,

(iv) $\mathrm{R}\,\mathrm{S}(a) = \mathrm{P}\,\mathrm{R}(a) \wedge \mathrm{Ra}\,\mathrm{S}(a) = \mathrm{S}\,\mathrm{Ra}(a)$,

(v) $\mathrm{R}\,\mathrm{P}(a) = \mathrm{P}\,\mathrm{R}(a) \wedge \mathrm{Ra}\,\mathrm{P}(a) = \mathrm{S}\,\mathrm{Ra}(a)$,

(vi) $\mathrm{R}\,\mathrm{R}(a) = \mathrm{R}(a) \wedge \mathrm{Ra}\,\mathrm{Ra}(a) = \mathrm{Ra}(a)$,

(vii) $\mathrm{R}\,\mathrm{Ra}(a) = \mathrm{R}(a) \wedge \mathrm{Ra}\,\mathrm{R}(a) = \mathrm{Ra}(a)$,

(viii) $\mathrm{Nat}(a) \rightharpoonup \mathrm{Ra}(a) = a$.

(ix) $\exists x(\mathrm{Nat}(x) \wedge a \in \mathrm{R}(x))$.

(x) $a \in b \rightharpoonup \mathrm{Ra}(a) < \mathrm{Ra}(b) \wedge \mathrm{R}(a) \in \mathrm{R}(b)$.

(xi) $a \subseteq b \rightharpoonup \mathrm{Ra}(a) \leq \mathrm{Ra}(b) \wedge \mathrm{R}(a) \subseteq \mathrm{R}(b)$.

(xii) $b \in \mathrm{R}(v) \rightleftharpoons \mathrm{Ra}(b) < v$.

(xiii) $\mathrm{R}(v) \subseteq \mathrm{R}(\mathrm{S}(v))$.

(xiv) $v = \mathrm{Ra}(a) \rightleftharpoons a \in \mathrm{R}(\mathrm{S}(v)) - \mathrm{R}(v)$.

We omit the proof of **T.15.1.**

Theorem 15.2. *If $A(a), \Gamma \vdash \exists x \in a A(x)$, where a is not in $A(x)$ or in Γ, then $A(a), \Gamma \vdash \curlywedge$.*

Proof. Define $S(n, b, y; a, x)$ inductively by

$$S(n, b, y; a, x) \overset{\mathrm{ind}}{\Longleftrightarrow} (n = 0 \wedge b = a \wedge y = x)$$

$$\vee \exists m \exists c \exists z (n = \mathrm{S}(m) \wedge b \in c \wedge A_y(b) \wedge \mathrm{S}(m, c, z; a, x)).$$

($A_y(b)$ is the notation introduced in Section 6.) First we claim that

(1) $\quad \Gamma, A_x(a) \vdash \exists b \exists y(S(n, b, y; a, x) \wedge A_y(b) \wedge \mathrm{Ra}(b) + n \leq \mathrm{Ra}(a))$,

by the induction on n.

$$\Gamma, A_x(a) \vdash \exists b \exists y(S(0, b, y; a, x) \wedge A_y(b) \wedge \mathrm{Ra}(b) + 0 \leq \mathrm{Ra}(a)),$$

is obvious. We have to show

$$\Gamma,\ A_x(a),\ \exists b\exists y(S(n,\ b,\ y;\ a,\ x)\wedge A_y(b)\wedge \mathrm{Ra}(b)+n\leq \mathrm{Ra}(a))$$

$$\vdash \exists d\exists u(S(\mathrm{S}(n),\ d,\ u;\ a,\ x)\wedge A_u(d)\wedge \mathrm{Ra}(d)+\mathrm{S}(n)\leq \mathrm{Ra}(a)).$$

This follows from

$$\Gamma,\ A_x(a),\ S(n,\ b,\ y;\ a,\ x),\ A_y(b)\vdash \exists x\in b\exists u A_u(x)$$

(by assumption) and

$$\Gamma,\ A_x(a),\ S(n,\ b,\ y;\ a,\ x),\ d\in b,\ A_u(d),\ \mathrm{Ra}(b)+n\leq \mathrm{Ra}(a)$$

$$\vdash S(\mathrm{S}(n),\ d,\ u;\ a,\ x)\wedge A_u(d)\wedge \mathrm{Ra}(d)+\mathrm{S}(n)\leq \mathrm{Ra}(a).$$

Now we have (1). Then, taking $n=\mathrm{S}(\mathrm{Ra}(a))$, we obtain

$$\Gamma,\ A_x(a)\vdash \exists b\exists y(S(n,\ b,\ y;\ a,\ x)\wedge A_y(b)\wedge \mathrm{Ra}(b)+\mathrm{S}(\mathrm{Ra}(a))\leq \mathrm{Ra}(a)).$$

But obviously we have

$$\neg \mathrm{Ra}(b)+\mathrm{S}(\mathrm{Ra}(a))\leq \mathrm{Ra}(a),$$

since $\neg(l+n+1\leq n)$. So $\Gamma,\ A_x(a)\vdash\curlywedge$ and hence $\Gamma,\ A(a)\vdash\curlywedge$. **q.e.d.**

Corollary 15.3. *If* $A(a,\ b),\ \Gamma\vdash \exists x\in a\exists y\in b A(x,\ y)$, *where* a *and* b *are distinct and not occurring in* $A(x,\ y)$ *or in* Γ, *then* $A(a,\ b),\ \Gamma\vdash\curlywedge$.

Proof. The same as the theorem.

These theorem and corollary provide us with a method of proving some uniqueness results.

Corollary 15.4. *If*

$$A(c_1,\ b)\wedge A(c_2,\ b)\wedge c_1\neq c_2,\ \Gamma\vdash \exists y\in b\exists x_1\exists x_2(A(x_1,\ y)$$

$$\wedge A(x_2,\ y)\wedge x_1\neq x_2),$$

then $\Gamma,\ A(c_1,\ b),\ A(c_2,\ b)\vdash c_1=c_2$. (*The proof is omitted.*)

We can prove the following variations of inductive schemata, the meaning of which are obvious.

Theorem 15.5.

(i) $$\frac{r \subseteq a \times a,\ b \in a,\ \forall y \in a(\langle yb\rangle \in r \rightharpoonup A(y)),\ \Gamma \vdash A(b)}{r \subseteq a \times a,\ \Gamma \vdash \forall x \in a A(x)}$$

(ii) $$\frac{b \in a,\ \forall y \in a(b \in y \rightharpoonup A(y)),\ \Gamma \vdash A(b)}{\Gamma \vdash \forall x \in a A(x)}$$

(iii) $$\frac{A(a),\ \Gamma \vdash \exists x(x \subsetneqq a \wedge A(x))}{A(a),\ \Gamma \vdash \curlywedge}$$

(iv) $$\frac{b \subseteq a,\ \forall y \subseteq a(b \subsetneqq y \rightharpoonup A(y)),\ \Gamma \vdash A(b)}{\Gamma \vdash \forall x \subseteq a A(x)}$$

(v) $$\frac{b \subseteq a,\ \forall y \subseteq a(y \subsetneqq b \rightharpoonup A(y)),\ \Gamma \vdash A(b)}{\Gamma \vdash \forall x \subseteq a A(x)}$$

(vi) $$\frac{\Gamma \vdash A(0) \text{ and } b \subsetneqq a,\ A(b),\ \Gamma \vdash \exists y \in a(y \notin b \wedge A(b \# y))}{b \subseteq a,\ \Gamma \vdash A(b).}$$

The proofs of these schemata are omitted.

D.15.2. (i) $a \prec b \overset{\text{ind}}{\Longleftrightarrow} \exists y \in b \forall x \in a(x \prec y)$,

(ii) $a \preceq b \overset{\text{ind}}{\Longleftrightarrow} \forall x \in a \exists y \in b(x \preceq y)$.

Then we have

Theorem 15.6. (i) $\vdash a \prec b \vee b \preceq a$

(ii) $a \prec b,\ b \preceq a \vdash \curlywedge$.

In other words, $(a \prec b,\ b \preceq a)$ *and* $(b \preceq a,\ a \prec b)$ *constitute* ΔF's.

Proof. (i) By the induction principle of Theorem 7.2 (iii). It suffices to prove

$$\forall x \in a \forall y \in b(x \prec y \vee y \preceq x) \vdash a \prec b \vee b \preceq a.$$

This follows from

$$\forall x \in a \forall y \in b(x \prec y \vee y \preceq x) \vdash \exists y \in b \forall x \in a(x \prec y)$$
$$\vee \forall y \in b \exists x \in a(y \preceq x).$$

Now we show (ii) by using Corollary 15.3. It suffices to prove

$$a \prec b \wedge b \preceq a \vdash \exists x \in a \exists y \in b(x \prec y \wedge y \preceq x).$$

But this comes easily from the facts that

$$a \prec b \vdash \exists y \in b \forall x \in a (x \prec y)$$

and that

$$b \preceq a \vdash \forall y \in b \exists x \in a (y \preceq x) . \qquad \textbf{q. e. d.}$$

Now that we see $(a \prec b,\ b \preceq a)$ is a ΔF, we can expand our system by definition of $\prec$. Then we may well use such formulas as $\neg a \prec b$, $a \prec b \rightarrow a \preceq b$. The same holds for $a \preceq b$.

T.15.7. (i) $a \prec b \rightarrow a \preceq b$

(ii) $a \preceq a$

(iii) $\neg a \prec a$

(iv) $\neg (a \prec b \wedge b \preceq a)$

(v) $\neg (a \prec b \wedge b \prec a)$

(vi) $a \preceq b \wedge b \preceq a \rightarrow a = b$

(vii) $a \preceq b \rightarrow a = b \vee a \prec b.$

(viii) $a \preceq b \wedge b \preceq c \rightarrow a \preceq c$

(ix) $a \prec b \wedge b \preceq c \rightarrow a \prec c$

(x) $a \preceq b \wedge b \prec c \rightarrow a \prec c$

(xi) $a \prec b \wedge b \prec c \rightarrow a \prec c$

(xii) $a \prec b \vee a = b \vee b \prec a$

(xiii) $a \in b \rightarrow a \prec b$

(xiv) $a \subseteq b \rightarrow a \preceq b$

(xv) $a \subsetneqq b \rightarrow a \prec b$

(xvi) $a \preceq b \rightarrow a \subseteq \mathrm{R}(b) \wedge a \in \mathrm{PR}(b)$.

(xvii) $b \notin a \rightarrow a \prec a \# b \wedge b \prec a \# b.$

(xviii) $a \neq 0 \rightarrow \exists y \in a \forall x \in a (x \preceq y) \wedge \exists y \in a \forall x \in a (y \preceq x)$.

Theorem 15.8. (i) *If* $A(a)$ *is a* $\sum$F *and if*

$$\forall x \in p\mathrm{R}(b) \cdot (x \prec b \rightarrow A(x)),\ \Gamma \vdash A(b) .$$

Then $\Gamma \vdash A(s)$, *for each term* s.

(ii) *If* $\varphi(a)$ *is an* RF *in an expansion of* FCS *by definition, then*

$$\exists x \varphi(x) \vdash \exists x (\varphi(x) \wedge \forall y \in \mathrm{PR}(x) \cdot (y \prec x \rightarrow \neg \varphi(y))) .$$

(iii) *If* $A(n_1, a)$, $A(n_2, a)$, $n_1 \neq n_2$, Γ

$$\vdash \exists x \exists m_1 \exists m_2 (x \prec a \wedge A(m_1, x) \wedge A(m_2, x) \wedge m_1 \neq m_2),$$

then we have

$$A(n_1, a),\ A(n_2, a),\ \Gamma \vdash n_1 = n_2.$$

Proof. Similar to that of Theorem 15.2.

Theorem 15.9. (*Uniformization theorem*). *Let* $A(a, b)$ *be a* $\sum$F. *Then there exists a* $\sum$F $B(a, b)$ *such that*

(i) $B(a, b) \vdash A(a, b)$,

(ii) $\exists y A(a, b) \vdash \exists y B(a, b)$,

(iii) $B(a, b_1), B(a, b_2) \vdash b_1 = b_2$.

Proof. As usual. Let $B(a, b)$ be

$$\exists u (A_u(a, b) \wedge \forall x \in \mathrm{PR}(\langle u, b\rangle) \cdot \forall y \in \mathrm{PR}(\langle u, b\rangle) \cdot$$

$$(\langle x, y\rangle \prec \langle u, b\rangle \rightharpoonup \neg A_x(a, y)).$$

Note that $A_x(a, y)$ is an RF. **q.e.d.**

D.15.3. (i) $J(n, a) \Longleftrightarrow \forall m \in n \exists x (x \prec a \wedge J(m, x))$

$$\wedge \forall x \in \mathrm{PR}(a) (x \prec a \rightharpoonup \exists m \in n J(m, x)).$$

T.15.10. (i) $\vdash \exists ! n J(n, a)$

(ii) $J(n, a) \vdash \mathrm{Nat}(n)$

(iii) $\mathrm{Nat}(n) \vdash \exists ! a J(n, a)$.

Proof. (i) $\exists n J(n, a)$ is proved by the induction on a along $\prec$ (Theorem 15.8 (i)), as follows.

$$\forall x \in \mathrm{PR}(a) (x \prec a \rightharpoonup \exists m J(m, x))$$

$$\vdash \forall x \in \mathrm{PR}(a) \exists m (x \prec a \rightharpoonup J(m, x))$$

$$\vdash \exists n (\forall x \in \mathrm{PR}(a) \exists m \in n (x \prec a \rightharpoonup J(m, x))$$

$$\wedge \forall m \in n \exists x \in \mathrm{PR}(a) (x \prec a \wedge J(m, x))$$

$$\vdash \exists n(\forall m \in n \exists x(x \prec a \wedge J(m, x))$$

$$\wedge \forall x \in \mathrm{PR}(a)(x \prec a \rightarrow \exists m \in n J(m, x)))$$

$$\vdash \exists n J(n, a).$$

The induction is complete.
On account of Theorem 15.8 (iii), the uniqueness, i.e.,

$$J(n_1, a), \quad J(n_2, a) \vdash n_1 = n_2$$

will follow from

$$J(n_1, a), \quad J(n_2, a), \quad n_1 \neq n_2$$

$$\vdash \exists x \exists m_1 \exists m_2(x \prec a \wedge J(m_1, x) \wedge J(m_2, x) \wedge m_1 \neq m_2).$$

We prove the latter as follows:

$$n_1 \neq n_2 \vdash \exists x((x \in n_1 \wedge x \notin n_2) \vee (x \notin n_1 \wedge x \in n_2))$$

$$J(n_1, a), \quad m_1 \in n_1, \quad m_1 \notin n_2$$

$$\vdash \exists x(x \prec a \wedge J(m_1, x))$$

$$J(n_2, a), \quad b \prec a \vdash \exists m_2 \in n_2 J(m_2, x)$$

$$m_1 \notin n_2, \quad J(m_1, b), \quad m_2 \in n_2, \quad J(m_2, b)$$

$$\vdash J(m_1, b) \wedge J(m_2, b) \wedge m_1 \neq m_2$$

$$J(n_1, a), \quad J(n_2, a), \quad m_1 \in n_1, \quad m_1 \notin n_2$$

$$\vdash \exists x \exists m_1 \exists m_2(x \prec a \wedge J(m_1, x) \wedge J(m_2, x) \wedge m_1 \neq m_2).$$

Similarly

$$J(n_1, a), \quad J(n_2, a), \quad m_2 \notin n_1, \quad m_2 \in n_2$$

$$\vdash \exists x \exists m_1 \exists m_2(x \prec a \wedge J(m_1, x) \wedge J(m_2, x) \wedge m_1 \neq m_2).$$

So

$$J(n_1, a), \quad J(n_2, a), \quad n_1 \neq n_2$$

$$\vdash \exists x \exists m_1 \exists m_2 (x \prec a \wedge J(m_1, x) \wedge J(m_2, x) \wedge m_1 \neq m_2).$$

Now the proof of (i) is complete.

(ii) First we prove

$$J(n, a) \vdash \mathrm{Trans}(n),$$

i.e.

$$J(n, a), \quad m \in n, \quad l \in m \vdash l \in n.$$

By the recursion theorem

$$J(n, a), \quad m \in n \vdash \exists x(x \prec a \wedge J(m, x))$$

$$J(m, b), \quad l \in m \vdash \exists y(y \prec b \wedge J(l, y))$$

$$c \prec b, \quad b \prec a \vdash c \prec a$$

$$c \prec a, \quad J(n, a) \vdash \exists k \in n J(k, c)$$

$$k \in n, \quad J(l, c), \quad J(k, c) \vdash l = k \wedge l \in n \vdash l \in n.$$

Hence

$$J(l, c), \quad c \prec b, b \prec a, \quad J(n, a) \vdash l \in n.$$

Hence

$$b \prec a, \quad J(m, b), \quad l \in m, \quad J(n, a) \vdash l \in n$$

$$J(n, a), \quad m \in n, \quad l \in m \vdash l \in n,$$

as desired.

(iii) Similar to (i) but use Theorem 13.3 (ii) and Corollary 15.4.

q.e.d.

D.15.4. $J(\mathrm{T}(a), a)$.

This definition is justified by **T.15.10** (i). By **T.15.10** (i), (ii) and (iii), T maps R_ω onto natural numbers. This is a formalization of the function t introduced in Section 1.

By **T. 15.10**, we have

T.15.11. (i) $\mathrm{Nat}(\mathrm{T}(a))$,

(ii) $\mathrm{T}(a)=\mathrm{T}(b)\rightarrow a=b$,

(iii) $\exists!a(\mathrm{T}(a)=n)$.

16. Formalizing Formal Systems into FCS

According to the program suggested in section 1, we shall consider in this section the problem of formalizing formal systems (especially finistic logical calculi) into FCS. To examplify this let us adopt, as the formal system to be formalized, just this system FCS under consideration.

As suggested in section 1, let us assume that formal objects of FCS such as terms, formulas and proofs are h.f. sets. To fix the idea, semi-term 0 is the h.f. set $\langle 0, 0\rangle$ $(=\{\{\emptyset\}\}$ and denoted also by $\ulcorner 0\urcorner$), free variables are h.f. sets of form $\langle 1, x\rangle$, where x is an arbitrary h.f. set, bound variables are of the form $\langle 2, x\rangle$, and $\# st$ is $\langle\ulcorner\#\urcorner, s, t\rangle$, where $\ulcorner\#\urcorner$ is 3 (1, 2, 3 are von Neumann ordinals as h.f. sets). Hence semi-term (which we denote by Term′) is defined inductively as follows:

$$(1)\qquad \mathrm{Term}'(a)\overset{\mathrm{ind}}{\Longleftrightarrow}(\boldsymbol{\exists}x)(\boldsymbol{\exists}y)(a=\langle 0, 0\rangle$$

$$\boldsymbol{\vee}\, a=\langle 1, x\rangle$$

$$\boldsymbol{\vee}\, a=\langle 2, x\rangle$$

$$\boldsymbol{\vee}\,(a=\langle 3, x, y\rangle\,\boldsymbol{\wedge}\,\mathrm{Term}'(x)\,\boldsymbol{\wedge}\,\mathrm{Term}'(y))).$$

Here boldface $\boldsymbol{\exists}$, $\boldsymbol{\vee}$, $\boldsymbol{\wedge}$ are the logical connectives in the metalanguage. Term′ is defined as the least solution of this equivalence. Note that this is an informal definition of semi-term (in the informal theory of h.f. sets and should not be confused with a formal definition (in the formal theory FCS of h.f. sets). Nevertheless the right-hand side of (1) would become a $\sum^{+}$F (c.f. Section 14) if the boldfaces are replaced by lightfaces. Then by the recursion theorem in FCS, the modified (1) defines a $\sum$F, say $\mathrm{Term}'^{*}(a)$ up to the equivalence. This $\mathrm{Term}'^{*}(a)$ is called the formalization of the notion of semi-term.

For each of other notions we can proceed similarly, as far as it is defined by the same form as a $\sum$F explicitly or a $\sum^{+}$F inductively.

It would be confusing if each informal notion and the corresponding formal notion were denoted by the same symbols. So we distinguish them by boldfaces and lightfaces. That is, informal notions are written in boldfaces and formal notions are written in lightfaces. However, we shall sometimes use ↄ to indicate formal notions when lightfaces were already used for informal notions. Moreover when no confusion seems to arise, two corresponding notions may be written by the same letters or symbols. (0, 1, 2, 3, etc. are such examples.)

We shall write down only formal definitions, because the corresponding informal definitions are then obtained automatically.

Also, for the sake of notational simplicity, we shall omit writing the left-most existential quantifiers in the right-hand side of each definition. This convention will be used in both formal and informal definitions and only in definitions. For instance, the formalized (1) is written simply:

D.16.1. $\mathrm{Term}'(a) \overset{\mathrm{ind}}{\Longleftrightarrow} (a = \langle 0, 0\rangle$

$\vee\, a = \langle 1, x\rangle$

$\vee\, a = \langle 2, x\rangle$

$\vee\, (a = \langle 3, x, y\rangle \wedge \mathrm{Term}'(x) \wedge \mathrm{Term}'(y)))$.

Term, constant (Const), free variable (FV), bound variable (BV) and variable (Var) are defined by

D.16.2. (i) $\mathrm{Term}(a) \overset{\mathrm{ind}}{\Longleftrightarrow} a = \langle 0, 0\rangle$

$\vee\, a = \langle 1, x\rangle$

$\vee\, (a = \langle 3, x, y\rangle \wedge \mathrm{Term}(x) \wedge \mathrm{Term}(y))$

(ii) $\mathrm{Const}(a) \overset{\mathrm{ind}}{\Longleftrightarrow} a = \langle 0, 0\rangle$

$\vee\, (a = \langle 3, x, y\rangle \wedge \mathrm{Const}(x) \wedge \mathrm{Const}(y))$,

RF′ *and* ∑F′ *are defined by*

(iii) $\mathrm{RF}'(a) \overset{\mathrm{ind}}{\Longleftrightarrow} (a = \langle \ulcorner \in \urcorner, x, y\rangle \wedge \mathrm{Term}'(x) \wedge \mathrm{Term}'(y))$

$\vee (a = \langle \ulcorner \rightharpoondown \urcorner, x \rangle \wedge \mathrm{RF}'(x))$
$\vee (a = \langle \ulcorner \wedge \urcorner, x, y \rangle \wedge \mathrm{RF}'(x) \wedge \mathrm{RF}'(y))$
$\vee (a = \langle \ulcorner \vee \urcorner, x, y \rangle \wedge \mathrm{RF}'(x) \wedge \mathrm{RF}'(y))$
$\vee (a = \langle \ulcorner \rightharpoonup \urcorner, x, y \rangle \wedge \mathrm{RF}'(x) \wedge \mathrm{RF}'(y))$
$\vee (a = \langle \ulcorner \forall \urcorner, x, y, z \rangle \wedge \mathrm{BV}(x) \wedge \mathrm{Term}'(y) \wedge \mathrm{RF}'(z))$
$\vee (a = \langle \ulcorner \exists \urcorner, x, y, z \rangle \wedge \mathrm{BV}(x) \wedge \mathrm{Term}'(y) \wedge \mathrm{RF}'(z))$

where $\ulcorner \in \urcorner = 4$, $\ulcorner \rightharpoondown \urcorner = 5$, $\ulcorner \wedge \urcorner = 6$, $\ulcorner \vee \urcorner = 7$, $\ulcorner \rightharpoonup \urcorner = 8$,
$\ulcorner \forall \urcorner = 9$, $\ulcorner \exists \urcorner = 10$.

(iv) $\sum \mathrm{F}'(a) \overset{\mathrm{ind}}{\Longleftrightarrow} \mathrm{RF}'(a)$
$\vee (a = \langle \ulcorner \wedge \urcorner, x, y \rangle \wedge \sum \mathrm{F}'(x) \wedge \sum \mathrm{F}'(y))$
$\vee (a = \langle \ulcorner \vee \urcorner, x, y \rangle \wedge \sum \mathrm{F}'(x) \wedge \sum \mathrm{F}'(y))$
$\vee (a = \langle \ulcorner \rightharpoonup \urcorner, x, y \rangle \wedge \mathrm{RF}'(x) \wedge \sum \mathrm{F}'(y))$
$\vee (a = \langle \ulcorner \forall \urcorner, x, y, z \rangle \wedge \mathrm{BV}(x) \wedge \mathrm{Term}'(y) \wedge \sum \mathrm{F}'(z))$
$\vee (a = \langle \ulcorner \exists \urcorner, x, y, z \rangle \wedge \mathrm{BV}(x) \wedge \mathrm{Term}'(y) \wedge \sum \mathrm{F}'(z))$
$\vee (a = \langle \ulcorner \exists . \urcorner, x, y \rangle \wedge \mathrm{BV}(x) \wedge \sum \mathrm{F}'(y))$,

where $\ulcorner \exists . \urcorner = 11$.

Next we define the predicate $\tilde{V}(p, a)$ that a is a semi-term or a $\sum \mathrm{F}'$ and p is the set of all the variables occurring in a as free.

D.16.3. (i) $\tilde{V}(p, a) \overset{\mathrm{ind}}{\Longleftrightarrow} (a = \ulcorner 0 \urcorner \wedge p = 0)$
$\vee (\mathrm{Var}(a) \wedge p = \{a\})$
$\vee (a = \langle \ulcorner \# \urcorner, y, z \rangle \wedge \mathrm{Term}'(y) \wedge \mathrm{Term}'(z) \wedge \tilde{V}(p_1, y)$
$\wedge \tilde{V}(p_2, z) \wedge p = p_1 \cup p_2)$
$\vee (a = \langle \ulcorner \in \urcorner, y, z \rangle \wedge \mathrm{Term}'(y) \wedge \mathrm{Term}'(z) \wedge \tilde{V}(p_1, y)$
$\wedge \tilde{V}(p_2, z) \wedge p = p_1 \cup p_2)$
$\vee (a = \langle \ulcorner \rightharpoondown \urcorner, y \rangle \wedge \mathrm{RF}'(y) \wedge \tilde{V}(p, y))$
$\vee (a = \langle \ulcorner \vee \urcorner, y, z \rangle \wedge \sum \mathrm{F}'(y) \wedge \sum \mathrm{F}'(z)$
$\wedge \tilde{V}(p_1, y) \wedge \tilde{V}(p_2, z) \wedge p = p_1 \cup p_2)$
$\vee (a = \langle \ulcorner \wedge \urcorner, y, z \rangle \wedge \sum \mathrm{F}'(y) \wedge \sum \mathrm{F}'(z)$
$\wedge \tilde{V}(p_1, y) \wedge \tilde{V}(p_2, z) \wedge p = p_1 \cup p_2)$
$\vee (a = \langle \ulcorner \rightharpoonup \urcorner, y, z \rangle \wedge \mathrm{RF}'(y) \wedge \sum \mathrm{F}'(z)$
$\wedge \tilde{V}(p_1, y) \wedge \tilde{V}(p_2, z) \wedge p = p_1 \cup p_2)$
$\vee (a = \langle \ulcorner \forall \urcorner, y, z, u \rangle \wedge \mathrm{BV}(y) \wedge \mathrm{Term}'(z)$
$\wedge \sum \mathrm{F}'(u) \wedge \tilde{V}(p_1, z)$
$\wedge \tilde{V}(p_2, z) \wedge p = (p_2 - \{y\}) \cup p_1)$

$$\begin{aligned}
&\vee (a=\langle\ulcorner\exists\urcorner,\ y,\ z,\ u\rangle \wedge \mathrm{BV}(y) \wedge \mathrm{Term}'(z)\\
&\wedge \textstyle\sum \mathrm{F}'(u) \wedge \tilde{V}(p_1,\ z) \wedge \tilde{V}(p_2,\ z) \wedge p=(p_2-\{y\}) \cup p_1)\\
&\vee (a\langle\ulcorner\exists.\urcorner,\ y,\ z\rangle \wedge \mathrm{BV}(y) \wedge \textstyle\sum \mathrm{F}'(z)\\
&\wedge \tilde{V}(p_1,\ z) \wedge p=p_1-\{y\}).
\end{aligned}$$

Then RF *and* $\sum$F *are defined by*

(ii) $\mathrm{RF}(a) \Longleftrightarrow \mathrm{RF}'(a) \wedge \tilde{V}(p, a) \wedge \forall x \in p\mathrm{FV}(x)$.

(iii) $\sum \mathrm{F}(a) \Longleftrightarrow \sum \mathrm{F}'(a) \wedge \tilde{V}(p, a) \wedge \forall x \in p\mathrm{FV}(x)$.

Note that

T.16.1. $\tilde{V}(p, a) \vdash (\mathrm{Term}'(a) \vee \sum \mathrm{F}'(a)) \wedge \forall x \in p(\mathrm{FV}(x) \vee \mathrm{BV}(x))$.

Proof. Let $\mathfrak{A}(p, a, \tilde{V})$ be the $\sum^{+}$F which has defined $\tilde{V}$ inductively above, and let $\tilde{V}'$ be the right-hand side formula of 16.1. Then it is easy to verify that

$$\mathfrak{A}(p,\ a,\ \tilde{V}') \vdash \tilde{V}'(p,\ a).$$

Hence by the recursion theorem,

$$\tilde{V}(p,\ a) \vdash \tilde{V}'(p,\ a),$$

as was to be proved.

D.16.4. $\mathrm{Seq}(\Gamma) \Longleftrightarrow \forall A \in \Gamma(\Sigma \mathrm{F}(A))$.

Let us define

D.16.5. (i) $r \overset{\circ}{\#} s=\langle\ulcorner\#\urcorner,\ r,\ s\rangle$,

(ii) $r \overset{\circ}{\in} s=\langle\ulcorner\in\urcorner,\ r,\ s\rangle$,

(iii) $\overset{\circ}{\neg} A=\langle\ulcorner\neg\urcorner,\ A\rangle$,

(iv) $A \overset{\circ}{\vee} B=\langle\ulcorner\vee\urcorner,\ A,\ B\rangle$,

(v) $A \overset{\circ}{\wedge} B=\langle\ulcorner\wedge\urcorner,\ A,\ B\rangle$,

(vi) $A \overset{\circ}{\rightharpoonup} B=\langle\ulcorner\rightharpoonup\urcorner,\ A,\ B\rangle$,

(vii) $\overset{\circ}{\forall} x \overset{\circ}{\in} rA=\langle\ulcorner\forall\urcorner,\ x,\ r,\ A\rangle$,

(viii) $\overset{\circ}{\exists} x \overset{\circ}{\in} rA=\langle\ulcorner\exists\urcorner,\ x,\ r,\ A\rangle$,

(ix) $\overset{\circ}{\exists} xA=\langle\ulcorner\exists.\urcorner,\ x,\ A\rangle$,

(x) $r \overset{\circ}{\subseteq} s = \overset{\circ}{\forall} x \overset{\circ}{\in} r (x \overset{\circ}{\in} s)$, *where* $x = \langle 2, 0 \rangle$,

(xi) $(r \overset{\circ}{=} s) = (r \overset{\circ}{\subseteq} s) \overset{\circ}{\wedge} (s \overset{\circ}{\subseteq} r)$.

D.16.6. (i) $\mathrm{Sb}(A', A; t, x)$ (A' *is the result of substituting* t *for* x *in* A)$\Longleftrightarrow \mathrm{Var}(x) \wedge \mathrm{Term}'(t) \wedge ((A = \ulcorner 0 \urcorner \wedge A' = A)$

$$\begin{aligned}
&\vee (A = x \wedge A' = t)\\
&\vee (\mathrm{Var}(A) \wedge A \neq x \wedge A' = A)\\
&\vee ((A = B \overset{\circ}{\#} C) \wedge (A' = B' \overset{\circ}{\#} C') \wedge \mathrm{Term}'(B) \wedge \mathrm{Term}'(C)\\
&\quad \wedge \mathrm{Sb}(B', B; t, x) \wedge \mathrm{Sb}(C', C; t, x))\\
&\vee ((A = B \overset{\circ}{\in} C) \wedge (A' = B' \overset{\circ}{\in} C') \wedge \mathrm{Term}'(B) \wedge \mathrm{Term}'(C)\\
&\quad \wedge \mathrm{Sb}(B', B; t, x) \wedge \mathrm{Sb}(C', C; t, x))\\
&\vee ((A = \overset{\circ}{\neg} B) \wedge (A' = \overset{\circ}{\neg} B') \wedge \mathrm{RF}'(B) \wedge \mathrm{Sb}(B', B; t, x))\\
&\vee ((A = B \overset{\circ}{\vee} C) \wedge (A' = B \overset{\circ}{\vee} C') \wedge \textstyle\sum \mathrm{F}'(B) \wedge \textstyle\sum \mathrm{F}'(C)\\
&\quad \wedge \mathrm{Sb}(B', B; t, x) \wedge \mathrm{Sb}(C', C; t, x))\\
&\vee ((A = B \overset{\circ}{\wedge} C) \wedge (A' = B \overset{\circ}{\wedge} C') \wedge \textstyle\sum \mathrm{F}'(B) \wedge \textstyle\sum \mathrm{F}'(C)\\
&\quad \wedge \mathrm{Sb}(B', B; t, x) \wedge \mathrm{Sb}(C', C; t, x))\\
&\vee ((A = B \overset{\circ}{\rightharpoonup} C) \wedge (A' = B' \overset{\circ}{\rightharpoonup} C') \wedge \mathrm{RF}'(B) \wedge \textstyle\sum \mathrm{F}'(C)\\
&\quad \wedge \mathrm{Sb}(B', B; t, x) \wedge \mathrm{Sb}(C', C; t, x))\\
&\vee ((A = \overset{\circ}{\forall} x \overset{\circ}{\in} u B) \wedge (A' = \overset{\circ}{\forall} x \overset{\circ}{\in} u' B) \wedge \mathrm{Term}'(u) \wedge \textstyle\sum \mathrm{F}'(B)\\
&\quad \wedge \mathrm{Sb}(u', u; t, x))\\
&\vee ((A = \overset{\circ}{\exists} x \overset{\circ}{\in} u B) \wedge (A' = \overset{\circ}{\exists} x \overset{\circ}{\in} u' B) \wedge \mathrm{Term}'(u) \wedge \textstyle\sum \mathrm{F}'(B)\\
&\quad \wedge \mathrm{Sb}(u', u, t, x))\\
&\vee ((A = \overset{\circ}{\exists} x B) \wedge A' = A \wedge \textstyle\sum \mathrm{F}'(B))\\
&\vee ((A = \overset{\circ}{\forall} y \overset{\circ}{\in} u B) \wedge (A' = \overset{\circ}{\forall} y \overset{\circ}{\in} u' B') \wedge y \neq x \wedge \mathrm{BV}(y) \wedge \mathrm{Term}'(u)\\
&\quad \wedge \textstyle\sum \mathrm{F}'(B) \wedge \mathrm{Sb}(u', u; t, x) \wedge \mathrm{Sb}(B', B; t, x))\\
&\vee ((A = \overset{\circ}{\exists} y \overset{\circ}{\in} u B) \wedge (A' = \overset{\circ}{\exists} y \overset{\circ}{\in} u' B') \wedge y \neq x \wedge \mathrm{BV}(y) \wedge \mathrm{Term}'(u)\\
&\quad \wedge \textstyle\sum \mathrm{F}'(B) \wedge \mathrm{Sb}(u', u; t, x) \wedge \mathrm{Sb}(B', B; t, x))\\
&\vee ((A = \overset{\circ}{\exists} y B) \wedge (A' = \overset{\circ}{\exists} y B') \wedge y \neq x \wedge \mathrm{BV}(y)\\
&\quad \wedge \textstyle\sum \mathrm{F}'(B) \wedge \mathrm{Sb}(B', B; t, x)).
\end{aligned}$$

(ii) $\Gamma \overset{\circ}{\vdash} A \Longleftrightarrow \mathrm{Seq}(\Gamma) \wedge \sum \mathrm{F}(A) \wedge \mathrm{Term}(r) \wedge \mathrm{Term}(s)$

$$\begin{aligned}
&\wedge \mathrm{Term}(t) \wedge \mathrm{RF}(\varphi) \wedge \mathrm{RF}(\psi) \wedge \textstyle\sum \mathrm{F}(B) \wedge \textstyle\sum \mathrm{F}(C) \wedge \textstyle\sum \mathrm{F}'(D)\\
&\wedge (A \in \Gamma\\
&\vee (\Gamma \overset{\circ}{\vdash} r \overset{\circ}{\in} \ulcorner 0 \urcorner)\\
&\vee ((\Gamma \overset{\circ}{\vdash} r \overset{\circ}{\in} s) \wedge (A = r \overset{\circ}{\in} s \overset{\circ}{\#} t))
\end{aligned}$$

$$\begin{aligned}
&\vee ((\Gamma \overset{\circ}{\vdash} r \overset{\circ}{=} s) \wedge (A = r \overset{\circ}{\in} s \overset{\circ}{\#} t))\\
&\vee ((\Gamma \overset{\circ}{\vdash} r \overset{\circ}{\in} s \overset{\circ}{\#} t) \wedge (\Gamma \cup \{r \overset{\circ}{\in} s\} \overset{\circ}{\vdash} A) \wedge (\Gamma \cup \{r \overset{\circ}{=} t\} \overset{\circ}{\vdash} A))\\
&\vee ((\Gamma \cup \{\psi\} \overset{\circ}{\vdash} \varphi) \wedge (\Gamma \cup \{\psi\} \overset{\circ}{\vdash} \overset{\circ}{\neg} \varphi) \wedge (A = \overset{\circ}{\neg} \psi))\\
&\vee ((\Gamma \overset{\circ}{\vdash} \varphi) \wedge (\Gamma \overset{\circ}{\vdash} \overset{\circ}{\neg} \varphi))\\
&\vee ((\Gamma \overset{\circ}{\vdash} B) \wedge (A = B \overset{\circ}{\vee} C))\\
&\vee ((\Gamma \overset{\circ}{\vdash} C) \vee (A = B \overset{\circ}{\vee} C))\\
&\vee ((\Gamma \cup \{B\} \overset{\circ}{\vdash} A) \wedge (\Gamma \cup \{C\} \overset{\circ}{\vdash} A) \wedge (\Gamma \overset{\circ}{\vdash} B \overset{\circ}{\vee} C))\\
&\vee (\Gamma \overset{\circ}{\vdash} A \overset{\circ}{\wedge} B)\\
&\vee (\Gamma \overset{\circ}{\vdash} B \overset{\circ}{\wedge} A)\\
&\vee ((\Gamma \overset{\circ}{\vdash} B) \wedge (\Gamma \overset{\circ}{\vdash} C) \wedge (A = B \overset{\circ}{\vee} C))\\
&\vee ((\Gamma \cup \{\varphi\} \overset{\circ}{\vdash} B) \wedge (A = \varphi \overset{\circ}{\rightarrow} B))\\
&\vee ((\Gamma \overset{\circ}{\vdash} \varphi \overset{\circ}{\rightarrow} A) \wedge (\Gamma \overset{\circ}{\vdash} \varphi))\\
&\vee ((\Gamma \overset{\circ}{\vdash} s \overset{\circ}{\in} r) \wedge (A = \overset{\circ}{\exists} x \overset{\circ}{\in} rD) \wedge (\Gamma \overset{\circ}{\vdash} D') \wedge \mathrm{Sb}(D', D; a, x))\\
&\vee ((\Gamma \overset{\circ}{\vdash} \overset{\circ}{\exists} x \overset{\circ}{\in} rD) \wedge \mathrm{Sb}(D', D; a, x) \wedge (\Gamma \cup \{D'\} \overset{\circ}{\vdash} A))\\
&\vee ((\Gamma \cup \{a \overset{\circ}{\in} r\} \overset{\circ}{\vdash} D') \wedge \mathrm{Sb}(D', D; a, x) \wedge (A = \overset{\circ}{\forall} x \overset{\circ}{\in} rD))\\
&\vee ((\Gamma \overset{\circ}{\vdash} \overset{\circ}{\forall} x \overset{\circ}{\in} rD) \vee (\Gamma \overset{\circ}{\vdash} s \overset{\circ}{\in} r) \wedge \mathrm{Sb}(A, D; s, x))\\
&\vee ((\Gamma \overset{\circ}{\vdash} D') \wedge \mathrm{Sb}(D', D; s, x) \wedge (A = \overset{\circ}{\exists} xD))\\
&\vee ((\Gamma \overset{\circ}{\vdash} \overset{\circ}{\exists} xD) \wedge \mathrm{Sb}(D', D, a, x) \wedge (\Gamma \cup \{D'\} \overset{\circ}{\vdash} A))\\
&\vee ((\Gamma \overset{\circ}{\vdash} D') \wedge (\Gamma \cup \{D'', D'''\} \overset{\circ}{\vdash} D'''') \wedge \textstyle\sum \mathrm{F}(E) \wedge \mathrm{Sb}(D', E, \ulcorner 0 \urcorner, x)\\
&\quad \wedge \mathrm{Sb}(D'', E, a, x) \wedge \mathrm{Sb}(D''', E, b, x) \wedge \mathrm{Sb}(D'''', E, a \overset{\circ}{\#} b, x)\\
&\quad \wedge \mathrm{Sb}(A, E, r, x))).
\end{aligned}$$

Now we have completed defining the system FCS within FCS itself. What we have to do next is to prove in FCS the metatheorems (including particular theorems) about the system FCS which we have proved above. Indeed, all of formalizations of these metatheorems will turn out to be provable in FCS.

For instance the formalization of **T.4.3** (i) is:

T.16.2. $\mathrm{FV}(a) \rightarrow \overset{\circ}{\vdash} a \overset{\circ}{\subseteq} a$.

Proof. This is provable as follows:

$$\mathrm{FV}(a) \wedge \mathrm{FV}(b) \vdash \mathrm{RF}(a \overset{\circ}{\subseteq} a) \wedge \mathrm{RF}(b \overset{\circ}{\in} a),$$

$$\mathrm{FV}(a) \wedge \mathrm{FV}(b) \wedge a \neq b \vdash (\{b \overset{\circ}{\in} a\} \overset{\circ}{\vdash} b \overset{\circ}{\in} a),$$

$$\begin{aligned}
&\mathrm{FV}(a)\wedge \mathrm{FV}(b)\wedge a\neq b \vdash (\overset{\circ}{\vdash} \overset{\circ}{\forall} x \overset{\circ}{\in} a(x \overset{\circ}{\in} a)),\\
&\mathrm{FV}(a)\vdash \exists b(\mathrm{FV}(a)\wedge \mathrm{FV}(b)\wedge a \mathrel{\dot{\neq}} b),\\
&\mathrm{FV}(a)\vdash (\overset{\circ}{\vdash} a \overset{\circ}{\subseteq} a),\\
&\vdash \mathrm{FV}(a)\rightharpoonup (\overset{\circ}{\vdash} a \overset{\circ}{\subseteq} a).
\end{aligned}$$

q. e. d.

By the same way it is clear that the formalization of each particular theorem of FCS is provable in FCS. (A proof is an h.f. set!) Before considering formalization of metatheorems, we need to prove formalization of somewhat trivial facts such as

T.16.3. (i) $\tilde{V}(p, A)\rightharpoonup(\mathrm{Term}'(A)\vee \sum \mathrm{F}'(A))\wedge \forall u\in p\cdot \mathrm{Var}(u)$,

(ii) $(\mathrm{Term}'(A)\vee \sum \mathrm{F}'(A))\rightharpoonup \exists p\tilde{V}(p, A)$,

(iii) $\tilde{V}(p, A)\wedge \tilde{V}(q, A)\rightharpoonup p=q$

(iv) $\mathrm{Sb}(A', A, t, x)\rightharpoonup((\mathrm{Term}'(A')\wedge \mathrm{Term}'(A))\vee(\sum \mathrm{F}'(A')$
$\wedge \sum \mathrm{F}'(A)))\wedge \mathrm{Term}(t)\wedge \mathrm{Var}(x)$.

(v) $(\mathrm{Term}'(A)\vee \sum \mathrm{F}'(A))\wedge \mathrm{Term}(t)\wedge \mathrm{Var}(x)\rightharpoonup \exists A'\mathrm{Sb}(A', A; t, x)$

(vi) $\mathrm{Sb}(A', A; t, x)\wedge \mathrm{Sb}(A'', A, t, x)\rightharpoonup A'=A''$.

Proof. (i) is by induction on $\tilde{V}$. (ii) is by induction on $\sum \mathrm{F}'$. For (iii) use Corollary 15.4. Similarly for (iv), (v) and (vi). **q. e. d.**

Next let us consider e.g. the formalization of metatheorem 4.4 (i), that is,

T.16.4. $\mathrm{FV}(a)\wedge \mathrm{FV}(b)\wedge a\neq b\wedge \mathrm{BV}(a)\wedge \mathrm{Term}'(r)$

$$\wedge \tilde{V}(p, r)\wedge \forall z\in p(\mathrm{BV}(z)\rightharpoonup z=x)\wedge \mathrm{Sb}(x, r, a, x)$$

$$\wedge \mathrm{Sb}(t, r, b, x)\vdash(\{a\overset{\circ}{=}b\}\overset{\circ}{\vdash} s=t).$$

Proof. We can show this as follows:

$$T(r; a, b, x)\Longleftrightarrow \exists p(\tilde{V}(p, r)\wedge \exists s\exists t(\mathrm{Sb}(s, r; a, x)\wedge \mathrm{Sb}(t, r; b, x)$$

$$\wedge \forall z\in p(\mathrm{BV}(z)\rightharpoonup z=x)\rightharpoonup(\{a\overset{\circ}{=}b\}\overset{\circ}{\vdash} s\overset{\circ}{=}t)).$$

Then **T.16.4** will follow from

(2) $\mathrm{FV}(a)\wedge \mathrm{FV}(b)\wedge a\neq b\wedge \mathrm{BV}(x)\wedge \mathfrak{D}(r, T)\vdash T(r; a, b, x)$,

where $\mathfrak{D}(r, T)$ is the $\sum^{+}$F which expresses the inductive definition of Term$'$. The proof of (2) is straightforward. **q.e.d.**

For 4.4 (iii) some difficulty may arise concerning the use of double induction. But in this case it would be overcome easily.

By almost obvious ways we can also prove the formalization of other metatheorems: Theorems 4.4, 4.5, 6.1, 7.2, 8.1 (with Lemmata 8.1.1, 8.1.2, Corollary 8.2), 8.3, 9.1, 9.2.

Moreover we can define in FCS the formalization of expansions by definition of predicates and functions described in Sections 10 and 11 and prove that they are conservative extensions (Theorems 10.1 and 11.1). Also we have in FCS Theorems 11.2, 12.2, 12.3, 12.4 and so on to the results of this section. The first formalized metatheorem, which is impossible to prove in FCS, will be the plausibility theorem for FCS itself of the next section. (It is actually impossible by Gödel's consistency theorem below.) This will be discussed below. Those theorems in later sections which are impossible to prove formally in FCS will be marked by †.

17. The Standard Model $\mathbf{R}_{\omega}$, Plausibility and Completeness Theorems

R_{ω} has been defined in the introduction.

Definition 17.1. Let $A(a_1,\ldots, a_n)$ be a $\sum$F whose free variables are among $a_1,\ldots, a_n$. Let $k_1,\ldots, k_n$ be h.f. sets. Then $R_{\omega}\models A[k_1,\ldots, k_n/a_1,\ldots, a_n]$, or shortly $R_{\omega}\models A[k_1,\ldots, k_n]$, means that A is true in R_{ω} when the variables $a_1,\ldots, a_n$ are interpreted as $k_1,\ldots, k_n$, respectively. R_{ω} is a model of FCS (called the standard model of FCS), that is,

Theorem 17.1† (*Plausibility theorem*). (i) *If* $\vdash A(a_1,\ldots, a_n)$, *then* $R_{\omega}\models A[k_1,\ldots, k_n]$ *for every* $k_1,\ldots, k_n\in R_{\omega}$, *and*

(ii) *If* $\Gamma(a_1,\ldots, a_n)\vdash A(a_1,\ldots, a_n)$, *then if* $R_{\omega}\models\Gamma[k_1,\ldots, k_n]$, (*i.e.*, $R_{\omega}\models B[k_1,\ldots, k_n]$ *for all* $B\in\Gamma$), *then* $R_{\omega}\models A[k_1,\ldots, k_n]$ *for every* $k_1,\ldots, k_n$.

Proof. We can prove (ii) by the induction on $\Gamma\vdash A$. In the case of primitive induction we must also use an informal induction on h.f. set *a*. (i) is a special case of (ii). **q.e.d.**

For later use we give here a formalized inductive definition of truth.

$$\mathrm{Ass}(f) \Longleftrightarrow \mathrm{Fnc}(f) \wedge \forall x \in \mathrm{dom}(f) \cdot \mathrm{Var}(x).$$

$$\mathrm{Val}_1(p, r, f) \overset{\mathrm{ind}}{\Longleftrightarrow} \mathrm{Term}'(r) \wedge \mathrm{Ass}(f)$$

$$\wedge \tilde{V}(v, r) \wedge v \subseteq \mathrm{dom}(f) \wedge ((r = \ulcorner 0 \urcorner \wedge p = 0)$$

$$\vee (\mathrm{Var}(r) \wedge p = f'r)$$

$$\vee (r = s \overset{\circ}{\#} t \wedge \mathrm{Val}_1(p_1, s, f) \wedge \mathrm{Val}_1(p_2, t, f) \wedge p = p_1 \overset{\circ}{\#} p_2)).$$

$$\mathrm{Val}_2(p, \varphi, f) \overset{\mathrm{ind}}{\Longleftrightarrow} \mathrm{RF}'(\varphi) \wedge \mathrm{Ass}(f)$$

$$\wedge \tilde{V}(v, \varphi) \wedge v \subseteq \mathrm{dom}(f)$$

$$\wedge ((\varphi = r \overset{\circ}{\in} s \wedge \mathrm{Val}_1(p_1, r, f) \wedge \mathrm{Val}_1(p_2, s, f)$$

$$\wedge ((p_1 \in p_2 \wedge p = 1) \vee (p_1 \notin p_2 \wedge p = 0)))$$

$$\vee ((\varphi = \overset{\circ}{\neg} \psi) \wedge \mathrm{Val}_2(p_1, \varphi, f) \wedge (p = 1 - p_1))$$

$$\vee ((\varphi = \psi \overset{\circ}{\wedge} \chi) \wedge \mathrm{Val}_2(p_1, \psi, f) \wedge \mathrm{Val}_2(p_2, \chi, f)$$

$$\wedge p = \min(p_1, p_2))$$

$$\vee ((\varphi = \psi \overset{\circ}{\vee} \chi) \wedge \mathrm{Val}_2(p_1, \psi, f) \wedge \mathrm{Val}_2(p_2, \chi, f)$$

$$\wedge p = \max(p_1, p_2))$$

$$\vee ((\varphi = \psi \overset{\circ}{\rightarrow} \chi) \wedge \mathrm{Val}_2(p_1, \psi, f) \wedge \mathrm{Val}_2(p_2, \chi, f)$$

$$\wedge p = \min(1 - p_1, p_2))$$

$$\vee ((\varphi = \overset{\circ}{\forall} x \overset{\circ}{\in} r \psi) \wedge \mathrm{Val}_1(p_1, r, f)$$

$$\wedge ((\forall q \in p_1 \, \mathrm{Val}_2(1, \psi, (f \upharpoonright (\mathrm{dom}(f) - \{x\})) \cup \{\langle q, x \rangle\}) \wedge p = 1)$$

$$\vee (\exists q \in p_1 \, \mathrm{Val}_2(0, \psi, (f \upharpoonright (\mathrm{dom}(f) - \{x\})) \cup \{\langle q, x \rangle\}) \wedge p = 0)))$$

$$\vee ((\varphi = \overset{\circ}{\exists} x \overset{\circ}{\in} r \psi) \wedge \mathrm{Val}_1(p_1, r, f)$$

$$\wedge ((\exists q \in p_1 \mathrm{Val}_2(1, \psi, (f \upharpoonright (\mathrm{dom}(f) - \{x\})) \cup \{\langle q, x \rangle\}) \wedge p = 1)$$

$$\vee (\forall q \in p_1 \mathrm{Val}_2(0, \psi, (f \upharpoonright (\mathrm{dom}(f) - \{x\})) \cup \{\langle q, x \rangle\}) \wedge p = 0)))).$$

$$\mathrm{Tr}(A, f) \overset{\mathrm{ind}}{\Longleftrightarrow} \sum \mathrm{F}'(A) \wedge \mathrm{Ass}(f)$$

$$\wedge \tilde{V}(v, A) \wedge v \subseteq \mathrm{dom}(f)$$

$$\wedge ((\mathrm{RF}'(A) \wedge \mathrm{Val}_2(1, A, f))$$

$$\vee ((A = B \overset{\circ}{\vee} C) \wedge (\mathrm{Tr}(B, f) \vee \mathrm{Tr}(C, f)))$$

$$\vee ((A = B \overset{\circ}{\wedge} C) \wedge \mathrm{Tr}(B, f) \wedge \mathrm{Tr}(C, f))$$

$$\vee ((A = \varphi \overset{\circ}{\rightarrow} C) \wedge (\mathrm{Val}_2(0, \varphi, f) \vee \mathrm{Tr}(C, f)))$$

$$\vee ((A = \overset{\circ}{\exists} x \overset{\circ}{\in} t B) \wedge \mathrm{Val}_1(p, t, f)$$

$$\qquad \wedge \exists q \in p \cdot \mathrm{Tr}(B, (f \upharpoonright (\mathrm{dom}(f) - \{x\})) \cup \{\langle q, x \rangle\}))$$

$$\vee ((A = \overset{\circ}{\forall} x \overset{\circ}{\in} t B) \wedge \mathrm{Val}_1(p, t, f)$$

$$\wedge \forall q \in p \cdot \mathrm{Tr}(B, (f \restriction (\mathrm{dom}(f) - \{x\})) \cup \{\langle q, x\rangle\}))$$
$$\vee ((A = \overset{\circ}{\exists} xB) \wedge \exists q \cdot \mathrm{Tr}(B, (f \restriction (\mathrm{dom}(f) - \{x\})) \cup \{\langle q, x\rangle\}))).$$

Lemma 17.2. *Let r and s be constants in* FCS. *Then,*

(i) *If* $R_\omega \models r \in s$, *then* $\vdash r \in s$;

(ii) *If* $R_\omega \models r \subseteq s$, *then* $\vdash r \subseteq s$;

(iii) *If* $R_\omega \models r = s$, *then* $\vdash r = s$.

Proof. Let us recall that the following (intuitively) true statements hold in FCS:

1° $\vdash 0 \subseteq r$;

2° $s \# t \subseteq r \dashv\vdash s \subseteq r \wedge t \in r$;

3° $t \in 0 \dashv\vdash \curlywedge$;

4° $r \in s \# t \dashv\vdash r \in s \vee r = t$;

5° $t = s \dashv\vdash t \subseteq s \wedge s \subseteq t$.

Hence we can prove the lemma by the induction on the complexity of r and s. **q.e.d.**

Theorem 17.3. (*Completeness theorem*). *Let A be a* $\sum$F *without free variables. If* $R_\omega \models A$, *then* $\vdash A$. (*This kind of completeness theorem was first obtained by Myhill.*)

Proof. First we prove this theorem for RF A. This can be done by the induction on the complexity of A with the use of Lemma 16.2 and the fact that the following true statements hold in FCS:

6° $\vdash \forall x \in 0\, A$

7° $\forall x \in r \# s\, A \dashv\vdash \forall x \in r\, A \wedge A(s/x)$

8° $\exists x \in 0\, A \dashv\vdash \curlywedge$

9° $\exists x \in r \# s\, A \dashv\vdash \exists x \in r\, A \vee A(s/x)$.

Then we prove the theorem for general $\sum$F A. Again this is done by the induction on the complexity of A but with the use of the fact that if $\exists xA$ is true, then $A(s/x)$ is true for some constant s. **q.e.d.**

We remark here that this metatheorem can be formalized and it is provable in FCS. The fact will play an important role in the proof of Gödel's theorem on consistency in the next section.

T.17.4. $\mathrm{Tr}(A, 0) \vdash \overset{\circ}{\vdash} A$. (*Here* A *is a variable.*)

(Note that by our definition of Tr, we have

$$\mathrm{Tr}(A, 0) \vdash \sum \mathrm{F}(A) \wedge \tilde{V}(0, A).)$$

Outline of Proof. The formal proof of this formalized theorem is almost obtained by formalizing the above proof of Theorem 17.3 (with Lemma 17.2). It should be noted that apparent need of double induction suggested in 7° and 9° above can be eliminated, for we can use instead (the formalization of) the following general equivalence:

$7^{\circ\prime}$ If r is a term of the form $(\cdots(0 \# s_1) \# \cdots) \# s_n$, then

$$\forall x \in r A \vdash\dashv A(s_1) \wedge \cdots \wedge A(s_n).$$

(Similarly for $\exists x \in r A$.) **q.e.d.**

However, as mentioned before, the formalization of the plausibility theorem (Theorem 17.1) cannot be proved. Thc reason is because it essentially uses a double induction (see the above outline of proof of it).

Theorem 17.5. *It is not the case that*

$$\tilde{V}(p, a) \wedge \mathrm{Ass}(f) \wedge p \subseteq \mathrm{dom}(f) \wedge (\overset{\circ}{\vdash} a) \vdash \mathrm{Tr}(a, f)$$

and a fortiori not that

$$\tilde{V}(p, a) \wedge \tilde{V}(q, b) \wedge \mathrm{Ass}(f) \wedge p \cup q \subseteq \mathrm{dom}(f) \wedge (a \overset{\circ}{\vdash} b)$$

$$\wedge \mathrm{Tr}(a, f) \vdash \mathrm{Tr}(b, f).$$

Proof. Use the Gödel theorem of next section. **q.e.d.**

Theorem 17.6. (i) *If* $r(a_1, \ldots, a_n)$ *is a semi-term whose variables are among* $a_1, \ldots, a_n$, *then*

$$\mathrm{Val}_1(p, r^*, f) \vdash\dashv \mathrm{Ass}(f) \wedge \{a_1^*, \ldots, a_n^*\} \subseteq \mathrm{dom}(f)$$

$$\wedge p = r(f'a_1^*, \ldots, f'a_n^*).$$

(ii) *If* $\varphi(a_1, \ldots, a_n)$ *is an* RF′ *whose variables are among* $a_1, \ldots, a_n$, *then*

$$\mathrm{Val}_2(p, \varphi^*, f) \dashv\vdash \mathrm{Ass}(f) \wedge \{a_1^*, \ldots, a_n^*\} \subseteq \mathrm{dom}(f)$$

$$\wedge (\varphi(f'a_1^*, \ldots, f'a_n^*) \wedge p = 1)$$

$$\vee (\neg \varphi(f'a_1^*, \ldots, f'a_n^*) \wedge p = 0),$$

(iii) *If* $A(a_1, \ldots, a_n)$ *is a* $\sum \mathrm{F}'$ *whose variables are among* $a_1, \ldots, a_n$, *then*

$$\mathrm{Tr}(A^*, f) \dashv\vdash \mathrm{Ass}(f) \wedge \{a_1^*, \ldots, a_n^*\} \subseteq \mathrm{dom}(f)$$

$$\wedge A(f'a_n^*, \ldots, f'a_n^*),$$

(iv) *If* A *is a* Σ*-sentence, then*

$$A \dashv\vdash \mathrm{Tr}(A^*, 0)$$

and hence

$$A \vdash (\overset{\circ}{\vdash} A^*).$$

Proof. (i) By the induction on the complexity of $r(a_1, \ldots, a_n)$.

(ii) By the induction on the complexity of $\varphi(a_1, \ldots, a_n)$.

(iii) By the induction on the complexity of $A(a_1, \ldots, a_n)$.

(iv) If A is a Σ-sentence, then $A \dashv\vdash \mathrm{Tr}(A^*, 0)$ is a special case of (iii), and we also have $\mathrm{Tr}(A^*, 0) \vdash (\overset{\circ}{\vdash} A^*)$ already by 17.4, and hence $A \vdash (\overset{\circ}{\vdash} A^*)$. **q.e.d.**

18. Gödelization and Gödel's Theorems

D.18.1. $\mathrm{Nm}(b, a) \overset{\mathrm{ind}}{\Longleftrightarrow} (a = 0 \wedge b = 0^*)$

$$\vee (a \neq 0 \wedge c \in a \wedge \forall x \in a (x \leq c) \wedge c \notin d \wedge a = d \# c$$

$$\wedge \mathrm{Nm}(u, d) \wedge \mathrm{Nm}(v, c) \wedge b = u \overset{\circ}{\#} v).$$

Intuitively, $\mathrm{Nm}(b, a)$ means that b is a canonical constant expressing a.

T.18.1. (i) $\vdash \exists! b\, \mathrm{Nm}(b, a)$.

(ii) $\mathrm{Nm}(b, a) \vdash \mathrm{Const}(b) \wedge \mathrm{Val}_1(a, b, 0)$.

Proof. The proof of (i) is similar to that of Theorem 15.10 (i) and so we only prove (ii).

(ii) Let $\mathrm{Nm}'(b, a)$ be $\mathrm{Const}(b) \wedge \mathrm{Val}_1(a, b, 0)$. By the recursion theorem we have only to show

$$(a=0 \wedge b=0^*) \vee (a \neq 0 \wedge c \in a \wedge \forall x \in a(x \preceq c) \wedge c \notin d$$

$$\wedge \mathrm{Nm}'(u, d) \wedge \mathrm{Nm}'(v, c) \wedge b = u \overset{\circ}{\#} v) \vdash \mathrm{Nm}'(b, a).$$

This will follow from

(1) $\mathrm{Const}(0^*) \wedge \mathrm{Val}_1(0, 0^*, 0)$ and

(2) $\mathrm{Const}(u) \wedge \mathrm{Const}(v) \wedge \mathrm{Val}_1(d, u, 0) \wedge \mathrm{Val}_1(c, v, 0)$

$\wedge c \notin d \vdash \mathrm{Const}(u \overset{\circ}{\#} v) \wedge \mathrm{Val}_1(d \# c, u \overset{\circ}{\#} v, 0)$,

both of which are obvious. **q.e.d.**

By Section 11 we can define a function Num as follows:

D.18.2. (i) $\mathrm{Nm}(\mathrm{Num}(a), a)$.

Num is a formalization of * defined in Section 14.

We have immediately

T.18.2. (i) $\mathrm{Const}(\mathrm{Num}(a))$,

(ii) $\mathrm{Val}_1(a, \mathrm{Num}(a), 0)$,

(iii) $\mathrm{Fnc}(f) \wedge \forall x \in \mathrm{dom}(f) \cdot \mathrm{Var}(x) \rightarrow \mathrm{Val}_1(a, \mathrm{Num}(a), f)$.

Lemma 18.3. (*Gödel*). *Let $A(a)$ be a $\sum$F with only free variable a. Then there is a Σ-sentence G such that*

$$G \dashv\vdash A(G^*).$$

Proof. Let z be a fixed variable. We consider the formula

$$\exists y(A(y) \wedge \mathrm{Sb}(y, z, \mathrm{Num}(z), \ulcorner z \urcorner^*)).$$

Call this formula $B(z)$. Let $c=B(z)^*$. (Here we are considering formulas (and also other objects) as h.f sets.) Let G be the Σ-sentence $B(c)$. Then by direct computation we have

$$\vdash \mathrm{Sb}(B(c)^*, B(z)^*, c^*, \ulcorner z \urcorner^*),$$

that is,

$$\vdash \mathrm{Sb}(G^*, c, c^*, \ulcorner z \urcorner^*).$$

But we also have

$$\vdash \mathrm{Num}(c)=c^*.$$

Now

$$\begin{aligned} A(G^*) &\vdash A(G^*) \wedge \mathrm{Sb}(G^*, c, \mathrm{Num}(c), \ulcorner z \urcorner^*) \\ &\vdash \exists y(A(y) \wedge \mathrm{Sb}(y, c, \mathrm{Num}(c), \ulcorner z \urcorner^*) \\ &\vdash B(c) \\ &\vdash G. \end{aligned}$$

On the other hand

$$G \vdash \exists y(A(y) \wedge \mathrm{Sb}(y, c, \mathrm{Num}(c), \ulcorner z \urcorner^*)),$$

$$\begin{aligned} & A(y) \wedge \mathrm{Sb}(y, c, \mathrm{Num}(c), \ulcorner z \urcorner^*) \\ &\vdash A(y) \wedge \mathrm{Sb}(y, c, \mathrm{Num}(c), \ulcorner z \urcorner^*) \wedge \mathrm{Sb}(G^*, c, \mathrm{Num}(c), \ulcorner z \urcorner^*) \\ &\vdash A(y) \wedge y=G^* \\ &\vdash A(G^*). \end{aligned}$$

Hence $G \vdash A(G^*)$. Hence $G \dashv\vdash A(G^*)$. **q.e.d.**

Now we are ready to prove Gödel's incompleteness theorem and the consistency theorem for our system.

Theorem 18.4.[†] (*Gödel's incompleteness theorem*). *There exists a Σ-sentence G such that neither $\vdash G$ nor $G \vdash \curlywedge$.*

Proof. Use the last lemma with $a \overset{\circ}{\vdash} 人^*$ as $A(a)$, to obtain a Σ-sentence G such that $G \dashv\vdash G^* \overset{\circ}{\vdash} 人^*$.

Suppose we have

$$G \vdash 人.$$

Then we must have $\vdash G^* \overset{\circ}{\vdash} 人^*$ and hence $\vdash G$. So we have both $\vdash G$ and $G \vdash 人$ and hence $\vdash 人$. But 人 is not true and hence not provable. This contradiction shows that $G \vdash 人$ is not the case. Moreover since we have just shown that $G^* \overset{\circ}{\vdash} 人^*$ is not true, G is not true and hence not provable. **q.e.d.**

Corollary 18.5. *There is an* RF $\varphi(a)$ *with* a *as its only variable such that it is valid in* R_ω *(by any assignment of h.f. sets to* a*) but not* $\vdash \varphi(a)$.

Proof. Let G be a Σ-sentence such that neither $\vdash G$ nor $G \vdash 人$. Then,

$$G \dashv\vdash \exists y G_y,$$

where G_y is defined in Section 6.

Let $\varphi(a)$ be the RF, $\neg G_a$. In R_ω, G is false and hence $\exists y G_y$ is false so that $\varphi(a)$ is true for any assignment. But if $\vdash \varphi(a)$, then we would have

$$\neg\varphi(a) \vdash 人,$$

$$\exists y \neg\varphi(a) \vdash 人,$$

and

$$G \vdash 人.$$

This is contrary to the assumption. So $\nvdash \varphi(a)$. **q.e.d.**

We can proceed further. The consistency of FCS can be stated as "人 is not provable". This can be formalized as

$$\overset{\circ}{\vdash} 人^* \nvdash 人.$$

(This means $\overset{\circ}{\vdash}\curlywedge^{*}\vdash\curlywedge$ is not the case.) (We cannot negate the formula $\overset{\circ}{\vdash}\curlywedge^{*}$ directly since $\overset{\circ}{\vdash}\curlywedge^{*}$ is a $\sum$F but not an RF.

Theorem 18.6. (*Gödel's theorem on consistency*). *The consistency of* FCS *cannot be proved by a method formalizable in* FCS; *in other words,* $\overset{\circ}{\vdash}\curlywedge^{*}\nvdash\curlywedge$.

Proof. Let G be the sentence having the property

$$G\dashv\vdash G^{*}\overset{\circ}{\vdash}\curlywedge^{*},$$

as constructed in the last theorem. We proved there that $G\nvdash\curlywedge$.

Now assume that $\overset{\circ}{\vdash}\curlywedge^{*}\vdash\curlywedge$. Then we would have a contradiction as follows.

$$G\vdash\overset{\circ}{\vdash}G^{*} \qquad \text{(by Theorem 17.6 (iv))}.$$

But also we have

$$G\vdash G^{*}\overset{\circ}{\vdash}\curlywedge^{*}.$$

Hence

$$\begin{aligned} G&\vdash\overset{\circ}{\vdash}G^{*}\wedge G^{*}\overset{\circ}{\vdash}\curlywedge^{*}\\ &\vdash\overset{\circ}{\vdash}\curlywedge^{*}\\ &\vdash\curlywedge. \end{aligned}$$

So we have $G\vdash\curlywedge$, contrary to the fact we have already seen. **q.e.d.**

We wish to generalize these results in the rest of this section. First we note that we have proved in the proof of the last theorem that

$$G\vdash\overset{\circ}{\vdash}\curlywedge^{*}$$

whenever G satisfies $G\dashv\vdash G\overset{*}{\vdash}\curlywedge^{*}$. In this case the converse $\overset{\circ}{\vdash}\curlywedge^{*}\vdash G$ holds since

$$\overset{\circ}{\vdash}\curlywedge^{*}\vdash G^{*}\overset{\circ}{\vdash}\curlywedge^{*}\vdash G.$$

So it follows that if G satisfies $G \dashv\vdash G^* \overset{\circ}{\vdash} \curlywedge^*$, then G is equivalent to $\overset{\circ}{\vdash} \curlywedge^*$. And there exists such a G. So by substitution we obtain

$$\overset{\circ}{\vdash} \curlywedge^* \dashv\vdash (\overset{\circ}{\vdash} \curlywedge^*)^* \overset{\circ}{\vdash} \curlywedge^*,$$

that is,

Theorem 18.7. *For any Σ-sentence A,*

$$A \dashv\vdash A^* \overset{\circ}{\vdash} \curlywedge^* \quad \textit{iff} \quad A \dashv\vdash \overset{\circ}{\vdash} \curlywedge^*.$$

Theorem 18.8. (*Löb*). (i) *Let A be a Σ-sentence. If $(\overset{\circ}{\vdash} A^*) \vdash A$, then $\vdash A$.*

(ii) *If $(B^* \overset{\circ}{\vdash} A^*) \vdash A$, then $B \vdash A$.*

(iii) $((A \overset{\circ}{\vdash} {}^*)^* \overset{\circ}{\vdash} A^*) \vdash (\overset{\circ}{\vdash} A^*)$,

(iv) $((B^* \overset{\circ}{\vdash} A^*)^* \overset{\circ}{\vdash} A^*) \vdash (B^* \overset{\circ}{\vdash} A^*)$.

(v) *Let*

$$\textstyle\sum \mathrm{S}(a) \Longleftrightarrow \sum \mathrm{F}(a) \wedge \tilde{V}(0, a).$$

Then

$$\textstyle\sum \mathrm{S}(a) \wedge ((\overset{\circ}{\vdash} a)^* \overset{\circ}{\vdash} a) \vdash \overset{\circ}{\vdash} a$$

(vi) $\sum \mathrm{S}(a) \wedge \sum \mathrm{S}(b) \wedge ((b \overset{\circ}{\vdash} a)^* \overset{\circ}{\vdash} a) \vdash (b \overset{\circ}{\vdash} a)$.

(v) *and* (vi) *are formalizations of* (i) *and* (ii).

Proof. We prove only (i). Suppose $(\overset{\circ}{\vdash} A^*) \vdash A$. Let J be a Σ-sentence such that

$$J \dashv\vdash J^* \overset{\circ}{\vdash} A^*. \tag{3}$$

Then, since $J \vdash \overset{\circ}{\vdash} J^*$ (**T.17.6** (iv)),

$$J \vdash \overset{\circ}{\vdash} A^*.$$

Hence by the assumption that $\overset{\circ}{\vdash} A^* \vdash A$, we obtain

$$J \vdash A. \tag{4}$$

Then since $\overset{\circ}{\vdash}$ numeralwise represents $\vdash$, we have

$$\vdash J^* \overset{\circ}{\vdash} A^*.$$

Hence by (3) we have $\vdash J$ and hence by (4) $\vdash A$, as desired. **q.e.d.**

As an application of the well-known proof of Rossor form of incompleteness theorem we can prove

Theorem 18.9. (*Rosser*). (i) *Let A and B be Σ-sentences and assume $B \nvdash A$. Then there is a Σ-sentence C such that $B \nvdash C$ and $C \nvdash A$. Moreover, if $A \vdash B$ in addition, then, the above C can be taken such that $A \vdash C$ and $C \vdash B$. (In other words, C lies strictly between A and B. So the pseudo-order relation $\vdash$ is dense.)*

(ii) *There exist Σ-sentences A and B such that $A \nvdash B$, $B \nvdash A$ and $A \wedge B \vdash \curlywedge$. (So, there are incomparables in the pseudo-order relation $\vdash$.)*

Proof. The first part of (i) comes from the second part of (i). So assume $A \vdash B$. By Lemma 18.3, let R be a $\sum$S such that

$$(5) \qquad R \dashv\vdash \exists y((B^* \overset{\circ}{\wedge} R^* \overset{\circ}{\vdash} A^*)_y \wedge \forall x \in P(R(y)) \cdot (x \preceq y \rightharpoonup$$
$$\rightharpoonup (B^* \overset{\circ}{\vdash} R^* \overset{\circ}{\vee} A^*)_x),$$

where the notation D_x was introduced in Section 6. Let C be $(B \wedge R) \vee A$, (since it is equivalent to $B \wedge (R \vee A)$, by the modular law, we may write $B \wedge R \vee A$). Then it is obvious that $A \vdash C$ and $C \vdash B$.

Suppose $B \vdash C$. Then $B \vdash R \vee A$. Hence for some h.f. set n we have

$$\vdash (B^* \overset{\circ}{\vdash} R^* \overset{\circ}{\vee} A^*)_{n^*}.$$

So by (5) we have

$$(6) \qquad R \dashv\vdash \exists y (y \preceq n^* \wedge (B^* \overset{\circ}{\wedge} R^* \overset{\circ}{\vdash} A^*)_y).$$

But for every h.f. set $k \preceq n$, we have

$$(7) \qquad \vdash \neg (B^* \overset{\circ}{\wedge} R^* \overset{\circ}{\vdash} A^*)_{k^*},$$

for, otherwise we have $B \wedge R \vdash A$ and hence $B \vdash A$ (since we have also $B \vdash R \vee A$). This contradicts the assumption. We also have

(8) $$y\leq n^*\dashv\vdash y=k_1^*\vee\cdots\vee y=k_r^*,$$

where $k_1,\ldots,k_r$ are all h.f. sets preceding n. From (6), (7), and (8) we have

$$R\vdash \text{人},$$

and hence, using $B\vdash R\vee A$, $B\vdash A$. This again is a contradiction. This shows $B\nvdash C$.

Suppose $C\vdash A$. Then $B\wedge R\vdash A$. Hence for some h.f. set n we have

$$\vdash(B^*\overset{\circ}{\wedge}R^*\overset{\circ}{\vdash}A^*)_{n^*}.$$

But we also have

$$\vdash\neg(B^*\overset{\circ}{\vdash}R^*\overset{\circ}{\vee}A^*)_{k^*}$$

for each h.f. sets k and hence by (5) above we have $\vdash R$. But if so we must have $B\vdash A$, since $B\wedge R\vdash A$. This is a contradiction. So $C\nvdash A$.

q.e.d.

19. Characterization of Primitive Recursive Functions

As mentioned in Section 1, a function $f\colon R_\omega\to R_\omega$ is primitive recursive iff $t^{-1}\circ f\circ t\colon N\to N$ is primitive recursive. In this section, we identify R_ω with N via t. We shall characterize primitive recursive functions as provably recursive functions in FCS. (A similar characterization is announced by Mint [1].)

Definition 19.1. We write $\models_n A[m_1,\ldots,m_k]$, if it is true when each unbounded quantifier $\exists x$ in A is interpreted as $\exists x_{x\leq n}$ (but bounded quantifiers are interpreted with their original meaning, e.g., $\exists x\in a$ is *not* interpreted as $\exists x_{x\leq n}(x\in a\wedge\cdots)$).

It is obvious from the definition that

(1) If $n<l$ and $\models_n A[m_1,\ldots,m_k]$, then $\models_l A[m_1,\ldots,m_k]$ and $R_\omega\models A[m_1,\ldots,m_k]$, and

(2) If $R_\omega\models A[m_1,\ldots,m_k]$, then there exists an n such that $\models_n A[m_1,\ldots,m_k]$.

Note that, for an RF φ, $\models_n\varphi$ iff $R_\omega\models\varphi$, since these two interpretations coincide.

We shall prove the following theorem:

Theorem 19.1.† (i) *If* $\vdash \exists y A(a_1,\ldots, a_k, y)$, *where* $V(A) \subseteq \{a_1,\ldots, a_k, y\}$, *then A represents a primitive recursive function, that is to say, there exists a primitive recursive function* $f(m_1,\ldots, m_k)$ *such that*

$$(3) \qquad R_\omega \models A[m_1,\ldots, m_k, f(m_1,\ldots, m_k)]$$

for all natural numbers $m_1,\ldots, m_k$.
(ii) *If in addition* $\vdash \exists ! y A(a_1,\ldots, a_k, y)$, *then such f is unique.*

To prove this theorem we need the following lemma.

Lemma 19.2.† *If* $\Gamma \vdash A$, *where* $V(\Gamma) \cup V(A) \subseteq \{a_1,\ldots, a_k\}$, *then there exists a primitive recursive function ρ of one variable such that* $n \leq \rho(n)$ *for every n and that for every n and* $m_1,\ldots, m_k \leq n$,

$$(4) \qquad \models_n \Gamma[m_1,\ldots, m_k] \Longrightarrow \models_{\rho(n)} A[m_1,\ldots, m_k],$$

where $\models_n \Gamma[m_1,\ldots, m_k]$ *means* $\models_n B[m_1,\ldots, m_k]$ *for all* $B \in \Gamma$. (*We call such a primitive recursive function ρ a majorant for* $\Gamma \vdash A$.)

We first prove the theorem by the aid of this lemma. If $\vdash \exists y A(a_1, \ldots, a_k, y)$, then by the lemma, there exists a primitive recursive (abbreviated p.r.) function ρ such that for every $n \in N$ and $m_1,\ldots, m_k \leq n$, we have $\models_{\rho(n)} \exists y A[m_1,\ldots, m_k]$, that is, there exists an $l \leq \rho(n)$ such that

$$(5) \qquad \models_{\rho(n)} A[m_1,\ldots, m_k, l].$$

But (5) is a primitive recursive predicate of $n, m_1,\ldots, m_k, l$ (see later Section 20, **D.20.1**). Hence, if we define

$$f(m_1,\ldots, m_k) = \mu y_{y \leq g} \models_g A[m_1,\ldots, m_k, y],$$

where $g = g(m_1,\ldots, m_k) = \rho(\max(m_1,\ldots, m_k))$, then f is primitive recursive and satisfies

$$R_\omega \models A[m_1,\ldots, m_k, f(m_1,\ldots, m_k)],$$

for all $m_1,\ldots, m_k \in \mathrm{N}$. **q.e.d.**

Proof of Lemma. We prove this lemma by the induction on $\Gamma \vdash A$.

Case (0). $A \in \Gamma$. In view of (4), we may take as ρ any primitive recursive function such that $\rho(n) \geq n$, e.g., $\rho(n) \equiv n$.

In the following cases,

$$\text{(i)} \ \frac{\Gamma \vdash r \in 0}{\Gamma \vdash A}, \quad \text{(ii)} \ \frac{\Gamma \vdash r \in s}{\Gamma \vdash r \in s \# t}, \quad \text{(iii)} \ \frac{\Gamma \vdash r = t}{\Gamma \vdash r \in s \# t},$$

$$\text{(v)} \ \frac{\psi, \Gamma \vdash \varphi \quad \psi, \Gamma \vdash \neg \varphi}{\Gamma \vdash \neg \psi}, \quad \text{(vi)} \ \frac{\Gamma \vdash \varphi \quad \Gamma \vdash \neg \varphi}{\Gamma \vdash A}$$

where each of the lower expressions is identical with $\Gamma \vdash A$, we may also take as ρ arbitrary as the above case, since in Cases (ii), (iii) and (v), A is an RF and in Cases (i) and (vi), the hypothesis (i.e., $\models_n \Gamma[a_1, \dots, a_k]$) cannot hold.

$$\text{Case (iv).} \ \frac{\Gamma \vdash r \in s \# t \quad \{r \in s\} \cup \Gamma \vdash A \quad \{r = t\} \cup \Gamma \vdash A}{\Gamma \vdash A}.$$

Suppose that for each of three upper expressions our lemma holds. Then there exist majorants π, τ, σ for $\Gamma \vdash r \in s \# t$, $\{r \in s\} \cup \Gamma \vdash A$, and $\{r = t\} \cup \Gamma \vdash A$, respectively. Then we define $\rho(n) \equiv \max(\tau(n), \sigma(n))$. Clearly, $\rho(n) \geq n$. Now suppose

$$\models_n \Gamma[m_1, \dots, m_k] (= \Gamma[m_1, \dots, m_k / a_1, \dots, a_k]).$$

Then

$$\models_n \Gamma[m_1, \dots, m_k, 0, \dots, 0 / a_1, \dots, a_k, b_1, \dots, b_h],$$

where $\{b_1, \dots, b_h\} = V(r \in s \# t) - \{a_1, \dots, a_k\}$. Since π is a majorant for $\Gamma \vdash r \in s \# t$, it follows that

$$\models_{\pi(n)} r \in s \# t[m_1, \dots, m_k, 0, \dots, 0 / a_1, \dots, a_k, b_1, \dots, b_h].$$

Since $r \in s \# t$ is an RF,

$$R_\omega \models r \in s \# t[m_1, \dots, m_k, 0, \dots, 0].$$

Thus, we have either $R_\omega \models r \in s[m_1, \dots, m_k, 0, \dots, 0]$ or else $R_\omega \models r = t[m_1, \dots, m_k, 0, \dots, 0]$. Hence $\models_n r \in s[m_1, \dots, m_k, 0, \dots, 0]$ or $\models_n r = t[m_1, \dots, m_k, 0, \dots,$

0]. If the former is the case, since τ is a majorant for $\{r \in s\} \cup \Gamma \vdash A$, we have

$$\models_{\tau(n)} A[m_1, \dots, m_k, 0, \dots, 0],$$

and hence

$$\models_{\rho(n)} A[m_1, \dots, m_k, 0, \dots, 0].$$

Similarly, we have the same result also when the latter is the case. From this it follows that ρ is a majorant for $\Gamma \vdash A$.

Cases (vii) $\dfrac{\Gamma \vdash B}{\Gamma \vdash B \vee C}$, (viii) $\dfrac{\Gamma \vdash C}{\Gamma \vdash B \vee C}$, (xi) $\dfrac{\Gamma \vdash B \wedge C}{\Gamma \vdash B}$,

(xii) $\dfrac{\Gamma \vdash B \wedge C}{\Gamma \vdash C}$, (xiii) $\dfrac{\varphi, \Gamma \vdash B}{\Gamma \vdash \varphi \rightharpoonup B}$,

where it is assumed that the lower expressions are $\Gamma \vdash A$. By the induction hypothesis there exists a majorant τ for the upper expression in each of these inference rules. Then we may take this τ as majorant for the lower expression, since obviously we have

(6) $\models_{\tau(n)} B[m_1, \dots, m_k] \Longrightarrow \models_{\tau(n)} B \vee C[m_1, \dots, m_k]$,

(7) $\models_{\tau(n)} C[m_1, \dots, m_k] \Longrightarrow \models_{\tau(n)} B \vee C[m_1, \dots, m_k]$,

(8) $\models_{\tau(n)} B \wedge C[m_1, \dots, m_k] \Longrightarrow \models_{\tau(n)} B[m_1, \dots, m_k]$ and

$\models_{\tau(n)} C[m_1, \dots, m_k]$,

(9) $(R_\omega \models \varphi[m_1, \dots, m_k] \Longrightarrow \models_{\tau(n)} B[m_1, \dots, m_k]) \Longrightarrow \models_{\tau(n)} \varphi \rightharpoonup$

$B[m_1, \dots, m_k]$.

Case (x). $\dfrac{\Gamma \vdash B \quad \Gamma \vdash C}{\Gamma \vdash B \wedge C}$,

where A is $B \wedge C$. Let τ and σ be majorants for $\Gamma \vdash B$ and $\Gamma \vdash C$, respectively. Then $\rho(n) \equiv \max(\tau(n), \sigma(n))$ is a majorant for $\Gamma \vdash B \wedge C$, since $\models_{\tau(n)} B[m_1, \dots, m_k]$ and $\models_{\sigma(n)} C[m_1, \dots, m_k]$ imply $\models_{\rho(n)} B \wedge C[m_1, \dots, m_k]$.

Case (ix). $\dfrac{\Gamma \vdash B \vee C \quad \{B\} \cup \Gamma \vdash A \quad \{C\} \cup \Gamma \vdash A}{\Gamma \vdash A}.$

Let π, τ, σ be majorants, for which the lemma holds for $\Gamma \vdash B \vee C$, $\{B\} \cup \Gamma \vdash A$ and $\{C\} \cup \Gamma \vdash A$, respectively. Then we define $\rho(n) \equiv \max(\tau(\pi(n)), \sigma(\pi(n)))$. Suppose $\models_n \Gamma$. Then $\models_{\pi(n)} B \vee C$. Hence $\models_{\pi(n)} B$ or $\models_{\pi(n)} C$. Since $n \leq \pi(n)$, $\models_{\pi(n)} \{B\} \cup \Gamma$ or $\models_{\pi(n)} \{C\} \cup \Gamma$. Hence $\models_{\tau(\pi(n))} A$ or $\models_{\sigma(\pi(n))} A$. So $\models_{\rho(n)} A$.

Case (xiv). $\dfrac{\Gamma \vdash \varphi \rightharpoonup A \quad \Gamma \vdash \varphi}{\Gamma \vdash A}.$

Let τ and σ be majorants for $\Gamma \vdash \varphi \rightharpoonup A$ and $\Gamma \vdash \varphi$, respectively. This it is obvious that $\rho \equiv \tau$ is a majorant for $\Gamma \vdash A$.

Case (xv). $\dfrac{\Gamma \vdash s \in r \quad \Gamma \vdash D(s/x)}{\Gamma \vdash \exists x \in r D}.$

Let τ and σ be majorants for $\Gamma \vdash s \in r$ and $\Gamma \vdash \exists x \in r D$, respectively. Then $\rho \equiv \sigma$ is a majorant for $\Gamma \vdash \exists x \in r D$, since $\models_{\sigma(n)} s \in r$ and $\models_{\sigma(n)} D(s/x) \Rightarrow \models_{\sigma(n)} \exists x \in r D$.

Case (xvi). $\dfrac{\Gamma \vdash \exists x \in r D \quad \{a \in r, D(a/x)\} \cup \Gamma \vdash A}{\Gamma \vdash A}.$

Let τ and σ be majorants for $\Gamma \vdash \exists x \in r D$ and for $\{a \in r, D(a/x)\} \cup \Gamma \vdash A$. Let θ_r is a p.r. function defined for each semi-term r by

$$\theta_0(n) = 0,$$

$$\theta_v(n) = n, \text{ where } v \text{ is a variable,}$$

$$\theta_{\sharp st}(n) = \theta_s(n) + 2^{\theta_t(n)}.$$

Then $\rho(n) \equiv \sigma(\max(\tau(n), \theta_r(n)))$ serves as majorant for $\Gamma \vdash A$. For suppose $m_1, \dots, m_k \leq n$ and $\models_n \Gamma[m_1, \dots, m_k]$. Then $\models_{\tau(n)} \exists x \in r D[m_1, \dots, m_k]$. Hence there exists an $m \in r[m_1, \dots, m_k]$ such that $\models_{\tau(n)} D[m_1, \dots, m_k, m/a_1, \dots, a_k, x]$. Since $V(r) \subseteq \{a_1, \dots, a_k\}$ and $m_1, \dots, m_k \leq n$, it is seen from our coding of h.f. sets that $r[m_1, .., m_k] \leq \theta_r(n)$ by the induction on r. Hence

$$m \leq r[m_1, .., m_k] \leq \theta_r(n) \leq \max(\tau(n), \theta_r(n)).$$

Also, $m_1,\dots, m_k \leq n \leq \max(\tau(n), \theta_r(n))$,

$$\models_{\max(\tau(n),\theta_r(n))} D[m_1,\dots, m_k, m/a_1,\dots, a_k, x],$$

$$\models_{\max(\tau(n),\theta_r(n))} a \in r[m_1,\dots, m_k, m/a_1,\dots, a_k, a],$$

and

$$\models_{\max(\tau(n),\theta_r(n))} \Gamma.$$

Since ρ is a majorant for $\{a \in r, D(a/x)\} \cup \Gamma \vdash A$, it follows that

$$\models_{\sigma(\max(\tau(n),\theta_r(n)))} A.$$

This shows that ρ is a majorant for $\Gamma \vdash A$.

Case (xvii). $\dfrac{\{a \in r\} \cup \Gamma \vdash D(a/\mathrm{x})}{\Gamma \vdash \forall x \in r D}$.

Let τ be a majorant for the upper expression. Let $\rho(n) \equiv \tau(\theta_r(n))$. We have to show that ρ is a majorant for the lower expression. Clearly, $\rho(n) \geq n$. Now suppose that $m_1,\dots, m_k \leq n$ and $\models_n \Gamma[m_1,\dots, m_k]$. It suffices to prove

$$\models_{\rho(n)} D[m_1,\dots, m_k, m/a_1,\dots, a_k, x],$$

for all $m \in r[m_1,\dots, m_k]$. Since $m_1,\dots, m_k \leq n$, it follows that $m \leq \theta_r(n)$. Therefore,

$$\models_{\theta_r(n)} (\{a \in r\} \cup \Gamma)\,[m_1,\dots, m_k, m/a_1,\dots, a_k, a].$$

(Note that $n \leq \theta_r(n)$.) So we have

$$\models_{\tau(\theta_r(n))} D(a/x)\,[m_1,\dots, m_k, m/a_1,\dots, a_k, a],$$

that is, $\models_{\rho(n)} D[m_1,\dots, m_k, m/a_1,\dots, a_k, x]$.

Case (xviii). $\dfrac{\Gamma \vdash \forall x \in r D \quad \Gamma \vdash s \in r}{\Gamma \vdash D(s/x)}$.

Let τ and σ be majorants for $\Gamma \vdash \forall x \in r D$ and $\Gamma \vdash s \in r$, respectively. Then $\rho \equiv \tau$ is a majorant for $\Gamma \vdash D(s/x)$. For suppose $\models_n \Gamma[m_1,\dots, m_k]$, where $m_1,\dots, m_k \leq n$. Then $\models_{\tau(n)} \forall x \in r D[m_1,\dots, m_k]$ and $s[m_1,\dots, m_k] \in$

$r[m_1,\dots, m_k]$. Hence

$$\models_{\tau(n)} D[m_1,\dots, m_k, s[m_1,\dots, m_k]],$$

that is,

$$\models_{\tau(n)} D(s/x)\,[m_1,\dots, m_k].$$

Case (xix). $\dfrac{\Gamma \vdash D(s/x)}{\Gamma \vdash \exists x D}$.

Let τ be a majorant for $\Gamma \vdash D(s/x)$. Then $\rho(n)=\max(\tau(n), \theta_s(n))$ is a majorant for $\Gamma \vdash \exists x D$. For suppose $\models_n \Gamma[m_1,\dots, m_k]$. Then $\models_{\tau(n)} D(s/x)$ $[m_1,\dots, m_k]$, i.e.,

$$\models_{\tau(n)} D[m_1,\dots, m_k, s[m_1,\dots, m_k]/a_1,\dots, a_k, x],$$

and a fortiori

$$\models_{\rho(n)} D[m_1,\dots, m_k, s[m_1,\dots, m_k]].$$

But $s[m_1,\dots, m_k] \leq \theta_s(n) \leq \rho(n)$. So $\models_{\rho(n)} \exists x D[m_1,\dots, m_k]$.

Case (xx). $\dfrac{\Gamma \vdash \exists x D \quad \{D(a/x)\} \cup \Gamma \vdash A}{\Gamma \vdash A}$.

Let τ and σ be majorants for $\Gamma \vdash \exists x D$ and $\{D(a/x)\} \cup \Gamma \vdash A$. In this case, let $\rho(n) \equiv \sigma(\tau(n))$. To prove ρ is a majorant for $\Gamma \vdash A$, suppose $\models_n \Gamma[m_1,\dots, m_k/a_1,\dots, a_k]$, where $m_1,\dots, m_k \leq n$. Since $a \notin V(\Gamma) \cup V(A) \cup V(\exists x D)$, we may assume $a \notin \{a_1,\dots, a_k\} \supseteq V(\Gamma) \cup V(A) \cup V(\exists x D)$. Then $\models_{\tau(n)} \exists x D[m_1,\dots, m_k]$. So there exists an $m \leq \tau(n)$ such that $\models_{\tau(n)} D[m_1,\dots, m_k, m/a_1,\dots, a_k, x]$, or equivalently $\models_{\tau(n)} D(a/x)\,[m_1,\dots, m_k, m/a_1,\dots, a_k, a]$. Also $\models_{\tau(n)} \Gamma[m_1,\dots, m_k, m/a_1,\dots, a_k, a]$. It follows that $\models_{\sigma(\tau(n))} A[m_1,\dots, m_k, m/a_1,\dots, a_k, a]$ and hence that $\models_{\sigma(\tau(n))} A[m_1,\dots, m_k/a_1,\dots, a_k]$. This proves that ρ is a majorant for $\Gamma \vdash A$.

Case (xxi). $\dfrac{\Gamma \vdash D(0/x) \quad \{D(a/x), D(b/x)\} \cup \Gamma \vdash D(a \# b/x)}{\Gamma \vdash D(r/x)}$.

Let τ and σ be majorants for $\Gamma \vdash D(0/x)$ and $\{D(a/x), D(b/x)\} \cup \Gamma \vdash D(a \# b/x)$. We define $\sigma(i, j)$ by $\sigma(i, 0)=\tau(i)$ and $\sigma(i, j+1)=\sigma(\sigma(i, j))+1$. Note that $j \leq \sigma(i, j)$. Let $\rho(n)=\sigma(n, \theta_r(n))$. We shall prove that ρ is a majorant for $\Gamma \vdash D(r/x)$. Suppose $\models_n \Gamma[m_1,\dots,m_k]$, where $m_1,\dots,m_k \leq n$. Then $r[m_1,\dots,m_k] \leq \theta_r(n)$. We shall show by the induction that $\models_{\sigma(n,i)} D[m_1,\dots,m_k, i]$ for all i. If $i=0$ it is is obvious from the hypothesis since $\sigma(n,0)=\tau(n)$. If $i \neq 0$, then there exist j and l less than i such that $i=j\# l$. By the induction hypothesis we have $\models_{\sigma(n,j)} D[m_1,\dots,m_k, j]$ and $\models_{\sigma(n,l)} D[m_1,\dots,m_k, l]$. Since $j \leq i-1$, $k \leq i-1$, we have both $\models_{\sigma(n,i-1)} D[m_1,\dots,m_k, j]$ and $\models_{\sigma(n,i-1)} D[m_1,\dots,m_k, l]$. Moreover $m_1,\dots,m_k, j, l \leq \sigma(n, i-1)$. Since $\sigma(n)$ is a majorant for $\{D(a/x), D(b/x)\} \cup \Gamma \vdash D(a\# b/x)$, we have

$$\models_{\sigma(\sigma(n,i-1))} D[m_1,\dots,m_k, j\# l].$$

Since $\sigma(\sigma(n, i-1)) \leq \sigma(n, i)$ and $j\# l=i$, we have $\models_{\sigma(n,i)} D(m_1,\dots,m_k, i)$. Thus we have, letting $i=r[m_1,\dots,m_k]$,

$$\models_{\rho(n)} D(m_1,\dots,m_k, r[m_1,\dots,m_k])$$

since $\sigma(n, r[m_1,\dots,m_k]) \leq \sigma(n, \theta_r(n)) = \rho(n)$. Hence ρ is majorant for $\Gamma \vdash D(r/x)$. This completes the proof of the theorem. **q.e.d.**

Corollary 19.3. *Let $\exists x A$ is a $\sum$F which does not have free variables. If $\vdash \exists x A$, then $\vdash A(s)$, for some constant s.*

Proof. This is a special case of Theorem 19.1 where $k=0$. **q.e.d.**

Incidentally, we have an alternative proof of the plausibility Theorem 17.1 as follows.

Suppose $R_\omega \models \Gamma[m_1,\dots,m_k]$. Then $\models_n \Gamma[m_1,\dots,m_k]$, for sufficiently large n, hence taking $n \geq m_1,\cdots,m_k$, by Theorem 19.1, it follows that $\models_{\rho(n)} A[m_1,\dots,m_k]$ for some p.r. function ρ. Hence $R_\omega \models A[m_1,\dots,m_k]$. **q.e.d.**

The converse of Theorem 19.1 holds.

Theorem 19.4. *If $f(m_1,\dots,m_k)$ is a primitive recursive function, then there can be found a $\sum$F $A(a_1,\dots,a_k,y)$ such that*

$$\vdash \exists ! y A(a_1,\dots,a_k, y)$$

and

$$R_\omega \models A[m_1,\dots, m_k, f(m_1,\dots, m_k)],$$

for every $m_1,\dots, m_k \in R_\omega$.

And hence

Theorem 19.5. *$f(m_1,\dots, m_k)$ is primitive recursive iff there is a $\sum$F $A(a_1,\dots, a_k, y)$ such that*

$$\vdash \exists ! y A(a_1,\dots, a_k, y)$$

and

$$R_\omega \models A[m_1,\dots, m_k, f(m_1,\dots, m_k)].$$

This is a characterization theorem for primitive recursive functions.

Proof of Theorem 19.4. We make use of Theorem 13.6. But there, natural numbers are regarded as von Neumann ordinals while here they are regarded as h.f. sets. So it is necessary to translate Theorem 13.6 using the function T introduced in **D.15.4.** We proceed as follows. Let a primitive recursive function $f(m_1,\dots, m_k)$ be given. Then, by Theorem 13.6, we can find a number-theoretic formal function $F(\lambda_1,\dots, \lambda_k)$ in a conservative expansion of FCS. Let $A(b, a_1,\dots, a_k)$ be a $\sum$F in FCS equivalent to

$$J(F(T(a_1),\dots, T(a_k)), b).$$

Then by **T.15.11**, we see,

$$\vdash \mathrm{Nat}(T(a_1)) \wedge \cdots \wedge \mathrm{Nat}(T(a_k))$$

and hence

$$\vdash \mathrm{Nat}(F(T(a_1),\dots, T(a_k))).$$

So by **T.15.10**,

$$\vdash \exists ! b A(b, a_1,\dots, a_k).$$

Moreover on account of the meaning of T and J we easily obtain that

$$R_\omega \models A[f(m_1,\dots, m_k), m_1,\dots, m_k],$$

for every $m_1, .., m_k \in R_\omega$. **q.e.d.**

Corollary 19.6. (i) *If* $(A(a_1,\dots, a_n), B(a_1,\dots, a_n))$ *is a* ΔF, *then the* n*-ary relation* $R_\omega \models A[m_1,\dots, m_n]$ *is primitive recursive.* (ii) *Conversely, every primitive recursive* n*-ary relation can be represented in this way.*

Proof. (i) If $(A(a_1,\dots, a_n), B(a_1,\dots, a_n))$ is a ΔF, then we have

$$\vdash \exists x((x=0 \wedge A(a_1,\dots, a_n)) \vee (x=1 \wedge B(a_1,\dots, a_n)).$$

Hence by our main Theorem 19.1, there is a primitive recursive function $f(m_1,\dots, m_n)$ such that

$$R_\omega \models (f(m_1,\dots, m_n)$$
$$=0 \wedge A(m_1,\dots, m_n)) \vee (f(m_1,\dots, m_n)=1 \wedge B(m_1,\dots, m_n)).$$

But since (A, B) is a ΔF, for every $m_1,\dots, m_n \in R_\omega$, exactly one of $R_\omega \models A(m_1,\dots, m_n)$ and $R_\omega \models B(m_1,\dots, m_n)$ holds. So

$$f(m_1,\dots, m_n)=0 \Longleftrightarrow R_\omega \models A[m_1,\dots, m_n].$$

Therefore $R_\omega \models A[m_1,\dots, m_n]$ is primitive recursive.
(ii) If $P(m_1,\dots, m_n)$ is a primitive recursive n-ary relation, then there exists a primitive recursive function f such that

$$P(m_1,\dots, m_n) \Longleftrightarrow f(m_1,\dots, m_n)=0.$$

By Theorem 19.5, there exists a $\sum$F, $A(b, a_1,\dots, a_n)$ such that

$$\vdash \exists ! y A(y, a_1,\dots, a_n)$$

and

$$R_\omega \models A[f(m_1,\dots, m_n), m_1,\dots, m_n].$$

But then we have a representation

$$P(m_1, .., m_n) \Longleftrightarrow R_\omega \models A(0, m_1,\dots, m_n).$$ **q.e.d.**

The following is an application of Theorem 19.1.

Let $f(m)$ and $h(m)$ be defined as follows:

$$f(m)=\begin{cases} x, & \text{if } m \text{ is not a square and } x \text{ is the least} \\ & \text{non-trivial solution of diophantine equation} \\ & x^2-my^2=1 \text{ (with } y>0\text{)}, \\ 0, & \text{if } m \text{ is a square.} \end{cases}$$

$$h(m)=\text{the ideal class number of } Q(\sqrt{-m}).$$

Then these functions are both primitive recursive, for the theory of quadratic diophantine equations and the elementary theory of ideals are formalizable in FCS so that we can prove the existence of the values of f and h in FCS. (Then by Theorem 19.1, they are primitive recursive.)

20. Equivalence to Primitive Recursive Arithmetic

For primitive recursive arithmetic (abbreviated by PRA), see Goodstein [4]. We shall use the results in the book.

First, let $[a/b]$ and $\text{rem}(a, b)$ be the quotient and the remainder function, for which

$$(1) \qquad a=b\cdot[a/b]+\text{rem}(a, b),$$

$$(2) \qquad b>0 \longrightarrow \text{rem}(a, b)<b,$$

and

$$(3) \qquad a=b\cdot s+r \wedge r<b \longrightarrow [a/b]=s \wedge \text{rem}(a, b)=r,$$

hold in primitive recursive arithmetic. (For definition of these functions, see Kleene [1] or Goodstein [4]. In the latter these are denoted by Q and R.)

Now we define

$$(4) \qquad E(a, b)=1\dot{-}\text{rem}([b/2^a], 2).$$

Since $E(a, b)$ takes only 0 and 1 as values, let us regard it as a proposition (0 as truth and 1 as falsity). Then it says that $[b/2^a]$ is odd.

We have in PRA that

$$2^0 = 1, \tag{5}$$

$$[b/1] = b, \tag{6}$$

$$[2c/2^{a+1}] = [c/2^a], \tag{7}$$

$$[(2c+1)/2^{a+1}] = [c/2^a]. \tag{8}$$

From these it follows that

$$E(0, b) \longleftrightarrow \mathrm{rem}(b, 2) = 1, \tag{9}$$

$$E(a+1, 2c) \longleftrightarrow E(a, c), \tag{10}$$

$$E(a+1, 2c+1) \longleftrightarrow E(a, c). \tag{11}$$

But the following facts are also provable in PRA:

$$b \le a \longrightarrow b < 2^a,$$

$$b < 2^a \longrightarrow [b/2^a] = 0,$$

$$1 - \mathrm{rem}(0, 2) = 1,$$

$$b \le a \vee a < b.$$

So, we have

$$E(a, b) \longrightarrow a < b, \tag{12}$$

$$\bar{E}(a, 0), \quad (\bar{\ } \text{ is the negation symbol in PRA}). \tag{13}$$

Next, we define $\natural$ by

$$a \natural c = \begin{cases} a, & \text{if } E(c, a), \\ a + 2^c, & \text{if } \bar{E}(c, a). \end{cases} \tag{14}$$

Then $\natural$ has the similar properties as $\#$:

$$E(c, a \natural c), \tag{15}$$

$$E(d,\ a) \longrightarrow E(d,\ a \natural c), \tag{16}$$

$$E(d,\ a \natural c) \longrightarrow E(d,\ a) \vee d = c, \tag{17}$$

$$E(d,\ a \natural c) \longleftrightarrow E(d,\ a) \vee d = c. \tag{18}$$

Proof of (15)–(18). (15) is obtained by using

$$[a + 2^b/2^b] = [a/2^b] + 1.$$

(16), (17) and (18) are obtained thus:

$$E(c,\ a) \vee \bar{E}(c,\ a),$$

$$E(c,\ a) \longrightarrow a \natural c = a,$$

$$E(c,\ a) \longrightarrow (E(d,\ a) \longleftrightarrow E(d,\ a \natural c)),$$

$$\bar{E}(c,\ a) \longrightarrow (E(d,\ a) \longrightarrow c \neq d),$$

$$\bar{E}(c,\ a) \longrightarrow [a/2^c] = 2 \cdot [a/2^{c+1}],$$

$$c \neq d \longrightarrow c < d \vee d < c,$$

$$c < d \longrightarrow d = c + 1 + ((d \dot{-} c) \dot{-} 1),$$

$$\bar{E}(c,\ a) \longrightarrow a = [a/2^{c+1}] \cdot 2^{c+1} + \operatorname{rem}(a,\ 2^c)$$

$$\wedge\, a + 2^c = [a/2^{c+1}] \cdot 2^{c+1} + 2^c + \operatorname{rem}(a,\ 2^c),$$

$$\operatorname{rem}(a,\ 2^c) < 2^{c+1} \wedge 2^c + \operatorname{rem}(a,\ 2^c) < 2^{c+1},$$

$$[a/2^{c+1}] = [[a/2^{c+1}]/2^x] \cdot 2^x + \operatorname{rem}([a/2^{c+1}],\ 2^x),$$

$$\operatorname{rem}([a/2^{c+1}],\ 2^x) \cdot 2^{c+1} + 2^c + \operatorname{rem}(a,\ 2^c) < 2^{c+1+x},$$

$$\bar{E}(c,\ a) \longrightarrow [a/2^{c+1+x}] = [[a/2^{c+1}]/2^x]$$

$$\wedge\, [(a + 2^c)/2^{c+1+x}] = [[a/2^{c+1}]/2^x],$$

$$\bar{E}(c,\ a) \longrightarrow [(a + 2^c)/2^{c+1+x}] = [a/2^{c+1+x}],$$

$$\bar{E}(c,\ a) \longrightarrow (E(c + 1 + x,\ a) \longrightarrow E(c + 1 + x,\ a \natural c)),$$

$$\bar{E}(c,\ a)\wedge c<d\longrightarrow(E(d,\ a)\longleftrightarrow E(d,\ a\natural c)),$$

$$d<c\longrightarrow c=d+1+((c\dot{-}d)\dot{-}1),$$

$$[a+2^{d+1+x}/2^{d}]=[a/2^{d}]+2\cdot 2^{x},$$

$$\bar{E}(c,\ a)\wedge d<c\longrightarrow(E(d,\ a)\longleftrightarrow E(d,\ a\natural c)),$$

$$\bar{E}(c,\ a)\wedge c\neq d\longrightarrow(E(d,\ a)\longleftrightarrow E(d,\ a\natural c)),$$

$$c\neq d\longrightarrow(E(d,\ a)\longleftrightarrow E(d,\ a\natural c)),$$

$$E(d,\ a)\longrightarrow E(d,\ a\natural c),$$

$$E(d,\ a\natural c)\longrightarrow E(d,\ a)\vee d=c,$$

$$E(d,\ a\natural c)\longleftrightarrow E(d,\ a)\vee d=c.$$

We establish a theorem on binary expansion in PRA;

Theorem 20.1. $a=\sum_{E(i,a)}2^{i}\ (=\sum_{i\leq a}(\overline{\text{sg}}(E(i,\ a)))\cdot 2^{i})$.

(c.f., 2.9 (page 35) of Goodstein's book.)

Proof. The following induction schema is acceptable in PRA (cf., 6.3 of Goodstein's book).

$$\frac{P(0)\quad P(a)\longrightarrow P(2a)\quad P(a)\longrightarrow P(2a+1)}{P(a)}.$$

So it suffices to show

$$0=\sum_{E(i,0)}2^{i},$$

$$a=\sum_{E(i,a)}2^{i}\longrightarrow 2a=\sum_{E(i,2a)}2^{i},$$

and

$$a=\sum_{E(i,a)}2^{i}\longrightarrow 2a+1=\sum_{E(i,2a+1)}2^{i}.$$

But these are established by easy computations. **q.e.d.**

Corollary 20.2. *In* PRA, *we have*

$$A_x^a(E(x, a) \longrightarrow E(x, b)) \wedge A_x^b(E(x, b) \longrightarrow E(x, a)) \longrightarrow a = b,$$

where A_x^a *is the bounded universal quantifier introduced in Goodstein's book, p.* 64. (*It means "for all x less than or equal to a.*")

For any primitive recursive (p.r.) predicate $P(x, a_1, \dots, a_n)$ in PRA, let $(\forall x \in a)P(x, a_1, \dots, a_n)$ be the predicate

$$A_x^a(E(x, a) \longrightarrow P(x, a_1, \dots, a_n)).$$

Similarly, let $(\exists x \in a)P(x, a_1, \dots, a_n)$ be the predicate

$$E_x^a(E(x, a) \wedge P(x, a_1, \dots, a_n)).$$

If we replace, in an RF φ, each expression $a \in b$, $a \# b$, propositional connectives and restricted quantifiers by $E(a, b)$, $a \natural b$, corresponding propositional connectives and bounded quantifiers in PRA, we obtain a p.r. predicate in PRA. We call this proposition $\tilde{\varphi}$.

Of course, it is impossible to correspond to each $\sum$F a proposition in PRA with the same meaning. However, we can correspond to each $\sum$F a certain proposition in PRA with a new variable, say n, as follows. (The intuitive intention is to bound each unrestricted existential quantifier to n.)

Definition 20.1. *Let A be a* $\sum$F. *Let n be a variable not occurring in A. Then we define* $A^{[n]}$ *to be the proposition obtained by replacing each unrestricted existential quantifier* $\exists x$ *by* E_x^n, *and at the same time by replacing* $a \in b$, $a \# b$, *propositional connectives, restricted quantifiers by* $E(a, b)$, $a \natural b$, *corresponding propositional connectives and bounded quantifiers in* PRA.

Note that for an RF φ, $\varphi^{[n]}$ coincides with $\tilde{\varphi}$ above.

By the induction on A we easily have

Lemma 20.3. $n \leq m \wedge A^{[n]} \longrightarrow A^{[m]}$, *in* PRA.

Now FCS is conservatively translated into PRA in the sense of the following theorem:

Theorem 20.4. (i) *If $\Gamma \vdash A$ in* FCS, *then there exists a primitive recursive* (*derivation of a*) *function $\rho(n)$ such that*

$$\rho(n) \geq n$$

and

$$a_1 \leq n \wedge \cdots \wedge a_k \leq n \wedge \Gamma^{[n]} \longrightarrow A^{[\rho(n)]}$$

are provable in PRA, *where $a_1, \ldots, a_k$ are all the free variables occurring in Γ and A, and $\Gamma^{[n]}$ is the conjunction of all $B^{[n]}$ with B in Γ.*
(ii) *If* $\vdash A(a_1, .., a_n)$ (*in* FCS), *then there exists a primitive recursive* (*derivation of a*) *function $f(a_1, \ldots, a_n)$ such that*

$$A^{[f(a_1, \ldots, a_n)]}(a_1, \ldots, a_n)$$

is provable in PRA.
(iii) *If φ is an* RF *in a conservative expansion of* FCS *by definition, then it is provable in* FCS *iff $\bar{\varphi}$ is provable in* PRA.
(iv) FCS *is consistent iff* PRA *is consistent.*

Outline of Proof. (ii), (iii) and (iv) are easy consequences of (i). The proof of (i) proceeds as in the proof of Lemma 19.2 of the last section. But we must also use the following:
(i) formal theorems of propositional calculus and predicate calculus with quantifier bounded, such as,

$$\frac{p \longrightarrow q \quad p}{q}, \quad \frac{p(a) \longrightarrow q}{E_x^n p(x) \longrightarrow q},$$

which are proved in Goodstein's book, and
(ii) course-of-values induction of the form

$$\frac{p \wedge A_x^n(x < n \longrightarrow q(x)) \longrightarrow q(n)}{p \longrightarrow q(n)},$$

which can easily be proved in PRA by the standard technique. **q.e.d.**

21. Conservative Expansion of PRA Including All First-Order Formulas

We consider the following system, named PRK.

1. Primitive recursive terms (PR-terms) are defined as in PRA. (See e.g. Curry [1].)

2. PR-formula is a formula of the form $r=s$, where r and s are PR-terms.

3. (First-order) formula is constructed from PR-formulas by means of logical connectives and quantifiers.

4. Sequent is an expression of form $\Gamma \to \Delta$, where Γ and Δ are finite sequences of formulas.

5. PR-sequent is a sequent composed of PR-formulas.

6. Basic sequent is a PR-sequent which is provable in PRA (when the sequent, say,

$$P_1, \ldots, P_m \longrightarrow Q_1, \ldots, Q_n$$

is construed as the PR-formula

$$P_1 \wedge \cdots \wedge P_m \longrightarrow Q_1 \vee \cdots \vee Q_n,$$

where $\wedge$, $\to$, $\vee$ are logical connectives defined in PRA, as in Goodstein's book [4]).

7. The inference rules are as in LK.

For example, inferences on quantifiers are

$$\frac{\Gamma \longrightarrow \Delta, A(t)}{\Gamma \longrightarrow \Delta, \exists x A(x)} \qquad \frac{A(a), \Gamma \longrightarrow \Delta}{\exists x A(x), \Gamma \longrightarrow \Delta}$$

$$\frac{\Gamma \longrightarrow \Delta, A(a)}{\Gamma \longrightarrow \Delta, \forall x A(x)} \qquad \frac{A(t), \Gamma \longrightarrow \Delta}{\forall x A(x), \Gamma \longrightarrow \Delta}.$$

A sequent is provable if it is obtainable from some basic sequents by successive applications of the above inference rules. A formula A is provable if the sequent $\to A$ is provable. This completes the description of PRK.

Theorem 21.1. *$A \to A$ is provable.*

Proof. If A is quantifier-free, then it is obviously a basic sequent. So this theorem is proved by the induction on the number of logical symbols in A. **q.e.d.**

Theorem 21.2. *If a sequent or a formula comes from a provable sequent or provable formula in* LK *by substitution, then it is provable in* PRK. *In particular, each instance of tantology is provable in* PRK.

Proof. This is immediate on account of Theorem 21.1 and the inference rules of PRK. **q.e.d.**

Example. $A \vee \neg A$ is provable in PRK.
Now, by exactly the same way as Gentzen's, we can prove the following cut-elimination theorem for PRK:

Theorem 21.3. *Every provable sequent is provable without using cut-inference.*

As a corollary of this theorem we have

Corollary 21.4. PRK *is a conservative expansion of* PRA. *i.e., If* $\Gamma \rightarrow \Delta$ *is a* PR-*sequent and if it is provable in* PRK, *then it is provable in* PRA.

Proof. A cut-free proof of a PR-sequent in PRK does not contain any inference on a logical connective.

So all the sequents occurring in it are basic sequents and hence provable in PRA. **q.e.d.**

We state more results about PRK without proofs.

Theorem 21.5. (i) $\forall x \forall y A(x, y) \rightleftarrows \forall z A((z)_1, (z)_2)$ (*and its dual*) *is provable in* PRK, *where* $(z)_u$ *is a primitive recursive function defined in Kleene* [1].

(ii) *an existential formula i.e., a formula of the form* $\exists y P(y, a_1, \ldots, a_n)$ *with* P *quantifier-free, is provable in* PRK *iff there is a* PR-*term* $f(a_1, \ldots, a_n)$ *such that* $P(f(a_1, \ldots, a_n), a_1, \ldots, a_n)$ *is provable in* PRA.

(iii) *an* $\forall\exists$-*formula i.e., a formula of the form* $\forall x \exists y P(x, y, a_1, \ldots, a_n)$

with P quantifier-free, is provable in PRK *iff there is a* PR-*term* $f(x, a_1,\dots, a_n)$ *such that* $P(x, f(x, a_1,\dots, a_n), a_1,\dots, a_n)$ *is provable in* PRA.

(iv) *If a formula* $\exists yP(y)$, *P quantifier free, does not have any free variable, and if it is provable in* PRK, *then* $P(n)$ *is provable in* PRK *for some numeral term n.*

(v) *If* $P(a)$ *is a* PR-*formula, then the principle of mathematical induction holds: that is,*

1°. $P(0)\wedge\forall x(P(x)\rightarrow P(x+1))\rightarrow\forall xP(x)$

is provable in PRK, *and*

2°. *If* $\Gamma\longrightarrow\Delta, P(0)$ *and* $P(a), \Gamma\longrightarrow\Delta, P(a+1)$

are provable in PRK, *then* $\Gamma\rightarrow\Delta, \forall xP(x)$ *is provable in* PRK.

(vi) *If* $\exists xP(x)\rightleftarrows\forall xQ(x)$ *is provable in* PRK *and if P and Q are quantifier free then* $R\rightleftarrows\exists xP(x)$ (*and hence* $R\rightleftarrows\forall xQ(x)$, *too*) *is provable in* PRK, *for some* PR-*formula R.*

(*In this case we say* $\exists xP(x)$ *is a decidable formula. Thus* (v) *holds for decidable formulas.*)

(vii) *If* $A(a)$ *is an existential formula and if* $\Gamma\rightarrow A(0)$ *and* $A(a)$, $\Gamma_1\rightarrow A(a+1)$, *where* Γ_1 *consists of existential formulas, are provable in* PRK, *then* $\Gamma, \Gamma_1\rightarrow\forall xA(x)$ *is provable in* PRK.

Similarly we may consider a formal system PRJ which is like LJ as PRK is like LK.

One difference between philosophies of PRA (or PRK) and of FCS is that in the former system the existence of the values of primitive recursive functions are assumed from the beginning while in the latter the existence of them are proved, only assuming the existence of a single, very elementary function, i.e., #.

By the way, from the results of this section it makes sense to say that any 1st order formula is provable in (a conservative expansion of) FCS.

22. Extensions of Number Systems

How to define in FCS negative integers and rational numbers etc., with their arithmetic operations are almost obvious. We follow the usual definitions, keeping in mind not to use infinistic methods. For this we must exhibit a unique (finite) presentation of each object (such as integers, rational numbers, algebraic numbers, etc.). Some complexity in defining them caused by this requirement would be inevitable. However, we try to minimize complications in proving theorems.

(I) Integers

D.22.1. (i) $\mathrm{Neg}(a) \Leftrightarrow \exists x \in \cup \cup a.\ (a = \langle 0, x \rangle \wedge \mathrm{Nat}(x) \wedge x \neq 0)$, ($\mathrm{Neg}(a)$ *stands for "a is a negative integer".*)

(ii) $\mathrm{Z}(a) \Leftrightarrow \mathrm{Nat}(a) \vee \mathrm{Neg}(a)$, ($\mathrm{Z}(a)$ *Stands for "a is a (rational) integer".*)

(iii)
$$-a = \begin{cases} \langle 0, a \rangle, & \mathit{if} \quad \mathrm{Nat}(a) \wedge a > 0, \\ 0, & \mathit{if} \quad a = 0, \\ x, & \mathit{if} \quad \mathrm{Neg}(a) \wedge a = \langle 0, x \rangle. \end{cases}$$

(iv)
$$|a| = \begin{cases} a, & \mathit{if} \quad \mathrm{Nat}(a), \\ -a, & \mathit{if} \quad \mathrm{Neg}(a). \end{cases}$$

(v)
$$\lambda \cdot \ \mu = \begin{cases} \lambda \dot{-} \mu, & \mathit{if} \quad \mathrm{Nat}(\lambda) \wedge \mathrm{Nat}(\mu) \wedge \lambda \geq \mu, \\ -(\lambda \dot{-} \mu), & \mathit{if} \quad \mathrm{Nat}(\lambda) \wedge \mathrm{Nat}(\mu) \wedge \lambda < \mu. \end{cases}$$

(vi)
$$a + b = \begin{cases} a + b, & \mathit{if} \quad \mathrm{Nat}(a) \wedge \mathrm{Nat}(b), \\ a - |b|, & \mathit{if} \quad \mathrm{Nat}(a) \wedge \mathrm{Neg}(b), \\ b - |a|, & \mathit{if} \quad \mathrm{Neg}(a) \wedge \mathrm{Nat}(b), \\ -(|a| + |b|), & \mathit{if} \quad \mathrm{Neg}(a) \wedge \mathrm{Neg}(b). \end{cases}$$

(vii)
$$a \cdot b = \begin{cases} a \cdot b, & \mathit{if} \quad \mathrm{Nat}(a) \wedge \mathrm{Nat}(b), \\ -(a \cdot |b|), & \mathit{if} \quad \mathrm{Nat}(a) \wedge \mathrm{Neg}(a), \\ -(|a| \cdot b), & \mathit{if} \quad \mathrm{Neg}(a) \wedge \mathrm{Nat}(b), \\ |a| \cdot |b|, & \mathit{if} \quad \mathrm{Neg}(a) \wedge \mathrm{Neg}(b). \end{cases}$$

(viii)
$$a^{\lambda} = \begin{cases} |a|^{\lambda}, & \mathit{if} \quad \exists \nu \leq \lambda (\lambda = 2\nu) \wedge \mathrm{Z}(a), \\ -|a|^{\lambda}, & \mathit{if} \quad \neg \exists \nu \leq \lambda (\lambda = 2\nu) \wedge \mathrm{Z}(a). \end{cases}$$

All other values of functions for unmentioned arguments are assumed to be 0.

Let us agree the convention that if $A \subseteq B, f$ is defined on A and g is a certain natural extension of f on B, then they shall be written by the same symbol.

We state following basic theorems on a arithmetic without proof. One will find their proofs easy if he tries to prove these in order.

T.22.1. (i) $\neg(\mathrm{Nat}(a) \wedge \mathrm{Neg}(a))$,

(ii) $-(\lambda-\mu)=\mu-\lambda \wedge \lambda-\mu=\lambda+(-\mu)$,

(iii) $\lambda-\mu=\xi-\nu \rightleftharpoons \lambda+\nu=\xi+\mu$,

(iv) $(\lambda-\mu)+(\xi-\nu)=(\lambda+\xi)-(\mu+\nu)$,

(v) $Z(a) \rightharpoonup \exists\lambda\exists\mu(a=\lambda-\mu)$,

(vi) $Z(a) \wedge Z(b) \rightharpoonup a+b=b+a \wedge (-a)+(-b)=-(a+b)$,

(vii) $Z(a) \wedge Z(b) \wedge Z(c) \rightharpoonup (a+b)+c=a+(b+c)$,

(viii) $Z(a) \rightharpoonup a+0=a \wedge a+(-a)=0$,

(ix) $(\lambda-\mu)\cdot(\xi-\nu)=(\lambda\cdot\xi+\mu\cdot\nu)-(\lambda\cdot\nu+\mu\cdot\xi)$,

(x) $Z(a) \wedge Z(b) \rightharpoonup a\cdot b=b\cdot a \wedge (-a)\cdot(-b)=a\cdot b$,

(xi) $Z(a) \wedge Z(b) \wedge Z(c) \rightharpoonup (a\cdot b)\cdot c=a\cdot(b\cdot c), \wedge (a+b)\cdot c=a\cdot c+b\cdot c$,

(xii) $Z(a) \rightharpoonup a\cdot 0=0 \wedge a\cdot 1=a$,

(xiii) $Z(a) \rightharpoonup a^{\lambda}a^{\mu}=a^{\lambda+\mu} \wedge (a^{\lambda})^{\mu}=a^{\lambda\cdot\mu}$,

(xiv) $Z(a) \wedge Z(b) \wedge a\neq 0 \wedge b\neq 0 \rightharpoonup a\cdot b\neq 0$.

(II) Rational numbers.

D.22.2. (i) $\mathrm{Frc}(a) \Longleftrightarrow a=\langle 1, \alpha, \mu\rangle \wedge Z(\alpha) \wedge \mathrm{Nat}(\mu) \wedge \mu\geq 2 \wedge \mathrm{Prime}(|\alpha|, \mu)$.

(Frc(a) *stands for "a is a fractional (but not an integral) number* α/μ".)

(ii) $Q(a) \Longleftrightarrow Z(a) \vee \mathrm{Frc}(a)$.

($Q(a)$ *stands for "a is a rational number*".)

(iii) $\alpha \div \beta=\gamma \Longleftrightarrow Z(\alpha) \wedge Z(\beta) \wedge \beta\neq 0$

$$\wedge ((Z(\gamma) \wedge \alpha=\beta\cdot\gamma)$$
$$\vee (\mathrm{Frc}(\gamma) \wedge \gamma=\langle 1, \delta, \nu\rangle \wedge \alpha\cdot\nu=\beta\cdot\delta)).$$

(iv) $$\bar{\gamma}=\begin{cases} \gamma, & \textit{if } Z(\gamma), \\ \alpha, & \textit{if } \mathrm{Frc}(\gamma) \wedge \gamma=\langle 1, \alpha, \mu\rangle. \end{cases}$$

(v) $$\underline{\gamma}=\begin{cases} 1, & \textit{if } Z(\gamma), \\ \mu, & \textit{if } \mathrm{Frc}(\gamma) \wedge \gamma=\langle 1, \alpha, \mu\rangle. \end{cases}$$

(vi) $\alpha+\beta=(\bar{\alpha}\cdot\beta+\alpha\cdot\bar{\beta})\div(\alpha\cdot\beta)$, *if* $Q(\alpha)\wedge Q(\beta)$.

(vii) $\alpha\times\beta=(\bar{\alpha}\cdot\bar{\beta})\div(\underline{\alpha}\cdot\underline{\beta})$, *if* $Q(\alpha)\wedge Q(\beta)$.

(viii) $-\alpha=(-\bar{\alpha})\div\underline{\alpha}$.

(ix) $\alpha^{-1}=\underline{\alpha}\div\bar{\alpha}$, *if* $Q(\alpha)\wedge\alpha\neq 0$.

(x) $\alpha-\beta=\alpha+(-\beta)$, *if* $Q(\alpha)\wedge Q(\beta)$.

(xi) $\alpha\div\beta=\alpha\times\beta^{-1}$, *if* $Q(\alpha)\wedge Q(\beta)\wedge\beta\neq 0$.

Remark. We have defined in (iii) the division for integers and in (xi) for rationals, and they are denoted by the same symbol.

T.22.2. (i) $Q(\alpha)\rightarrow Z(\bar{\alpha})\wedge Z(\underline{\alpha})\wedge\alpha\neq 0\wedge\alpha=\bar{\alpha}\div\underline{\alpha}$.

(ii) $Z(\alpha)\wedge Z(\beta)\wedge Z(\gamma)\wedge Z(\delta)\wedge\beta\neq 0\wedge\delta\neq 0\rightarrow(\alpha\div\beta=\gamma\div\delta\rightleftarrows\alpha\cdot\delta=\beta\cdot\gamma)$

$\wedge(\alpha\div\beta)\cdot(\gamma\div\delta)=(\alpha\cdot\gamma)\cdot(\beta\cdot\delta)$

$\wedge(\alpha\div\beta)+(\gamma\div\delta)=(\alpha\cdot\delta+\beta\cdot\gamma)\div(\beta\cdot\delta)$.

(iii) $Q(\alpha)\wedge Q(\beta)\wedge Q(\gamma)\rightarrow\alpha+\beta=\beta+\alpha$

$\wedge(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)\wedge\alpha+(-\alpha)=0\wedge\alpha\cdot\beta=\beta\cdot\alpha$

$\wedge(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)\wedge(\alpha+\beta)\cdot\gamma=\alpha\cdot\gamma+\beta\cdot\gamma\wedge\alpha\cdot 0=0$

$\wedge\alpha\cdot 1=\alpha\wedge(\alpha\neq 0\rightarrow\alpha\cdot\alpha^{-1}=1)\wedge(\alpha\cdot\beta=0\rightarrow\alpha=0\vee\beta=0)$.

(III) Polynomials.

For the sake of brevity we only define here polynomials of one indeterminate with integral coefficients. We define them as sequences of non-vanishing coefficients. Other kinds of polynomials can be defined similarly.

D.22.3. (i) $f\in Z[X]\Leftrightarrow \mathrm{Fnc}(f)\wedge\forall i\in\mathrm{dom}(f)\cdot\mathrm{Nat}(i)\wedge\forall j\in\mathrm{rng}(f)\cdot(Z(j)\wedge j\neq 0)$.

(The symbol Z[*X*] *suggests the set of all polynomials of one variable with integral coefficients. But of course, it does not exist as an h.f. set. Formally f*∈Z[*X*] *is a unary notion of f.)*

(ii) $\deg(f)=\bigcup\mathrm{dom}(f)$.

(iii) $f+g=h\Longleftrightarrow f\in Z[X]\wedge g\in Z[X]\wedge h\in Z[X]\wedge\mathrm{dom}(h)\subseteq\mathrm{dom}(f)\cup\mathrm{dom}(g)$

$\wedge\forall i\in\mathrm{dom}(f)-\mathrm{dom}(g).\ (i\in\mathrm{dom}(h)\wedge h'i=f'i)$

$\wedge\forall i\in\mathrm{dom}(g)-\mathrm{dom}(f).\ (i\in\mathrm{dom}(h)\wedge h'i=g'i)$

$\wedge\forall i\in\mathrm{dom}(f)\wedge\mathrm{dom}(g).\ ((f'i+g'i\neq 0\rightarrow i\in\mathrm{dom}(h)$

$\wedge\, h'i = f'i + g'i) \wedge (f'i + g'i = 0 \rightharpoonup i \notin \mathrm{dom}(h))$.

(iv) $f \cdot g = h \Longleftrightarrow f \in Z[X] \wedge g \in Z[X] \wedge h \in Z[X]$

$\wedge\, \mathrm{dom}(h) = \{k | k \leq \mathrm{dom}(f) + \mathrm{dom}(g) \wedge 0 \neq \sum_{\langle i, j\rangle \in s} f'i \cdot g'j\}$

$\wedge\, \forall k \in \mathrm{dom}(h)(h'k = \sum_{\langle i, j\rangle \in s} f'i \cdot g'j)$,

where s denotes $\{\langle i, j\rangle \in \mathrm{dom}(f) \times \mathrm{dom}(g) | i + j = k\}$.

(v) $\mathrm{Ap}(f, a) = \sum_{i \in \mathrm{dom}(f)} (f'i) \cdot a^i$, *if* $f \in Z[X] \wedge Z(a)$.

($\mathrm{Ap}(f, a)$ *is the value* $f(a)$ *of polynomial* f *at* a.)

(vi) $X = \{\langle 1, 1\rangle\}$, $X^n = \{\langle 1, n\rangle\}$, *if* $\mathrm{Nat}(n)$.

(vii) $[c] = \begin{cases} 0, & \textit{if} \quad c = 0 \\ \{\langle c, 0\rangle\}, & \textit{if} \quad Z(c) \wedge c \neq 0. \end{cases}$

(viii) $-f = g \Longleftrightarrow f \in Z[X] \wedge g \in Z[X] \wedge \mathrm{dom}(f) = \mathrm{dom}(g) \wedge \forall i \in \mathrm{dom}(f)$. $(g'i = -f'i)$.

(ix) $f - g = f + (-g)$ *if* $f \in Z[X] \wedge g \in Z[X]$.

(x) $f | g$ (*divisibility of polynomials*).

The definition of it is left to the reader.

(xi) $f \equiv g \pmod h \Longleftrightarrow h | f - g$.

((iii), (iv), (viii) *are easily justified.*)

T.22.3. (i) $f \in Z[X] \wedge g \in Z[X] \rightharpoonup -f \in Z[X]$

$\wedge\, f + g \in Z[X] \wedge f - g \in Z[X] \wedge f \cdot g \in Z[X]$.

(ii) $f \in Z[X] \wedge g \in Z[X] \wedge h \in Z[X]$

$\rightharpoonup (f + g = g + f \wedge (f + g) + h = f + (g + h) \wedge f + (-f) = 0$

$\wedge\, f \cdot g = g \cdot f \wedge (f \cdot g) \cdot h = f \cdot (g \cdot h) \wedge (f + g) \cdot h = f \cdot h + g \cdot h$

$\wedge\, f \cdot [1] = f \wedge f \cdot 0 = 0)$.

(0 *as polynomial happens to be* 0 *as h.f. set*!)

(iii) $f \in Z[X] \wedge g \in Z[X] \wedge f \neq 0 \wedge g \neq 0$

$\rightharpoonup \deg(f \cdot g) = \deg(f) + \deg(g)$.

(iv) $Z(c) \wedge Z(a) \rightharpoonup [c] \in Z[X] \wedge \deg([c]) = 0 \wedge \mathrm{Ap}([c], a) = c$.

(v) $f \in Z[X] \wedge Z(a) \rightharpoonup Z(\mathrm{Ap}(f, a))$.

(vi) $X \in Z[X] \wedge \deg(X) = 1 \wedge (Z(a) \rightharpoonup \mathrm{Ap}(X, a) = a)$.

(vii) $X^\mu \in Z[X] \wedge \deg(X^\mu) = \mu \wedge \mathrm{Ap}(x^\mu, \lambda) = \lambda^\mu$.

(viii) $f \in Z[X] \wedge g \in Z[X] \rightharpoonup \mathrm{Ap}(f + g, \lambda)$

$= \mathrm{Ap}(f, \lambda) + \mathrm{Ap}(g, \lambda) \wedge \mathrm{Ap}(f \cdot g, \lambda) = \mathrm{Ap}(f, \lambda) \cdot \mathrm{Ap}(g, \lambda)$.

(ix) $f \in Z[X] \wedge h \in Z[X] \wedge \deg(h) > 0$

$\rightharpoonup \exists! g(g \in Z[X] \wedge \deg(g) < \deg(h) \wedge f \equiv g \pmod h)$.

(IV) Elementary theory of polynomials and linear algebra can be developed in FCS. In most cases the usual arguments can be word by word translated into FCS. However there are cases where some care is needed. The following is one of such cases.

(V) Irreducibility of polynomials.

In order to explain what kind of argument is formalizable in FCS and what kind of argument is not, we shall give two methods of determining irreducibility of a polynomial.

1°. The first idea is as follows. Given a polynomial $f(x)$ in $Z[X]$, we compute from its coefficients an upper bound for the absolute values of its roots.

Then we can compute an upper bound of the absolute values of coefficients of any factor of $f(x)$ (by the relation between roots and coefficients). Hence candidates for proper factor of $f(x)$ are finite and we have only to check whether they actually divide $f(x)$ or not (by the usual division algorithm).

Although this method gives us a complete algorithm for deciding whether a given polynomial is irreducible or not, it assumes the existence of roots of $f(x)$ in the complex number field (i.e., the fundamental theorem of algebra). So this method cannot be formalized into FCS until the latter theorem is proved in FCS. (For an effective proof of the fundamental theorem of algebra, see e.g., Rosenbaum [1].)

2°. The second idea is much simpler and due to Kronecker (c.f. van der Waerden [1]). Given a polynomial $f(x)$ in $Z[x]$ of degree n, say. We may assume $n>1$. We compute $f(0), f(1),..., f(n)$. If one of these numbers is 0, then $f(x)$ has a linear factor and hence is not irreducible. Suppose all of these are non-zero. Then if there is any proper factor $g(x)$ of $f(x)$, then $g(0), g(1),..., g(n)$ must be factors of $f(0), f(1),..., f(n)$ respectively. Hence there are only finite number of possibilities of the values $g(0),..., g(n)$. For each set of possible values of $g(0),..., g(n)$, we can compute each coefficient of g since the degree of g is less than n. Hence there are only finite number of possibilities of proper factors of $f(x)$. So we have only to check them as above.

The essence of this method consists in the following two points:

(i) To compute the value $f(i)$ of a given polynomial $f(x)$ at an integer i:

(ii) To determine a polynomial $g(x)$ of degree at most n from its $n+1$ values $g(0), g(1), \ldots, g(n)$, by solving simultaneous linear equations.

Both of these can easily be done in FCS. Hence the second algorithm for deciding the irreducibility of polynomials with integral coefficients can essentially be done in FCS. We shall use this to define the irreducibility of polynomials in $Z[X]$ in FCS.

The above consideration would suggest the similarity between formalizability into FCS and the so-called effectivity which is usually talked intuitively (i.e., without any mathematical definition of it). It is my opinion that the formalizability in FCS is a mathematical definition of effectivity in its strongest sense. Anyway this similarity will become clearer by more examples below.

Now we define the irreducibility of polynomials in $Z[X]$ as mentioned above.

D.22.4. (i) $\mathrm{Cd}(f)=\{g|g\in Z[X]\wedge\deg(g)\leq\deg(f)\wedge\forall i\leq\deg(f).(\mathrm{Ap}(f, i)\neq 0\wedge\mathrm{Ap}(g, i)|\mathrm{Ap}(f, i))\}$, *if* $f\in Z[X]$.

(Cd(f) *is a set of candidates for factors of a polynomial* f.)

(ii) $\mathrm{Ir}_{Z[X]}(f)\Longleftrightarrow f\in Z[X]\wedge(\deg(f)=1\vee(\deg(f)>1\wedge\forall i\leq\deg(f)\cdot \mathrm{Ap}(f, i)\neq 0\wedge\forall g\in\mathrm{Cd}(f)\cdot\forall h\in\mathrm{Cd}(f).(0<\deg(g)<\deg(f) \rightharpoonup f\neq g\cdot h)))$.

($\mathrm{Ir}_{Z[X]}(f)$ *means* f *is an irreducible polynomial.*)

(iii) $\mathrm{Red}_{Z[X]}(f)\Longleftrightarrow f\in Z[X]\wedge\neg\mathrm{Ir}_{Z[X]}(f)\wedge\deg(f)>0$.

($\mathrm{Red}_{Z[X]}(f)$ *means* f *is a reducible polynomial.*)

T.22.4. (i) $\mathrm{Ir}_{Z[X]}(f)\wedge g\in Z[X]\wedge h\in Z[X]\wedge f=g\cdot h \rightharpoonup(\deg(g)=0\wedge\deg(h)=\deg(f))\vee(\deg(g)=\deg(f)\wedge\deg(h)=0)$.

(ii) $\exists g\exists h(g\in Z[X]\wedge h\in Z[X]\wedge\deg(g)\neq 0\wedge\deg(h)\neq 0\wedge f=gh) \vdash\!\dashv\mathrm{Red}_{Z[X]}(f)$.

(iii) $f\in Z[X]\rightharpoonup\mathrm{Ir}_{Z[X]}(f)\vee\mathrm{Red}_{Z[X]}(f)\vee\deg(f)=0$.

The factorization theorem of polynomials can be formulated by the same way as that of natural numbers and proved by the usual method.

Next we define an algebraic number field $Q(\alpha)$, where α is a root of a given irreducible polynomial g in $Z[X]$.

D.22.5. (i) $\beta \in Q\langle g\rangle \Longleftrightarrow \mathrm{Ir}_{Z[X]}(g) \wedge \beta \in Q[X] \wedge \deg(\beta) < \deg(f)$. ($Q[X]$ *is defined similarly to* $Z[X]$.)
$Q\langle g\rangle$ *suggests the algebraic field* $Q(\alpha)$, *where* α *is a root of* g. *Of course* $Q\langle g\rangle$ *is not a set in* FCS, *but formally* $\beta \in Q\langle g\rangle$ *is only a binary relation in* β *and* g.

(ii) $\beta +_{(g)} \gamma = \beta + \gamma$ (*the sum as polynomials*), *if* $\mathrm{Ir}_{Z[X]}(g)$, $\beta \in Q\langle g\rangle \wedge \gamma \in Q\langle g\rangle$.

(iii) $\beta \times_{(g)} \gamma = \delta \Longleftrightarrow \mathrm{Ir}_{Z[X]}(g) \wedge \beta \in Q\langle g\rangle \wedge \gamma \in Q\langle g\rangle \wedge \delta \in Q\langle g\rangle \wedge \beta \cdot \gamma \equiv \delta \pmod{g}$.

Next we consider the problem of effective definition of irreducibility of polynomials in an algebraic field. Let $f(X)$ be a polynomial in $Q(\alpha)[X]$. If we assume, from the beginning, the existence of an algebraically closed field (or at least a Galois extension of Q) containing $Q(\alpha)$, then the problem is easily solved. That is, $f(X)$ is irreducible iff the irreducible polynomial $g(X)$ of $Q[X]$ which has a root in common with $f(X)$ has exactly the degree $\deg(f)+\deg(\alpha)$, where $\deg(\alpha)$ is $[Q(\alpha): Q]$. (And we know the algorithm for computing g from f.)

However in order to extend $Q(\alpha)$ (to an algebraically closed field or a Galois field over Q) it is usually necessary to use an irreducible polynomial in $Q(\alpha)[X]$. So if we want to do it effectively, (e.g. in our system FCS), the notion of irreducibility of polynomials in $Q(\alpha)[X]$ must be effectively defined. But this is the very problem we are considering. So we must avoid this vicious circle.

This difficulty was observed by van der Waerden [1] p. 140–144 (in its 2nd edition, which was intuitionistically written). And he overcame this difficulty by proving the following effective criterion for the irreducibility of polynomials:

Theorem. $f(X)=f(\alpha, X)$ *in* $Q(\alpha)[X]$ *is irreducible in* $Q(\alpha)[X]$ *iff one of the irreducible factors* (*in* $Q[z, u]$ *of* $Nf(\alpha, z-u\alpha)$ *is divisible by* $f(\alpha, z-u\alpha)$, *where* $Nf(\alpha, z-u\alpha)$, *the norm of* $f(\alpha, z-u\alpha)$ *should be defined as the determinent of the matrix* A *whose components are in* $Q[z, u]$ *and which is defined by*

$$\begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix} f(\alpha, z\text{-}u\alpha) = A \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix} \qquad (n = \deg(\alpha)).$$

(*Note that this definition of norm does not use the conjugate elements and that we can prove the necessary properties* $\mathrm{N}(f \cdot g) = \mathrm{N}f \cdot \mathrm{N}g$ *and* $f | \mathrm{N}f$ *by easy computation.*)

The proof of the theorem is by considering the greatest common divisor of $f(\alpha, z-u\alpha)$ and each irreducible factor of $\mathrm{N}f(\alpha, z-u\alpha)$ in $\mathrm{Q}[z, u]$. For further detail, see the above-mentioned book.

On account of the effectivity of this theorem and its proof we define the notion of the irreducible polynomials as follows.

D.22.6. (i) $\mathrm{Ir}_{\mathrm{Z}\langle h\rangle[X]}(f) \Longleftrightarrow \mathrm{Ir}_{\mathrm{Z}[X]}(h) \wedge f \in \mathrm{Z}\langle h\rangle\,[X]$ $\wedge \deg(f) > 0 \wedge \exists q(\mathrm{Ir}_{\mathrm{Z}\langle h\rangle[X,Y]}(q) \wedge \tilde{f} | q \wedge q | \mathrm{N}\tilde{f})$, *where* $\tilde{f} \in \mathrm{Z}\langle h\rangle\,[X, Y]$ *is such that* $\tilde{f}(X, Y) = f(X - Y\alpha)$ *and* $\mathrm{N}f$ *is defined by*

$$\mathrm{N}\tilde{f} = \det(A),$$

$$\begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix} \tilde{f} = A \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}$$

and A *is a matrix each of whose components is in* $\mathrm{Q}[X, Y]$. (*Exact definitions of them in* FCS *are left to the reader.*)

(ii) $\mathrm{Red}_{\mathrm{Z}\langle h\rangle[X]}(f) \Longleftrightarrow f \in \mathrm{Z}\langle h\rangle\,[X] \wedge \supset \mathrm{Ir}_{\mathrm{Z}\langle h\rangle[X]}(f) \wedge \deg(f) > 0.$

Remark. In the above definition the (apparently unbounded) quantifier $\exists q$ can easily be bounded.

T.22.6. (i) $\mathrm{Red}_{\mathrm{Z}\langle h\rangle[X]}(f) \dashv\vdash \exists f_1 \exists f_2 (f_1 \in \mathrm{Z}\langle h\rangle\,[X]$
$\wedge f_2 \in \mathrm{Z}\langle h\rangle\,[X] \wedge \deg(f_1) > 0 \wedge \deg(f_2) \vee 0 \wedge f = f_1 \cdot f_2).$

(ii) $f \in \mathrm{Z}\langle h\rangle\,[X] \rightarrow \mathrm{Ir}_{\mathrm{Z}\langle h\rangle[X]}(f) \vee \mathrm{Red}_{\mathrm{Z}\langle h\rangle[X]}(f) \vee \deg(f) = 0.$

(iii) $\mathrm{Ir}_{\mathrm{Z}\langle h\rangle[X]}(f) \wedge f_1 \in \mathrm{Z}\langle h\rangle\,[X] \wedge f_2 \in \mathrm{Z}\langle h\rangle\,[X]$
$\wedge f = f_1 \cdot f_2 \rightarrow (\deg(f_1) = 0 \wedge \deg(f_2) = \deg(f))$
$\vee (\deg(f_1) = \deg(f) \wedge \deg(f_2) = 0).$

This effective definition of the irreducibility of polynomials enables us to solve the isomorphism and the embedding problems between algebraic fields effectively.

D.22.7. (i) $Q\langle f\rangle \subseteq Q\langle g\rangle \Longleftrightarrow \mathrm{Ir}_{Z[X]}(f) \wedge \mathrm{Ir}_{Z[X]}(g)$
$\wedge \exists f_1(f_1 \mid f \wedge \deg(f_1)=1 \wedge f_1 \in Q\langle g\rangle [X])$.

(ii) $Q\langle f\rangle \simeq Q\langle g\rangle \longleftrightarrow Q\langle f\rangle \subseteq Q\langle g\rangle \wedge Q\langle g\rangle \subseteq Q\langle f\rangle$.

In this manner we can build in FCS the theory of algebraic numbers. For instance, we can define ideals as finite objects and prove their unique factorization theorem in FCS.

Some parts of analytic number theory can also be developed in FCS.

When we try to formalize such a theory, one thing which we should be careful of would be the projective argument, e.g. to form the range of an effectively defined (i.e., primitive recursive) function whose values are among some finite set, and to consider its least element. Such an argument occasionally arises in number theory and as it stands cannot be formalized in FCS. So, for this purpose it should be eliminated or amended by some device (although, in most cases, this is easily accomplished).

Bibliography

(For more information, see Kleene [1] or Péter [3] or Heijenoort [1]).

Asser, G., [1] Rekursive Wortfunktionen, *Z. Math. Logik Grundlagen Math.*, **6** (1960), 258–278.

Axt, P., [1] Enumeration and the Grzegorczyk hierarchy, *Ibid.*, **9** (1963), 53–65.

————, [2] Iteration of primitive recursion, *Ibid.*, **11** (1965), 253–255.

Baker, A., Effective method in number theory, *Proc. Symp. Pure Math. AMS*, **20** (1971), 195–205.

Becker, O., [1] Grundlagen der Mathematik in geschichtlicher Entwickelung.

Church, A., [1] An unsolvable problem of elementary number theory, *Amer. J. Math.*, **58** (1936), 345–363.

Cohen, P. J., [1] *Set theory and the continuum hypothesis,* New York, 1966.

Curry, H., [1] A formalization of recursive arithmetic, *Amer. J. Math.*, **63** (1941), 263–282.

Dedekind, R., [1] *Was sind und was sollen die Zahlen*? 1898.

Davis, M., [1] *Undecidable theories.*

Gentzen, G., [1] Untersuchungen über das logische Schliessen, *Math. Z.*, **39** (1934–35), 176–210, 405–431.

————, [2] Neue Fassung des Widerspruchs freiheitsbeweises für die reine Zahlentheorie, *Forsch. Log. u. Grund. Wiss. new series* no. 4, 1938, 19–44.

————, [3] *The collected papers of Gerhard Gentzen,* ed. by M. E. Szabo, Amsterdam, 1969.

Gödel, K., [1] Über formal unentscheidbare Sätze der Principia Mathematica und verwändter System I., *Manats. für Math. und Phys.,* **38** (1931), 173–198.

————, [2] *Consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory,* Princeton, 1940.

————, [3] Über eine bisher noch nicht benutzte Erweiterung des finiten Standpunktes, *Dialectica,* **12** (1958), 280–287.

Goodstein, R. L., [1] On the restricted ordinal theorem, *J. Symbolic Logic,* **9** (1944), 33–41.

————, [2] Transfinite ordinals in recursive number theory, *Ibid.,* **12** (1947), 123–129.

————, [3] Logic-free formalizations of recursive arithmetic, *Math. Scand.,* **2** (1954), 247–261.

————, [4] *Recursive number theory,* Amsterdam, 1957.

Grzegorczyk, A., [1] Some classes of recursive functions, *Rozprawy Matematyczne* IV, Warsaw, 1953.

Guard, J. R., [1] *Lecture notes on recursive arithmetic,* Princeton (mimeographed), 1962–63.

Heijenoort, J. van, [1] *From Frege to Gödel,* 1967, Cambridge.

Herbrand, J., [1] *Logical writings,* ed. by Goldfarb, W. D.

Hermes, H., [1] *Aufzählbarkeit, Entscheidbarkeit, Berechnenbarkeit.* Berlin, 1961.

Heyting, A., [1] *Intuitionism, an introduction,* Amsterdam, 1956.

Hilbert, D., [1] On the infinite, *Philosophy of mathematics* (ed. by Benacerraf P. and Putnam H.), New Jersey, 1964, 134–151.

Hilbert, D. and Bernays, P., [1] *Grundlagen der Mathematik I, II,* Berlin, 1934, 1939.

Jensen, R. and Karp, C., [1] Primitive recursive set functions, *Proc. Axiomatic Set theory I,* Amer. Math. Soc. 1971, 143–176.

Jeroslow, R. G., [1] *On Gödel's consistency theorem,* mimeographed, 1971.

Kleene, S. C., [1] *Introduction to metamathematics,* Amsterdam, 1952.

Kreisel, G., [1] Set theoretic problems suggested by the notion of potential totality, *Infinistic methods,* Proc. Symp. on Foundations of Mathematics, Warszawa, 1959, 103–140.

————, [2] Mathematical significance of consistency proofs, *J. Symbolic Logic,* **23** (1958), 155–182.

————, [3] Hilbert's Programme, *Philosophy of Mathematics* (ed. by Benacerraf, P. and Putnam, H.), New Jersey, 1964, 157–180.

————, [4] Mathematical logic, *Lectures of Modern Mathematics III* (ed. by Saaty, T. L.), 1965, 95–195.

Kripke, S., [1] Transfinite recursions on admissible ordinals, (abstract), *J. Symbolic Logic,* **29** (1964), 161.

Landau, E., [1] *Elementary number theory,* New York (2nd ed.) 1958.

Lévy, A., [1] A hierarchy of formulas in set theory, *Memoir of AMS,* **57** (1965).

Löb, M. H., [1] Concatenation as basis for a complete system of arithmetic, *J.*

Symbolic Logic, **18** (1953), 1–6.

————, [2] Solution of problem of Leon Henkin, *J. Symbolic Logic*, **20** (1955), 115–118.

————, [3] Formal systems of constructive mathematics, *J. Symbolic Logic*, **21** (1956), 63–75.

————, [4] Constructive truth, *Constructivity in Mathematics*, 159–168.

Mahn, F. K., [1] Zu den primitiv-rekursiven Funktionen über einem Bercich endlicher Mengen, *Archiv. Math. Logik Grundlagenforsch*, **10** (1967), 30–33.

Meyer, A. R., [1] Depth of nesting and the Grzegorczyk hierarchy, *Notice of AMS*, **12** (1965), 342.

Mint, G. E., [1] Quantifier-free and one-quantifier systems, *Journal of Soviet mathematics* (translation) **1**, (1973), 71–84.

————, [2] Exact estimates for provability of the rule of transfinite induction in initial parts of arithmetic, *Ibid.* (1973), 85–91.

Myhill, J. R., [1] A complete theory of natural, rational, and real numbers, *J. Symbolic Logic*, **15** (1950), 185–196.

Nelson, D., [1] Recursive functions and intuitionistic number theory, *Trans. Amer. Math. Soc.*, **71** (1951), 307–368.

Ono, K., Logische Untersuchungen über die Grundlagen der Mathematik, *J. Fac. Sci. Univ. Tokyo Section* 1, **3** (1934–38), 329–389.

Parsons, C., [1] On a number theoretic choice schema and its relation to induction, *Intuitionism and Proof Theory*, Amsterdam, 1970, 459–473.

Peano, G., [1] Formulaire de mathematique, *Rivista di Matematica*. Turin, 1894.

————, [2] Arithmetices Principia nova Methods Exposita. 1899, *Opere Scelte* **2**, Roma, 20–55.

Péter, R., [1] Über den Zusammenhang der verschiedenen Begriffe der rekursiven Funktionen, *Math. Ann.*, **110** (1935), 612–632.

————, [2] Contribution to recursive number theory, *Acta Sci. Math.* (*Szeged.*), **9** (1940), 233–238.

————, [3] *Rekursive Funktionen*, Budapest, 1951. (Zweite aufl. 1957).

Platek, R., [1] *Foundation of recursion theory*, doctoral dissertation.

Pogorzelski, H. A., [1] Recursive arithmetic of Skolem, *Math. Scand.*, **11** (1962), 33–36, II, 156–160.

Reid, C., [1] *Hilbert*. Berlin, New York, 1970.

Ritchie, D. M., [1] Complexity classification of primitive recursive functions by their machine programs, *Notice of AMS*, **12** (1965), 343.

Rödding, D., [1] Primitive rekursive Funktionen über einem Bereich endlicher Mengen, *Archiv. Math. Logik Grundlagenforsch*, **10** (1967), 13–29.

————, [2] Klassen rekursiver Funktionen, *Proc. Summer School Logic, Leeds*, (1967), 159–222.

Rosenbloom, P. C., [1] An elementary constructive proof of the fundamental theorem of algebra, *Math. Monthly*, **52** (1945), 562–570.

Schurchtenberg, H., [1] Rekursionszahlen und die Grzegorczyk-Hierarchie, *Archiv. Math. Logik Grundlagenforsch*.

Selberg, A., [1] An elementary proof of Dirichlet's theorem about primes in arithmetic progression, *Ann. of Math.*, **50** (1949), 297–304.

Shoenfield, J. R., [1] *Mathematical Logic*, Massachusetts, 1967.

Skolem, T., [1] Begründung der elementaren Arithmetik durch die rekurrierende

Denkweise ohne Anwendung scheinbarer Veränderlichen mit unendlichem Ausdehnungsbereich, *Selected works in logic*, by Th. Skolem, Oslo, 1969, 153–188.

———, [2] Eine Bemerkung über die Induktionsschemata in der rekursiven Zahlentheorie, *Ibid.*, 441–449.

———, [3] Some remarks on recursive arithmetic, *Ibid.*, 487–490.

———, [4] A note on recursive arithmetic, *Ibid.*, 491–493.

———, [5] The development of recursive arithmetic, *Ibid.*, 499–514.

———, [6] A remark on induction scheme, *Ibid.*, 515–518.

———, [7] Some considerations concerning recursive arithmetic, *Ibid.*, 563–574.

———, [8] A version of the proof of equivalence between complete induction and the uniqueness of primitive recursions, *Ibid.*, 601–606.

Tait, W. W., [1] Nested recursion, *Math. Ann.*, **143** (1961), 236–250.

Takagi, T., [1] *Lecture on elementary number theory* (Japanese), Tokyo, 1931.

Takahashi, M., [1] An induction principle in set theory I, *Yokohama Math. J.*, **17** (1969), 53–59.

———, [2] Ackermann's model and recursive predicates, *Proc. Japan Acad.*, **44** (1968), 41–42.

———, [3] Many valued logics of extended Gentzen style II, *J. Symbolic Logic*, **35** (1970), 493–528.

Takeuti, G., [1] *A conservative extension of Peano arithmetic*, Lecture note (1972–73).

———, [2] *Sugaku Kisoron*, (Japanese), Tokyo.

van der Waerden, [1] *Moderne algebra I*, zweite Aufl. 1937.

Wette, E., [1] Definition eines (relativ vollständigen) formalen Systems konstruktiver Arithmetik, *Foundation of Mathematics*, Symp. Paper commemorating the 60th birth day of K. Gödel, ed. by J. J. Bulloff et al. 1969.

Weyl, H., [1] *Algebraic theory of numbers*, Princeton, 1940.

———, [2] Randbemerkungen zu Hauptproblem der Mathematik, *Math. Z.*, **20** (1924), 131–150.

Wilder, R. L., [1] *Introduction to the foundations of mathematics*, New York, 1965.

Yasuhara, A., [1] *Recursive function theory and logic*, New York, 1971.