76-8292

ASKANAS, Malgorzata, 1948-
ON TRUTH AND PROVABILITY IN PEANO ARITHMETIC.

The City University of New York
Ph.D., 1976
Mathematics

ON TRUTH AND PROVABILITY IN PEANO ARITHMETIC

by

MAŁGORZATA ASKANAS

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1975

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

October 22, 1975

Chairman of the Examining Committee
Professor Raymond M. Smullyan

October 22, 1975

Executive Officer
Professor Richard Sacksteder

Professor Alex Heller

Professor Arnold Koslow
Supervisory Committee

ACKNOWLEDGEMENTS

I want to express my gratitude to Blanche and Raymond Smullyan, who have created an atmosphere in which work and leisure are indistinguishable and bring equal joy; and who responded to my anxieties and doubts with patience, warmth and sanity. Raymond Smullyan has been my advisor; his advise and influence are responsible for what is of value in this paper.

I want to thank my parents and my friends, whose encouragement, support, help and ridicule enabled me to start, continue and finish this work.

TABLE OF CONTENTS

INTRODUCTION

This paper deals with a version of Gödel's Incompleteness Theorem which, following Raymond Smullyan, we will call "Tarski's version". Gödel's original version, which we will outline below, can be formulated and proven as a theorem of Peano Arithmetic. Tarski's formulation, on the other hand, makes use of some notions that are not directly translatable into the language of arithmetic. We will present a version that does lend itself to such a translation and also, we believe, preserves the essential idea of Tarski's proof.

Peano Arithmetic is a first-order theory whose alphabet consists of two two-argument function symbols: "+", "•", a one-argument function symbol "S", a constant symbol "1" and the equality symbol "=", and whose axioms are:

(P1) $x = y \rightarrow (x = z \rightarrow y = z)$

(P2) $x = y \rightarrow Sx = Sy$

(P3) $1 \neq Sx$

(P4) $Sx = Sy \rightarrow x = y$

(P5) $x + 1 = Sx$

(P6) $x + Sy = S(x + y)$

(P7) $x \cdot 1 = x$

(P8) $x \cdot Sy = (x \cdot y) + x$

(P9) All sentences of the form $F(1) \rightarrow [(\forall x)(F(x) \rightarrow F(Sx)) \rightarrow (\forall x)F(x)]$, where F is any formula with one free variable .

If we let the variables range over the set N of natural numbers, and if we interpret "1", "S", "+", "•", "=" as naming, respectively, the number one, the successor function, addition, multiplication and equality of natural numbers, all the axioms (P1)-(P9) will be satisfied - i.e. this interpretation is a model for Peano Arithmetic. We refer to it as the standard model, and when we talk about a sentence being true we mean that it is true in the standard model. The set of all true sentences will be called the truth set of arithmetic and denoted by Tr.

Any expression consisting of the symbol "1" either by itself or preceded by a finite string of "S"s will be called a numeral. If "1" and "S" are interpreted as above, every natural number n has a unique numeral corresponding to it, which we will denote by $\bar{n}$.

When we talk about a sentence as being provable, or a theorem, it should be understood that we mean "provable from (P1)-(P9)". The set of all theorems will be denoted by Th. The set of all refutable sentences - i.e. those whose negations are provable - will be denoted by Ref. Clearly if a sentence is provable it is also true - thus $Th \subset Tr$. That the converse does not hold, i.e. that the two sets are not equal, is a consequence of Gödel's Theorem.

We say that a set A of natural numbers is expressible if there exists a formula F with one free variable such that for all numbers n

$$F(\bar{n}) \text{ is true iff } n \in A.$$

We say that A is representable if there exists a formula F such that for all n

$$F(\bar{n}) \text{ is provable iff } n \in A.$$

In general, if Σ is any set of sentences of arithmetic, $A \subset N$ will be called Σ-definable - or definable in Σ - if there exists a formula F(x) such that for all n

$$F(\bar{n}) \in \Sigma \text{ iff } n \in A.$$

Thus expressibility and representability are special cases of definability, with Σ being Tr and Th, respectively.

If E_1 and E_2 are two expressions, the expression E_1E_2 consisting of E_1 immediately followed by E_2 is called the concatenation of E_1 and E_2, and denoted by $E_1 * E_2$.

We will assume that a one-to-one function g has been defined from the set of all expressions of arithmetic to N. Such a function is called a Gödel numbering and its value for each expression is called the Gödel number of that expression. We assume that this numbering is admissible, i.e. that there exists a formula G(x,y,z) with three free variables such that the sentence

$$(\forall x)(\forall y)(\exists! z)G(x,y,z)$$

is provable and also for all n, m, k in N

$$G(\bar{n},\bar{m},\bar{k}) \text{ is provable iff } g(g^{-1}(n)*g^{-1}(m)) = k.$$

Thus we want the correspondence between the Gödel numbers of two expressions and the Gödel number of their concatenation to be [illegible]resentable.

If A is a set of expressions, we will denote by $A_{[illegible]}$ [illegible]e image of A under g, and by A^* the set of Gödel numbers of those f[illegible]las with one free variable for which the result of substituting their own Gödel number for the free variable is an element of A. In other words, if $F_n = g^{-1}(n)$, then

$$n \in A^* \text{ iff } F_n(\bar{n}) \in A.$$

The sentence $F_n(\bar{n})$ is called the diagonalization of F_n. A^* is called the normalizer of A. Thus the normalizer of A is the set of Gödel numbers of all formulas whose diagonalizations are in A.

It is obvious that $\bar{A}^* = \overline{A^*}$.

We can now talk about the Incompleteness Theorem. The content of Gödel's original version is that if Peano arithmetic is ω-consistent then there exists a sentence such that neither it nor its negation is provable. By ω-consistency is meant that for any formula F(x) the sentences $F(\bar{1})$, $F(\bar{2})$,... and also $(\exists x)\sim F(x)$ cannot all be provable. Obviously if arithmetic is ω-consistent, it is also consistent (i.e. a sentence and its negation cannot both be provable), as in an inconsistent theory one can prove any sentence whatsoever. Thus an assumption of ω-consistency contains an assumption of consistency.

We will outline Gödel's argument. It turns out that there exist two formulas T(x) and R(x) which express, respectively, the normalizer Th^* of the set of provables and the normalizer Ref^* of the set of refutables. Moreover, if arithmetic is ω-consistent, those two formulas <u>represent</u> Th^* and Ref^*. Thus, if arithmetic is ω-consistent, for every n in N we have

$R(\bar{n})$ is provable iff $n \in Ref^*$.

Also, from the definition of Ref^*

$n \in Ref^*$ iff $F_n(\bar{n})$ is refutable.

Thus for every $n \in N$

$R(\bar{n})$ is provable iff $F_n(\bar{n})$ is refutable.

Let r be the Gödel number of R(x). Then for r in particular

$R(\bar{r})$ is provable iff $F_r(\bar{r})$ is refutable.

But as F_r is R, we get

$R(\bar{r})$ is provable iff $R(\bar{r})$ is refutable.

If arithmetic is consistent (which we have assumed by assuming it is ω-consistent) $R(\bar{r})$ cannot be both provable and refutable. The only other way in which the above equivalence can hold is if $R(\bar{r})$ is neither provable nor refutable. Thus from ω-consistency it follows that there exists a sentence outside of both Th and Ref.

Tarski's version, instead of assuming ω-consistency and thus making $R(x)$ represent Ref^*, uses $R(x)$ to express that set. We use the fact that for every n

$$R(\bar{n}) \text{ is true iff } n \in Ref^*, \text{ iff } F_n(\bar{n}) \text{ is refutable.}$$

So in particular for r – the Gödel number of $R(x)$ – we get

$$R(\bar{r}) \text{ is true iff } F_r(\bar{r}) \text{ is refutable.}$$

But F_r is R, so

$$R(\bar{r}) \text{ is true iff } R(\bar{r}) \text{ is refutable.}$$

This means that $R(\bar{r})$ is either both true and refutable, or not refutable and false. As everything that is provable is true – i.e. everything whose negation is provable must be false – the first of those two possibilities cannot hold. Therefore $R(\bar{r})$ has to be false but not refutable. Being false, $R(\bar{r})$ cannot be provable either – thus, again, $R(\bar{r})$ is outside of both Th and Ref.

Although we did not have to assume ω-consistency here, we did make an assumption of consistency by letting the notion of the truth set into the proof. If we regard Th and Ref as being respective subsets of two disjoint sets – the set of all sentences of arithmetic which are true about N and the set of all those which are false about N – we ipso facto regard them as disjoint.

The purpose of both arguments as we have presented them is to exhibit a sentence which can be neither proven nor refuted, i.e. to show that the two sets Th and Ref, accessible to our formal proof procedure, fail to exhaust the total set of all sentences of arithmetic. This non-exhaustiveness of the two sets is what is meant by the incompleteness of Peano Arithmetic. In Gödel's proof the inaccessible sentence is found by representing Ref, i.e. defining it within Th, in Tarski's - by expressing it, which means defining it in some superset of Th whose complement includes Ref. Plainly the fact that this superset happens to be the truth set is irrelevant, and the role of the superset is completely auxiliary - it is just some set within which Ref^* is conveniently defined.

But we could also say that the very purpose of both arguments is to compare Th with Tr, the provable with the true. The two arguments fulfill this purpose differently. To see this more clearly let us restate Tarski's argument using the formula T(x) expressing Th^* rather than the formula R(x). As T(x) expresses Th, $\neg T(x)$ will express $\overline{Th^*}$.[1] Thus for every n

(*) $\qquad \neg T(\bar{n}) \in Tr$ iff $n \in \overline{Th^*}$, iff $F_n(\bar{n}) \notin Th$.

Let T be the Gödel number of $\neg T(x)$. Then for t in particular we get

$$\neg T(\bar{t}) \in Tr \text{ iff } F_t(\bar{t}) \notin Th.$$

As F_t is $\neg T$, this means

$$\neg T(\bar{t}) \in Tr \text{ iff } \neg T(\bar{t}) \notin Th.$$

Thus the sentence $\neg T(\bar{t})$ is either true and not provable, or else provable but false. The latter possibility is precluded by the fact that Th is a subset of the truth set; it follows that $\neg T(\bar{t})$ has to be in the truth set, but outside of Th.

We can now see the different ways in which our two arguments show that the formal proof procedure is incapable of exhausting Tr. The gist of Gödel's argument is that we exhibit a property of the truth set which does not hold for the set of theorems: the union of the set of all provable sen-

---

1 Throughout this paper, we use " $\neg$ " as our negation symbol.

tences and the set of all sentences with provable negations is not equal to the set of all sentences of arithmetic. The union of the set of all true sentences, though, and all sentences whose negations are true, does exhaust the set of sentences. Therefore provability and truth do not coincide. In Tarski's version, on the other hand, we compare the two sets by directly exhibiting a sentence which is in Tr but not in the set of thoerems. The choice of Tr as the set in which we define $\overline{Th}^*$ is , from this point of view, clearly not arbitrary in the way in which it is if our main purpose were to establish incompleteness - i.e. dictated only by convenience; the expressibility of $\overline{Th}^*$ is the crucial point of the comparison. It establishes a one-to-one correspondence between some subset of the truth set and some subset of Th: some sentence is true if and only if some other sentence is not provable. This correspondence has a fixed point, and that is the sentence which we are looking for. $\overline{Th}^*$ here serves as a mediator between the two sets - every number in $\overline{Th}^*$ forces something into the truth set and something else out of the set of theorems. By a correct choice of the number from $\overline{Th}^*$ we can make those two things coincide.

In this proof, as in Gödel's, there is a particular property with respect to which we are comparing the two sets: their role with respect to the mediator $\overline{Th}^*$. In (*), the right equivalence is motivated by the definition of $\overline{Th}^*$, the left one - by its expressibility. The set on the left can not coincide with the set on the right. Thus

a) Th can not appear in the leftmost statement of (*), i.e. $\overline{Th}^*$ is not Th-definable (which means, not representable) and

b) Tr can not appear in the rightmost statement, i.e. the complement of the normalizer of Tr is not Tr-definable (which means, not expressible). As it can be shown that for any set of sentences Σ representability and expressibility are both transmitted from $g(\Sigma)$ to Σ^* and as, in addition, if a set is expressible, so is its complement, we can conclude that the set of Gödel numbers of nontheorems cannot be represented and the set of Gödel numbers of all true sentences cannot be expressed. The latter result is known as "Tarski's Theorem about the Undefinability of Truth".

The problem we want to deal with is this: It is known that Gödel's proof of the Incompleteness Theorem can be formalized within arithmetic itself. By that we mean that there exists a sentence of arithmetic expressing the fact that if arithmetic is ω-consistent then $R(\bar{r})$ is neither provable nor refutable, as well as a proof of this sentence from the axioms of Peano. Of course the language of arithmetic does not have an apparatus fit for talking directly about sentences or sets of sentences; instead, we talk about Gödel numbers and sets of Gödel numbers. Thus, more precisely, the sentence which is a formal translation of Gödel's Theorem and which is provable from the axioms of Peano expresses the fact that if the set Th_0 is such that together with every number of the form $g((\exists x)\neg F(x))$, it must contain some number of the form $g(\neg F(\bar{n}))$, then $g(R(\bar{r}))$ is in neither of Th_0, Ref_0.

Thus, in Gödel's version of the comparison between provability and truth, the proof that Th lacks a certain property, namely completeness, can be carried out within Peano Arithmetic, i.e. our object language. This is, so to speak, the "internal" part of the comparison. The actual confrontation of the two sets, the observation that as the truth set is complete, the two do not coincide, clearly cannot be so formalized in view of what we have just concluded about the inexpressibility of the truth set. This part of the argument, the "external" part, is incorrigibly metalinguistic.

The question that interests us now is whether we can perform a similar service for Tarski's version. Can Tarski's argument also be divided into an "internal" part, dealing with a certain property of Th and translatable into the object language, and an "external" part formulable only in the metalanguage, effecting the actual confrontation of the two sets? We will show that this is indeed possible and will produce a formalization of the kind desired.

As we will want to talk the object language, instead of considering the two sets of sentences Th and Tr, we will consider their respective sets of Gödel numbers Th_0 and Tr_0. Thus, to restate what we have said about the double equivalence (*), we are now dealing with two number sets and a special kind of one-to-one correspondence between them, "mediated" by a third number set. Below we will try to extract those general features of the proof which will be in accord with the way in which we want to perform the formalization.

Let $U = (U_n)$, $n = 1,2,\ldots$ be a sequence of subsets of N and let $f(x,y)$ be a 1-1 function from $N \times N$ to N. A set $A \subset N$ will be called <u>adequate for (U,f)</u> if for all n, m in N we have

$$f(n,m) \in A \text{ iff } m \in U_n.$$

For any number set X, X^f will be defined as follows:

$$x \in X^f \text{ iff } f(x,x) \in X.$$

Clearly $\bar{X}^f = \overline{X^f}$.

We will call the pair (U,f) <u>normal</u> if for every U_n in U, U_n^f is also in U. We will call (U,f) <u>complemented</u> if U contains the complements of all its members.

THEOREM. If A is adequate for (U,f) and $X^f \varepsilon U$, then $X \neq \bar{A}$.

PROOF. Notice that for any two sets X,Y, the condition that X is different from $\bar{Y}$ is equivalent to saying that there exists some x such that $x \varepsilon X$ iff $x \varepsilon Y$.

Consider any set X for which X^f is in U, i.e. such that there exists an m such that $X^f = U_m$. As A is adequate, we have for every x in N

$$x \varepsilon U_m \text{ iff } f(m,x) \varepsilon A.$$

From the definition of X^f we also have

$$x \varepsilon U_m \text{ iff } f(x,x) \varepsilon X.$$

Thus for every x,

$$f(m,x) \varepsilon A \text{ iff } f(x,x) \varepsilon X.$$

In particular,

$$f(m,m) \varepsilon A \text{ iff } f(m,m) \varepsilon X.$$

Thus there exists some number which is in A if and only if it is in X, which means that $X \neq \bar{A}$.

COROLLARY 1. If A is adequate for (U,f), then $\bar{A}^f$ is not in U.

COROLLARY 2. If (U,f) is normal and complemented, none of the elements of U can be adequate for it.

PROOF. If U is normal and complemented, then if X is in U, so is $\bar{X}^f$. Therefore, from Corollary 1, X cannot be adequate for (U,f).

For our purpose, we define (U,f) as follows: if n is the Gödel number of some formula F_n with one free variable, we take U_n to be the set expressed by that formula and f(n,m) to be the Gödel number of $F_n(\bar{m})$; otherwise we let U_n be $\emptyset$ and f(n,m), for all m, the Gödel number of $\ulcorner(1 = 1)$. Under this definition of (U,f), U_n^f becomes the normalizer of $g^{-1}(U_n)$. In view of what was said before about expressibility, (U,f) is normal and complemented - also, it is clear that the truth set is adequate for it. Thus we can conclude:

(T1) As Th^* is in U, Th_0 is not adequate for (U,f).

(T2) Tr_0 is not in U - i.e. is not expressible.

In (T2) the reader will recognize Tarski's Theorem about the Undefinability of Truth. (T1) gives a suggestion for the "internal" part of Tarski's version of Gödel's Theorem: Could inadequacy with respect to (U,f) be used as the desired property whose posession by Th_0 can be stated and proven within the object language? Can we somehow translate into arithmetic the statement

(**) $\ulcorner(\forall x)(\forall y)(f(x,y) \varepsilon Th_0 \equiv x \varepsilon U_y)$?

Let us state without proof some facts which will be helpful in our attempt at translating (**):

1. It follows from the admissibility of g that there exists a formula S(x,y,z) such that $(\forall x)(\forall y)(\exists ! z)S(x,y,z)$ is provable, and also for all n, m, k $S(\bar{n},\bar{m},\bar{k})$ is provable iff f(n,m) = k.
2. Th is expressible by some formula which we will call P.

We also notice that m ε U_n can be simply written as $F_n(m)$. Thus (**) becomes

(***) $\ulcorner(\forall x)(\forall y)(\forall z)[S(x,y,z) \rightarrow (P(z) \equiv F_x(y))]$.

The problem with (***) is that it contains the symbol $F_x(y)$. For any given x, y, $F_x(y)$ is a sentence of arithmetic which we, knowing what g is, can identify. But it is a <u>different</u> sentence for each x, y, and the function $\alpha(x,y) = F_x(y)$ from N to the set of sentences cannot possibly be defined within arithmetic. We know what $F_x(y)$ is, but the object language does not.

However, we can find a property of Tr_0 whose possession by Th_0 can be denied within arithmetic and such that for every particular n we can find a proof, within arithmetic, of the fact that if Th_0 did have that property, then we would have

$$(\forall y)(\forall z)[S(\bar{n},y,z) \rightarrow (P(z) \equiv F_n(y))].$$

Here is the property we are talking about:

Following Smullyan, we will say that a set Ψ of sentences of arithmetic is saturated, if

a) Ψ contains all true atomic sentences.

b) For any sentence S, Ψ contains either S or its negation, but not both.

c) Ψ contains $S_1 \vee S_2$ iff it contains at least one of S_1, S_2.

d) Ψ contains S_1 & S_2 iff it contains both S_1 and S_2.

e) Ψ contains $(\exists x)S(x)$ iff for some n, it contains $S(\bar{n})$.

f) Ψ contains $(\forall x)S(x)$ iff for all n, it contains $S(\bar{n})$.

It is clear that the truth set fulfills all of (a) - (f).

A set of numbers will be called saturated if it is the set of Gödel numbers of a saturated set of sentences.

Now, for every formula ψ it is possible to construct a sentence - we call it $Sat\psi$ - whose meaning is that the set expressed by ψ is saturated. Also, for every number n which is the Gödel number of some formula F(x) with one free variable, it is possible to construct a proof of

(i) $$Sat\psi \rightarrow (\forall y)(\forall z)[S(\bar{n},y,z) \rightarrow (\psi(z) \equiv F_n(y))].$$

In other words, for every particular n we can construct a proof that $Sat\psi$

implies the set expressed by ψ to be, so to speak, adequate for U_n.

Let F_n^* be the formula expressing U_n^f and let n* be its Gödel number. For every particular n, we next construct a proof of

(ii) $$(\forall z)[S(\bar{n}^*,\bar{n}^*,z) \rightarrow (F_n^*(\bar{n}^*) \equiv F_n(z))].$$

From this, together with

$$\text{Sat } \psi \rightarrow (\forall z)[S(\bar{n}^*,\bar{n}^*,z) \rightarrow (\psi(z) \equiv F_n^*(\bar{n}^*))],$$

which is of the form (i) and therefore provable, we can get

$$\text{Sat } \psi \rightarrow (\forall z)[S(\bar{n}^*,\bar{n}^*,z) \rightarrow (\psi(z) \equiv F_n(z))].$$

As was mentioned before, we can also prove

$$(\forall x)(\forall y)(\exists! z)\ S(x,y,z),$$

and therefore

(iii) $$\text{Sat } \psi \rightarrow (\exists z)(F_n(z) \equiv \psi(z)).$$

In particular, for each n there is a proof of

$$\text{Sat } F_n \rightarrow (\exists z)(\neg F_n(z) \equiv F_n(z))$$

and we can conclude

$$\neg \text{ Sat } F_n.$$

Thus, for every formula F_n it is possible, along these lines, to construct a proof of $\neg$ Sat F_n. In particular, as P is one of F_n, we can prove $\neg$ Sat P.

We see that the internal, object language part of the argument will be that Th is not saturated. We can conclude in the metalanguage that as, to the contrary, the truth set <u>is</u> saturated, the two cannot coincide. It is the goal of this paper to carry out in detail the formalization outlined above.

We further notice that if arithmetic were ω-consistent and complete, the set Th would have all the properties of a saturated set. It also turns out that we can construct a formula ω-Consist to express the ω-consistency of arithmetic and a formula Compl to express its completeness, and that the formula ω-Consist & Compl → Sat P is provable within Peano Arithmetic. Therefore we can obtain a formal proof of ⊢ (ω-Consist & Compl).

It would be nice if, instead of constructing a separate proof of ⊢ Sat ψ for every ψ , we could construct a formula Sat(x) to express the fact that x is the Gödel number of a saturated formula, and if we could then prove the sentence (∀x) ⊢ Sat x. In addition to translating into arithmetic the internal part of Tarski's version of the Incompleteness Theorem, this would also effect a partial embedding into arithmetic of (T2), Tarski's Theorem about the Undefinability of the Truth Set. It would express, within the object language, the fact that no element of U is the image under g of a saturated set of sentences. As Tr_0 is such an image, we could then conclude in the metalanguage, Tr_0 is not in U - i.e. is not expressible. However, we have not been able to find such a formula Sat(x), and have a strong suspicion that it cannot be done.

Our paper is divided into two parts: in the first we construct the formula to express the set Th_0; in the second we develop the machinery that will finally permit us to obtain, for each F_n, a proof of ⊢ Sat F_n, and from there a proof of ⊢ (ω-Cons & Compl). We have also included an Appendix, in which we show how to <u>represent</u> the set Th_0 and how the formula thus obtained, which would be used to carry out Gödel's original proof, differs from the one employed in our argument.

PART I

§1. Description of the Language

The alphabet of arithmetic consists of fifteen symbols: =, +, $\cdot$, $\neg$, $\vee$, &, $\rightarrow$, $\exists$, $\forall$, (,), x, ', S, 1 called, respectively, the equality sign, the addition sign, the multiplication sign, the negation sign, the disjunction sign, the conjunction sign, the implication sign, the existential and universal quantifiers, the left and right parentheses, the eks, the prime, the successor sign and the unit sign.

A finite string of symbols of the alphabet is called an expression. A variable is an expression consisting of the eks followed by primes. A numeral is an expression consisting of the unit sign either by itself or preceded by successor signs.

A term is defined inductively as follows:

(t_0) All variables and all numerals are terms.

(t_1) If τ_1, τ_2 are terms, then so are $S\tau_1$, $(\tau_1 + \tau_2)$ and $(\tau_1 \cdot \tau_2)$.

An expression of the form $\tau_1 = \tau_2$, where τ_1 and τ_2 are terms, is called an atomic formula.

A formula is defined inductively as follows:

(f_0) Every atomic formula is a formula.

(f_1) If ϕ_1, ϕ_2 are formulas, so are $\neg\phi_1$, $(\phi_1 \vee \phi_2)$, $(\phi_1 \& \phi_2)$ and $(\phi_1 \rightarrow \phi_2)$ (called, respectively, the negation of ϕ_1, the disjunction of ϕ_1 and ϕ_2, the conjunction of ϕ_1 and ϕ_2 and the implication with predecessor ϕ_1 and successor ϕ_2. ϕ_1 and ϕ_2 are the disjuncts of $(\phi_1 \vee \phi_2)$ and the conjuncts of $(\phi_1 \& \phi_2)$.)

(f_2) If ϕ is a formula and v a variable, then $(\exists v)(\phi)$ and $(\forall v)(\phi)$ are formulas (and are called, respectively, the existential and universal quantification of ϕ with respect to v).

If ϕ_1 and ϕ_2 are two formulas, we will use $(\phi_1 \equiv \phi_2)$ as shorthand for $((\phi_1 \to \phi_2) \& (\phi_2 \to \phi_1))$.

In a formula containing a quantifier the shorter formula which, surrounded by a left and a right parentheses, immediately follows the quantifier, is called the scope of that quantifier. A bound occurrence of a variable v within a formula ϕ is any occurrence of v in ϕ within the scope of $(\exists v)$ or $(\forall v)$. A free occurrence is one that is not bound. A formula in which no variable has a free occurrence is called a sentence.

If F is a formula whose only free variables are $v_1, v_2, \ldots, v_n$, we will also denote it by $F(v_1, v_2, \ldots, v_n)$. If $\tau_1, \tau_2, \ldots, \tau_n$ are terms, $F(\tau_1, \ldots, \tau_n)$ will denote the formula obtained from $F(v_1, \ldots, v_n)$ by substituting $\tau_1, \ldots, \tau_n$ for $v_1, \ldots, v_n$, respectively.

A term τ is called free for the variable v in the formula ϕ if, for any variable w in ϕ, no free occurrence of v in τ lies within the scope of either $(\exists w)$ or $(\forall w)$.

An instanciation of $(\exists v)(\phi)$ (or of $(\forall v)(\phi)$) is any formula obtained from ϕ by substituting the same numeral throughout for v.

§2. Interpretations

An interpretation of arithmetic is obtained in the following way: we specify a set X, an element u of X, a relation $E \subset X \times X$, a one-argument function $\sigma: X \to X$ and two two-argument functions $\alpha, \mu: X \times X \to X$. The choice of these uniquely determines a function i which assigns an element of X to every term not containing variables (such terms are called <u>pure</u>) and one of the symbols t,f to every sentence, in accordance with the following conditions:

1. $i(1) = u$

2. For every pure term τ, $i(S\tau) = \ (i(\tau))$

3. For any two pure terms τ_1, τ_2

$$i((\tau_1 + \tau_2)) = \alpha(i(\tau_1), i(\tau_2))$$

$$i((\tau_1 \cdot \tau_2)) = \mu(i(\tau_1), i(\tau_2))$$

4. For any two pure terms τ_1, τ_2

$$i(\tau_1 = \tau_2) = \begin{cases} t \text{ if } (i(\tau_1), i(\tau_2)) \in E \\ f \text{ otherwise} \end{cases}$$

5. For any sentence s, $i(\neg s) = \begin{cases} t \text{ if } i(s) = f \\ f \text{ otherwise} \end{cases}$

6. For any two sentences s_1, s_2

$$i((s_1 \vee s_2)) = \begin{cases} t \text{ if at least one of } i(s_1), i(s_2) \text{ is } t \\ f \text{ otherwise} \end{cases}$$

$$i((s_1 \,\&\, s_2)) = \begin{cases} t \text{ if both } i(s_1), i(s_2) \text{ are } t \\ f \text{ otherwise} \end{cases}$$

$$i((s_1 \rightarrow s_2)) = \begin{cases} t \text{ if } i(s_1) = f \text{ or } i(s_1) = i(s_2) = t \\ f \text{ otherwise} \end{cases}$$

7. For any formula ϕ with one free variable v, if s_1 is $(\exists v)(\phi)$ and s_2 is $(\forall v)(\phi)$, then

$$i(s_1) = \begin{cases} t \text{ if } i \text{ assigns } t \text{ to at least one instanciation of } s_1 \\ f \text{ otherwise} \end{cases}$$

$$i(s_2) = \begin{cases} t \text{ if } i \text{ assigns } t \text{ to all instanciations of } s_2 \\ f \text{ otherwise} \end{cases}$$

Sentences that are assigned the value t under a given interpretation are called _true_ under that interpretation. Those assigned the value f are called _false_ under the interpretation.

§3. The Axioms of Arithmetic

The following sentences comprise Peano's Axioms of Arithmetic:

(P1) All sentences of the form

$$(\forall u)((\forall v)((\forall w)((u = v \to (u = w \to v = w)))))$$

(P2) All sentences of the form

$$(\forall u)((\forall v)((u = v \to Su = Sv)))$$

(P3) All sentences of the form

$$(\forall u)(\neg\, 1 = Su)$$

(P4) All sentences of the form

$$(\forall u)((\forall v)((Su = Sv \to u = v)))$$

(P5) All sentences of the form

$$(\forall u)((u + 1) = Su)$$

(P6) All sentences of the form

$$(\forall u)((\forall v)((u + Sv) = S(u + v)))$$

(P7) All sentences of the form

$$(\forall u)((u \cdot 1) = u)$$

(P8) All sentences of the form

$$(\forall u)((\forall v)((u \cdot Sv) = ((u \cdot v) + u)))$$

(P9) All sentences of the form

$$(F(1) \to ((\forall u)(F(u) \to F(Su)) \to (\forall u)F(u)))$$

where u,v,w are any three variables and F is any formula with one free variable.

A <u>model</u> of arithmetic is an interpretation under which all of the above axioms are true. In particular if for X we take the set N of natural numbers and for u, E, σ, α, μ we take, respectively, the number one, equality, the successor function, addition and multiplication of natural numbers, we obtain an interpretation of arithmetic which is also a model. We call it the <u>standard model</u>. We will refer to the sentences true in the standard model simply as true, and to the set of all such sentences as to the <u>truth set</u> of arithmetic. We will denote this set by Tr.

Under the standard interpretation every number n corresponds to a unique numeral. This numeral mill be denoted by $\bar{n}$.

The following formulas will serve as our logical axioms:

(L1) All formulas of the form

$$(F \to (G \to F))$$

(L2) All formulas of the form

$$((F \to (G \to H)) \to ((F \to G) \to (F \to H)))$$

(L3) All formulas of the form

$$((\neg G \to \neg F) \to ((\neg G \to F) \to G))$$

where F, G, H are any three well-formed formulas.

(L4) All formulas of the form

$$((\forall u)(F(u)) \to F(\tau))$$

where u is a variable, F a formula, and τ is a term free for u in F(u).

(L5) All formulas of the form

$$((\forall u)((F \rightarrow G)) \rightarrow (F \rightarrow (\forall u)(G)))$$

where F, G are formulas and u is a variable with no free occurrence in F.

To explain the usage of the other connectives we also add, for any two formulas F, G and any variable v

(L6) All formulas of the form

$$((F \rightarrow G) \rightarrow (\neg F \vee G))$$

$$((\neg F \vee G) \rightarrow (F \rightarrow G))$$

(L7) All formulas of the form

$$(\neg(\neg F \vee \neg G) \rightarrow (F \& G))$$

$$((F \& G) \rightarrow \neg(\neg F \vee \neg G))$$

(L8) All formulas of the form

$$((\exists v)(F) \rightarrow \neg(\forall v)(\neg F))$$

$$(\neg(\forall v)(\neg F) \rightarrow (\exists v)(F))$$

A formula of arithmetic is called _provable_ (or a _theorem_) if it is a logical axiom, an axiom of arithmetic, or can be obtained from a finite number of axioms (of either kind) by a finite number of applications of the following _rules of inference_:

(I1) (Modus Ponens): From $(F \rightarrow G)$ and F, obtain G.

(I2) (Generalization): From F, obtain $(\forall u)(F)$ for any variable u.

In other words, a formula is provable if it is the last element of some finite sequence of formulas, each of which is either an axiom or has been obtained from some previous elements of the sequence by one of the rules of inference. Such a sequence is a _proof_ of its last element.

A <u>refutable</u> formula is one whose negation is provable.

The set of all theorems will be denoted by Th, the set of all refutables - by Ref. To say that arithmetic is <u>consistent</u> is to assert that Th and Ref are disjoint, i.e. that no formula can be both proven and refuted. For arithmetic to be <u>complete</u> every sentence would have to belong to either Th or Ref - whatever sentence we take, either it or its negation would have to be provable.

We will also need the notions of ω-consistency and ω-completeness. To say that arithmetic is <u>ω-consistent</u> means to assert that if $F(\bar{n})$ can be proven for every natural number n, then $(\exists v)(\neg F(v))$ is not provable. In other words, if there exists a proof of $(\exists v)(\neg F(v))$, then at least one of the formulas $F(\bar{n})$ does not have a proof.

For any two formulas F and G, $((F \,\&\, \neg F) \rightarrow G)$ is a theorem of arithmetic. It follows that if arithmetic is inconsistent, every formula can be proven. Therefore if arithmetic is assumed to be ω-consistent (which excludes some formulas from being provable), it is also assumed to be consistent.

To say that arithmetic is <u>ω-complete</u> is to assert that if $F(\bar{n})$ can be proven for every natural number n, then $(\forall v)(F(v))$ also has to be provable. For every formula F, the formula $(\neg(\exists v)(\neg F(v)) \rightarrow (\forall v)(F(v)))$ is a theorem of arithmetic. Therefore if arithmetic is ω-consistent and complete, it is also ω-complete.

§4. <u>Gödel Numbering</u>

As numerals tend to be very long strings, we will use the decimal notation for natural numbers as shorthand for the corresponding numerals. Thu, for instance, we will write 2 instead of S1 and 10 instead of SSSSSSSSS1.

We would like to construct a one-to-one correspondence between expressions of arithmetic and natural numbers, in order to be able to talk about expressions and sets of expressions within the object language itself. For this purpose we will employ the <u>seventeen-adic</u> representation of the natural numbers. Under this representation we let the symbols 1, 2, 3, 4, 5, 6, 7, 8, 9, T, E, ʃ, ɛ, ɟ, ƹ, ∂, ʕ correspond to the first seventeen natural numbers, and any string $a_k a_{k-1} \ldots a_0$ of these symbols correspond to the number $n_0 + n_1 \cdot 17 + \ldots + n_k \cdot 17^k$, where $n_0, n_1, \ldots, n_k$ are the numbers represented by $a_0, a_1, \ldots, a_k$, respectively. Thus, for instance, ʃ1ɟ is the seventeen-adic name of $14 + 1 \cdot 17 + 12 \cdot 17^2$, i.e. of three thousand four hundred ninety nine.

As we have mentioned earlier, by the <u>concatenation</u> $\eta_1 * \eta_2$ of two expressions η_1, η_2 we mean the expression consisting of η_1 immediately followed by η_2.

We define our one-to-one function g from the set of all expressions of arithmetic into the set of natural numbers as follows: let g assign to each of the alphabet symbols

= + · ⌐ v & → ∃ ∀ ( ) x ' S 1

the number whose seventeen-adic representation is, respectively

1 2 3 4 5 6 7 8 9 T E ʃ ɛ ɟ ƹ

and let $g(\eta_1 * \eta_2)$ be the number whose seventeen-adic name consists of $g(\eta_1)$ immediately followed by $g(\eta_2)$. Thus, for instance, g[x'(=] is the number represented by ʃɛT1.

For any expression η, $g(\eta)$ is called the Gödel number of η. If X is any set of expressions, X_0 will denote the image of X under g.

In addition to our shorthand practice concerning numerals, which was introduced above, we will adopt the following notational conventions:

If a formula is a disjunction, we will omit the parentheses around any disjunct which is itself a disjunction.

If a formula is a conjunction, we will omit the parentheses around any conjunct which is itself a conjunction.

In a formula which has the form of an implication we will omit the parentheses around the antecedent (or the consequent) provided that it itself does not have the form of an implication.

In a formula which is a conjunction we will omit the parentheses around any conjunct which has the form of a disjunction.

If a formula does not appear as part of another formula, we will omit the parentheses around it.

In forming the quantification of a formula F we may just write the quantifier in front of F, without putting F in an additional set of parentheses.

In a term which is a sum, we will omit the parentheses around any summand which is a product.

In a term which does not appear as part of another term, we will omit the parentheses around it.

For clarity, in addition to parentheses we will also use brackets and rosters. Also, we will use the letters r, s, t,..., z with or without subscripts as shorthand for the variables of the object language.

§5. Concatenation Is Expressible

Let A be a subset of N. We say that A is expressible iff there exists a formula F with one free variable such that for all natural numbers n

$$F(\bar{n}) \text{ is true iff } n \in A.$$

Such a formula expresses the set A. In general, a formula $F(v_1,\ldots,v_k)$ expresses a relation R iff for every k-tuple $n_1,\ldots, n_k$ of natural numbers

$$F(\bar{n}_1,\ldots,\bar{n}_k) \text{ is true iff R holds between } n_1,\ldots, n_k.$$

Suppose that s_1 and s_2 are the seventeen-adic names of two numbers n_1 and n_2. Then by $n_1 \circ n_2$ we denote the number whose seventeen-adic name consists of s_1 immediately followed by s_2. In particular if n_1, n_2 are the Gödel numbers of some two expressions, $n_1 \circ n_2$ will be the Gödel number of their concatenation.

We want to show that the function $z = x \circ y$ assigning the number $n_1 \circ n_2$ to the pair (n_1,n_2) is expressible. We notice that if $l(y)$ is the length (i.e. the number of digits) of the seventeen-adic name of y, then

$$x \circ y = x \cdot 17^{l(y)} + y.$$

The smallest number of length $l(y)$ is $\underbrace{11\ldots1}_{l(y)}$, which is equal to $1 + \frac{17^{l(y)} - 17}{16}$; the largest such number is $\underbrace{\Gamma\Gamma\ldots\Gamma}_{l(y)}$, which is $17(1 + \frac{17^{l(y)} - 17}{16})$. Therefore

$$1 + \frac{17^{l(y)} - 17}{16} \leq y \leq 17\left(1 + \frac{17^{l(y)} - 17}{16}\right),$$

which means

$$17^{l(y)} - 1 \leq 16y \leq 17(17^{l(y)} - 1)$$

Therefore $v = 17^{l(y)}$ iff v is a power of 17 such that

(*) $\qquad v - 1 \leq 16y \leq 17(v - 1)$

The property "v is a power of 17" is expressed by the formula

$P_{17}(v)$: $(\exists y)(v = 17 \cdot y)$ & $[(\exists y)(v = y \cdot x) \rightarrow x = 1 \vee (\exists w)(x = 17 \cdot w)]$

which expresses the fact that v, and all its proper divisors, are divisible by 17. (*), on the other hand, is expressed by

(**) $S(16 \cdot y) = v \vee 16 \cdot y + 17 = 17 \cdot v \vee [(\exists w)(v + w = S(16 \cdot y))$ & $(\exists w)((16 \cdot y + 17) + w = 17 \cdot v)]$

Thus we obtain the following formula to express $x \circ y = z$:

$x \circ y = z$: $(\exists v)(P_{17}(v)$ & (**) & $z = x \cdot v + y)$

We show later (Lemma 15.4) that the operation $\circ$ can be proven to be associative - i.e. the formula $(\forall x)(\forall y)(\forall z)((x \circ y) \circ z = x \circ (y \circ z))$ is a theorem of arithmetic. It seems that establishing this result now would not add to the clarity of our paper; therefore we take the liberty of using the associativity of $\circ$ before it has been proven and of dropping parentheses from expressions indicating multiple applications of $\circ$.

For any fixed k, we can express the function assigning to any k-tuple $(n_1,\ldots,n_k)$ of natural numbers the number $n_1 \circ n_2 \ldots \circ n_k$ by the formula

$y = x_1 \circ x_2 \ldots \circ x_k$: $(\exists y_1)\ldots(\exists y_{k-2})(y_1 = x_1 \circ x_2$ & $y_2 = x_2 \circ x_3$ &...& $y_{k-2} = x_{k-2} \circ x_{k-1}$ & $y = y_{k-2} \circ x_k)$.

§6. Finite Sequences

We will encode finite sequences of Gödel numbers of either terms or formulas[1] by means of the following device: If $(n_1,\ldots,n_k)$ is such a sequence, we encode it using the number $1 \circ 1 \circ n_1 \circ 1 \circ 1 \circ n_2 \circ \ldots \circ 1 \circ 1 \circ n_k \circ 1 \circ 1$, which we call the sequence number of $(n_1,\ldots,n_k)$.

1 as natural numbers

By "n begins m" we mean that the seventeen-adic name of n constitutes the initial part of the seventeen-adic representation of m. The expressions "n ends m", "n is part of m" should be understood analogously. All of these relations are expressible, by means of the following formulas:

x begins y

xBy: $x = y \vee (\exists z)(x \circ z = y)$

x ends y

xEy: $x = y \vee (\exists z)(z \circ x = y)$

x is part of y:

xPy: $xBy \vee xEy \vee (\exists z_1)(\exists z_2)(z_1 \circ x \circ z_2 = y)$.

We can also represent

x is a sequence number

Seq x: $1 \circ 1Bx \,\&\, 1 \circ 1Ex \,\&\, \neg\, 1 \circ 1 = x \,\&\, \neg\, 1 \circ 1 \circ 1Px$

y is an element of the sequence with sequence number x

$y \in x$: $\text{Seq } x \,\&\, 1 \circ 1 \circ y \circ 1 \circ 1Px$

z appears earlier than y in the sequence with number x

$z \underset{x}{<} y$: $\text{Seq } x \,\&\, y \in x \,\&\, (\exists t)(\text{Seq } t \,\&\, tBx \,\&\, z \in t \,\&\, \neg\, y \in t)$

§7. On Closures of Sets under Relations

Let R be a k-nary relation whose field is F. We say that a subset A of F is closed under R if, for all $a_1, \ldots, a_k \in F$, if $a_1, \ldots a_{k-1}$ are in A and $R(a_1, \ldots, a_k)$ holds, then $a_k \in A$. In other words A is closed under R if any element of F that stands in the relation R to some elements of A must also be in A.

The <u>closure</u> of A under R is the smallest superset of A closed under R. We denote it by A_R.

LEMMA. Let us define the following sequence of supersets of A:

$$A_0 = A$$

$$A_n = A_{n-1} \cup \{x \in F: (\exists x_1)\ldots(\exists x_{k-1})(x_1,\ldots, x_{k-1} \in A_{n-1} \ \& \ R(x_1,\ldots,x_{k-1},x))\}$$

Thus A_n is obtained from A_{n-1} by adjoining all elements of F which stand in the relation R to some elements of A_{n-1}.

Then $A_R = \bigcup A_n$.

PROOF. Let $B = \bigcup_n A_n$. Obviously $A \subset B$ and $A_0 \subset A_1 \subset \ldots \subset A_n \subset \ldots$. We have to show that (1) B is closed under R and (2) it is the smallest superset of A with this property. To prove (1), let us assume that $a_1,\ldots, a_{k-1} \in B$ and that $R(a_1,a_2,\ldots,a_{k-1},a_k)$ holds. Each of the a_i's for $i = 1, \ldots, k-1$ must belong to some A_{n_i}, and as the A_n's form an ascending chain, there is some A_{n_0} to which all these a_i's belong. But as $R(a_1,\ldots,a_{k-1},a_k)$ holds, a_k must belong to A_{n_0+1}, and therefore to B.

To show (2), let C be any superset of A closed with respect to R. We show that $B \subset C$. Obviously $A_0 \subset C$. Let us assume that $A_n \subset C$ and that $x \in A_{n+1}$. Then either x is in A_n, in which case it will be in C by assumption, or else there exist some $a_1, a_2,\ldots, a_{k-1}$ in A_n such that $R(a_1,\ldots,a_{k-1},x)$ holds. But as $a_1, a_2,\ldots, a_{k-1} \in C$ and as C is closed under R, x must also be in C. Therefore $A_{n+1} \subset C$. Hence all the A_n's are subsets of C and so is their union, B. We have proven (2), and thus our Lemma.

If $s_1 = (a_1,\ldots,a_{k_1})$ and $s_2 = (b_1,\ldots, b_{k_2})$ are two finite sequences, then by $s_1 \Delta s_2$ we will denote the sequence $(a_1,a_2,\ldots,a_{k_1},b_1,b_2,\ldots,b_{k_2})$.

THEOREM 7.1. x belongs to the closure of A under R if and only if there exists a finite sequence of elements of F having x as its last element, such that every element of the sequence either belongs to A or stands in the relation R to some earlier elements of the sequence.

PROOF. First we show that if such a sequence exists, then $x \varepsilon A_R$. If $(x_1,x_2,\ldots,x_m)$ is our sequence $(x_m = x)$, then x must be an element of A. Assume that all elements preceding x_n are in A_R. x_n either is in A - in which case we are done - or it stands in the relation R to some earlier elements of the sequence, all of which are in A_R. As A_R is closed under R, x_n must be in A_R as well. Thus all elements of our sequence are in A_R; in particular this is true of the last element, which is x.

Next let us assume that x is in A_R and construct the desired sequence. If $x \varepsilon A$, (x) will be such a sequence. Suppose now that sequences of the kind described exist for all elements of A_n and let x be in A_{n+1}. Then either x is in A_n - in which case we are done - or there are some $a_1,\ldots,a_{k-1} \varepsilon A_n$ such that $R(a_1,\ldots,a_{k-1},x)$ holds. Let $s_1,\ldots,s_{k-1}$ be the sequences for a_1, $\ldots a_{k-1}$, respectively. Then $s_1 \Delta s_2 \Delta \ldots \Delta s_{k-1} \Delta (x)$ is the desired sequence for x. We see that such a sequence can be found for any element of any of the A_n's, and therefore for any element of A_R.

THEOREM 7.2. If $A \subset N$ and $R \subset N^k$ are both expressible, then so is A_R.

PROOF. Let F_A and F_R be the formulas expressing A and R, respectively. According to Theorem 7.1, n is in A_R iff there exists a sequence $(n_1,\ldots,n_m)$ of natural numbers such that $n_m = n$ and every element of the sequence either belongs to A or else stands in the relation R to some earlier elements of the sequence. Thus the following formula will serve to express A_R:

$$A_R(x): \quad (\exists y)\{\mathrm{Seq}\ y\ \&\ 1 \circ 1 \circ x \circ 1 \circ 1 E y\ \&\ (\forall w)[w \in y \rightarrow F_A(w) \vee (\exists w_1)$$
$$(\exists w_2)\ldots(\exists w_{k-1})(w_1 \underset{y}{\lneq} w\ \&\ \ldots \&\ w_{k-1} \underset{y}{\lneq} w\ \&\ F_R(w_1,\ldots,w_{k-1},w))]\}.$$

§8. The Set of Formulas is Expressible

We will make use of the fact (see [3]) that for every natural number c, the relation $y = c^x$ is expressible.

We denote by Q the function which assigns to every natural number the Gödel number of its numeral. The numeral $\bar{n}$ consists of a string of n-1 successor signs followed by a 1. Hence Q(n) will be the number whose seventeen-adic name consists of a string of n-1 ʮ's followed by a ʔ, which is the number $14 \cdot (\frac{17^n - 17}{16}) + 15$. Therefore the following formula Q(x,y) expresses the function Q:

$$Q(x,y): \quad (x = 1\ \&\ y = 15) \vee (\exists y_1)(17^x = 16 \cdot y_1 + 17\ \&\ y = 14 \cdot y_1 + 15)$$

and we also obtain a formula to express the fact that x is the Gödel number of a numeral:

$$\mathrm{Num}\ x: \quad (\exists y)\ Q(x,y).$$

As under our Gödel numbering 12 and 13 correspond to x and ', respectively, the Gödel number of a variable will have a seventeen-adic representation of the form ʃɛɛ...ɛ . Thus the following formula expresses the property "x is the Gödel number of a variable":

$$\mathrm{Var}\ x: \quad (\exists y)[12 \circ y = x\ \&\ (\forall z)(zPy \rightarrow 13Pz)].$$

tb(x,y,z) will express the fact that z is the Gödel number of an expression resulting from the expressions with Gödel numbers x, y by one of the "term building" operations - i.e. either preceding an expression by "S" or putting one of "+", "·" between two expressions, with the appropriate placement of parentheses.

$tb(x,y,z)$: $z = 14 \circ x \vee z = 10 \circ x \circ 2 \circ y \circ 11 \vee z = 10 \circ x \circ 3 \circ y \circ 11.$

τ is a term iff it belongs to the closure of the set of all numerals and variables with respect to the "term building" operations. Therefore x is the Gödel number of a term iff it belongs to the closure of the set of Gödel numbers of all numerals and variables with respect to the operation tb expressed above. By Theorem 7.2 the set of Gödel numbers of all terms is expressible by some formula, which we call Term x.

Atf x will express the fact that x is the Gödel number of an atomic formula.

Atf x: $(\exists y)(\exists z)(\text{Term } y \ \& \ \text{Term } z \ \& \ x = y \circ 1 \circ z)$..

fb(x,y,z) will express the fact that z is the Gödel number of an expression obtained from the expressions with Gödel numbers x and y by one of the "formula building" operations - negating an expression, forming disjunctions, conjunctions and implications, or preceding an expression by a quantifier followed by a variable - with the correct placement of parentheses.

$fb(x,y,z)$: $z = 4 \circ x \vee z = 10 \circ x \circ 5 \circ y \circ 11 \vee z = 10 \circ x \circ 6 \circ y \circ 11 \vee z = 10 \circ x \circ 7 \circ y \circ 11 \vee (\exists v)(\text{Var } v \ \& \ (z = 10 \circ 8 \circ v \circ 11 \circ 10 \circ x \circ 11 \vee z = 10 \circ 9 \circ v \circ 11 \circ 10 \circ x \circ 11)).$

The Gödel number of a formula is an element of the closure of the set of numbers of atomic formulas under the operation fb. We will call the formula expressing the fact that x is such a number For x.

§9. Provability is Expressible

The formula $SB(x_1,x_2,y_1,y_2,z_1,z_2,v)$ will express the fact that the expression with Gödel number z_2 is "built up" from the expressions numbered x_2 and y_2 by the use of logical connectives, equality and operation symbols in exactly the same way in which the expression with number z_1 is built up from the ones numbered x_1 and y_1. Also, if both z_1 and z_2 are numbers of quantifier formulas, the quantification should be with respect to a variable (the same one in both cases) different from the one numbered v.

$$SB(x_1,x_2,y_1,y_2,z_1,z_2,v): \quad \mathrm{Var}\ v \ \&\ \{(z_1 = 14 \circ x_1 \ \&\ z_2 = 14 \circ x_2) \vee (z_1 = 10 \circ x_1 \circ 2 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 2 \circ y_2 \circ 11) \vee (z_1 = 10 \circ x_1 \circ 3 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 3 \circ y_2 \circ 11) \vee (z_1 = x_1 \circ 1 \circ y_1 \ \&\ z_2 = x_2 \circ 1 \circ y_2) \vee (z_1 = 4 \circ x_1 \ \&\ z_2 = 4 \circ x_2) \vee (z_1 = 10 \circ x_1 \circ 5 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 5 \circ y_2 \circ 11) \vee (z_1 = 10 \circ x_1 \circ 6 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 6 \circ y_2 \circ 11) \vee (z_1 = 10 \circ x_1 \circ 7 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 7 \circ y_2 \circ 11) \vee (\exists v_1)[\mathrm{Var}\ v_1 \ \&\ \neg\, v_1 = v \ \&\ ((z_1 = 10 \circ 8 \circ v_1 \circ 11 \circ 10 \circ x_1 \circ 11 \ \&\ z_2 = 10 \circ 8 \circ v_1 \circ 11 \circ 10 \circ x_2 \circ 11) \vee (z_1 = 10 \circ 9 \circ v_1 \circ 11 \circ 10 \circ x_1 \circ 11 \ \&\ z_2 = 10 \circ 9 \circ v_1 \circ 11 \circ 10 \circ x_2 \circ 11))]\}.$$

Let us encode <u>pairs</u> of expressions by using $2 \circ 2$ as a separator between the Gödel numbers of the first and the second element of the pair.

The formula BegSub(v,t,w) expresses the fact that w is the number of a pair whose first element is a variable, a numeral or a quantifier formula where the quantification is with respect to the variable numbered v, and whose second element results from the first by substituting the expression with number t for the variable with number v.

$$\mathrm{BegSub}(v,t,w): \quad \mathrm{Var}\ v \ \&\ (\exists u_1)(\exists u_2)[w = u_1 \circ 2 \circ 2 \circ u_2 \ \&\ ((\mathrm{Num}\ u_1 \ \&\ u_2 = u_1)$$

$\vee$ (Var u_1 & $\neg$ $u_1 = v$ & $u_1 = u_2$) $\vee$ ($u_1 = v$ & $u_2 = t$) $\vee$ $(\exists u_3)$(For u_3 & ($u_1 = 10 \circ 8 \circ v \circ 11 \circ 10 \circ u_3 \circ 11 \vee u_1 = 10 \circ 9 \circ v \circ 11 \circ 10 \circ u_3 \circ 11$) & $u_2 = u_1$)].

We can now express the fact that y is the Gödel number of the result of substituting the expression with number w for the variable numbered v in the expression numbered x.

Subst(x,v,w,y): $(\exists z)$[Seq z & $x \circ 2 \circ 2 \circ y \circ 1 \circ 1$Ez & $(\forall t)(t \in z \rightarrow$ BegSub(v,w,t) $\vee$ $(\exists t_1)(\exists t_2)(\exists x_1)(\exists x_2)(\exists y_1)(\exists y_2)(\exists z_1)(\exists z_2)(t_1 = x_1 \circ 2 \circ 2 \circ x_2$ & $t_2 = y_1 \circ 2 \circ 2 \circ y_2$ & $t = z_1 \circ 2 \circ 2 \circ z_2$ & SB$(x_1,x_2,y_1,y_2,z_1,z_2,v)))$].

Inst_1(x,y,z) will express the fact that y is the number of the instanciation of the formula with Gödel number x obtained by substituting the numeral with number z for the variable following the quantifier.

Inst_1(x,y,z): $(\exists x_1)(\exists v)$(Var v & Num z & ($x = 10 \circ 8 \circ v \circ 11 \circ 10 \circ x_1 \circ 11 \vee x = 10 \circ 9 \circ v \circ 11 \circ 10 \circ x_1 \circ 11$) & Subst$(x_1,v,z,y)$).

Inst(x,y) expresses the relation of y being the Gödel number of an instanciation of the formula with Gödel number x.

Inst(x,y): $(\exists z)$ Inst(x,y,z).

Free(v,x) expresses the fact that the variable with Gödel number v occurs free in the formula numbered x.

Free(v,x): $(\forall y)$(Subst(x,v,15,y) $\rightarrow$ y = x).

FrTerm(t,v,x) expresses the fact that the term with number t is free for the variable with number v in the formula numbered x.

FrTerm(t,v,x): For x & Var v & Term t & $(\forall w)$\{Var w & [w = t $\vee$ $(\exists t_1)(\exists t_2)(\neg$ 13Bt_2 & ($t = t_1 \circ w \vee t = w \circ t_2 \vee t = t_1 \circ w \circ t_2$) $\rightarrow \neg$ $(\exists y)$(Free(v,y) & $10 \circ 8 \circ w \circ 11 \circ 10 \circ u \circ 11$Px $\vee$ $10 \circ 9 \circ w \circ 11 \circ 10 \circ y \circ 11$Px)]\}.

ArAx(x) expresses the fact that x is the Gödel number of one of the axioms of arithmetic.

ArAx(x): $(\exists u)(\exists v)(\exists w)\{\mathrm{Var}\ u\ \&\ \mathrm{Var}\ v\ \&\ \mathrm{Var}\ w\ \&\ [x = 10\circ 9\circ u\circ 11\circ 10\circ 10\circ$
$9\circ v\circ 11\circ 10\circ 10\circ 9\circ w\circ 11\circ 10\circ 10\circ u\circ 1\circ v\circ 7\circ 10\circ u\circ 1\circ w\circ 7\circ v\circ$
$1\circ w\circ 11\circ 11\circ 11\circ 11\circ 11 \lor x = 10\circ 9\circ u\circ 11\circ 10\circ 10\circ 9\circ v\circ 11\circ 10\circ$
$10\circ u\circ 1\circ v\circ 7\circ 14\circ u\circ 1\circ 14\circ v\circ 11\circ 11\circ 11 \lor x = 10\circ 9\circ u\circ 11\circ$
$10\circ 4\circ 15\circ 1\circ 14\circ u\circ 11 \lor x = 10\circ 9\circ u\circ 11\circ 10\circ 10\circ 9\circ v\circ 11\circ$
$10\circ 10\circ 14\circ u\circ 1\circ 14\circ v\circ 7\circ u\circ 1\circ v\circ 11\circ 11\circ 11 \lor x = 10\circ 9\circ u\circ$
$11\circ 10\circ 10\circ u\circ 2\circ 15\circ 11\circ 1\circ 14\circ u\circ 11 \lor x = 10\circ 9\circ u\circ 11\circ 10\circ$
$10\circ 9\circ v\circ 11\circ 10\circ 10\circ u\circ 2\circ 14\circ v\circ 11\circ 1\circ 14\circ 10\circ u\circ 2\circ v\circ 11\circ$
$11\circ 11 \lor x = 10\circ 9\circ u\circ 11\circ 10\circ 10\circ u\circ 3\circ 15\circ 11\circ 1\circ u\circ 11 \lor$
$x = 10\circ 9\circ u\circ 11\circ 10\circ 10\circ 9\circ v\circ 11\circ 10\circ 10\circ u\circ 3\circ 14\circ v\circ 11\circ 1\circ$
$10\circ 10\circ u\circ 3\circ v\circ 11\circ 2\circ u\circ 11\circ 11\circ 11 \lor (\exists y)(\exists y_1)(\exists y_2)(\mathrm{Free}(u,y)$
$\&\ \mathrm{Subst}(y,u,15,y_1)\ \&\ \mathrm{Subst}(y,u,14\circ u,y_2)\ \&\ x = 10\circ y_1\circ 7\circ 10\circ$
$10\circ 9\circ u\circ 11\circ 10\circ y\circ 7\circ y_2\circ 11\circ 7\circ 10\circ 9\circ u\circ 11\circ y\circ 11\circ 11\circ 11)]\}.$

LogAx(x) represents the set of Gödel numbers of logical axioms.

LogAx(x): $(\exists y)(\exists w)(\exists z)\{\mathrm{For}\ y\ \&\ \mathrm{For}\ w\ \&\ \mathrm{For}\ z\ \&\ [x = 10\circ y\circ 7\circ 10\circ w\circ 7\circ$
$y\circ 11\circ 11 \lor x = 10\circ 10\circ y\circ 7\circ 10\circ w\circ 7\circ z\circ 11\circ 11\circ 7\circ 10\circ 10\circ$
$y\circ 7\circ w\circ 11\circ 7\circ 10\circ y\circ 7\circ z\circ 11\circ 11\circ 11 \lor x = 10\circ 10\circ 4\circ w\circ 7\circ$
$4\circ y\circ 11\circ 7\circ 10\circ 10\circ 4\circ w\circ 7\circ y\circ 11\circ 7\circ w\circ 11\circ 11 \lor (\exists v)(\exists t)$
$(\exists y_1)(\mathrm{FrTerm}(t,v,y)\ \&\ \mathrm{Subst}(y,v,t,y_1)\ \&\ x = 10\circ 10\circ 9\circ v\circ 11\circ$
$10\circ y\circ 11\circ 7\circ y_1\circ 11\ ) \lor (\exists v)(\mathrm{Var}\ v\ \&\ \neg \mathrm{Free}(v,y)\ \&\ x = 10\circ 10\circ$
$9\circ v\circ 11\circ 10\circ 10\circ y\circ 7\circ w\circ 11\circ 11\circ 7\circ 10\circ y\circ 7\circ 10\circ 9\circ v\circ 11\circ$
$10\circ w\circ 11\circ 11\circ 11) \lor x = 10\circ 10\circ y\circ 7\circ w\circ 11\circ 7\circ 10\circ 4\circ y\circ$
$5\circ w\circ 11\circ 11 \lor x = 10\circ 10\circ 4\circ y\circ 5\circ w\circ 11\circ 7\circ 10\circ y\circ 7\circ w\circ 11\circ 11$

$\vee\ x = 10 \circ 4 \circ 10 \circ 4 \circ y \circ 5 \circ 4 \circ w \circ 11 \circ 7 \circ 10 \circ y \circ 6 \circ w \circ 11 \circ 11 \vee x = 10 \circ$
$10 \circ y \circ 6 \circ w \circ 11 \circ 7 \circ 4 \circ 10 \circ 4 \circ y \circ 5 \circ 4 \circ w \circ 11 \circ 11 \vee (\exists v)(\mathrm{Var}\ v\ \&$
$x = 10 \circ 10 \circ 8 \circ v \circ 11 \circ 10 \circ y \circ 11 \circ 7 \circ 4 \circ 10 \circ 9 \circ v \circ 11 \circ 10 \circ 4 \circ y \circ 11 \vee$
$x = 10 \circ 4 \circ 10 \circ 9 \circ v \circ 11 \circ 10 \circ 4 \circ y \circ 11 \circ 7 \circ 10 \circ 8 \circ v \circ 11 \circ 10 \circ y \circ 11 \circ 11)]\}.$

Inf(x,y,z) expresses the fact that the formula with Gödel number z can be obtained from the formulas with numbers x and y by one of the rules of inference.

Inf(x,y,z): $\mathrm{For}\ x\ \&\ \mathrm{For}\ y\ \&\ (x = 10 \circ y \circ 7 \circ z \circ 11 \vee (\exists v)(\mathrm{Var}\ v\ \&$
$z = 10 \circ 9 \circ v \circ 11 \circ 10 \circ x \circ 11)).$

Proof(x,y) will express the fact that x is the sequence number of a proof of the formula with Gödel number y.

Proof(x,y): $\mathrm{Seq}\ x\ \&\ 1 \circ 1 \circ y \circ 1 \circ 1\mathrm{Ex}\ \&\ (\forall z)[z \in x \to \mathrm{ArAx}\ z \vee \mathrm{LogAx}\ z \vee$
$(\exists z_1)(\exists z_2)(z_1 \underset{x}{<} z\ \&\ z_2 \underset{x}{<} z\ \&\ \mathrm{Inf}(z_1,z_2,z))]$

and Prov x expresses Th_0 - i.e. the fact that x is the Gödel number of a theorem of arithmetic.

Prov x: $(\exists y)\ \mathrm{Proof}(x,y).$

PART II

§10. The Formula Sat ψ

Given any formula ψ with one free variable, we now wish to construct a formula Sat ψ to express the fact that the set expressed by ψ is the set of Gödel numbers of a saturated set of sentences.

Let $A(x,y,z)$ and $M(x,y,z)$ denote the following formulas:

$A(x,y,z)$: $(\exists x_1)(\exists y_1)(\exists z_1)(Q(x_1,x) \ \& \ Q(y_1,y) \ \& \ Q(z_1,z) \ \& \ x_1 = y_1 + z_1)$

$M(x,y,z)$: $(\exists x_1)(\exists y_1)(\exists z_1)(Q(x_1,x) \ \& \ Q(y_1,y) \ \& \ Q(z_1,z) \ \& \ x_1 = y_1 \cdot z_1)$

$A(x,y,z)$ expresses the fact that y and z are the Gödel numbers of some numerals $\bar{y}_1$, $\bar{z}_1$, and x is the number of $\overline{y_1 + z_1}$. In $M(x,y,z)$ again y and z are the Gödel numbers of some $\bar{y}_1$, $\bar{z}_1$; x now is the number of $\overline{y_1 \cdot z_1}$.

If ψ is any formula with one free variable, Sat ψ will be the universal quantification over x of the conjunction of the following formulas:

1. (Identity Input): $(\forall y_1)(\forall y_2)[\text{Num } y_1 \ \& \ \text{Num } y_2 \ \& \ x = y_1 \circ 1 \circ y_2 \rightarrow (\psi(x) \equiv y_1 = y_2)]$
2. (Addition Input): $(\forall y)(\forall z)(\forall w)[\text{Num } y \ \& \ \text{Num } z \ \& \ \text{Num } w \ \& \ x = 10 \circ z \circ 2 \circ w \circ 11 \circ 1 \circ y \rightarrow (\psi(x) \equiv A(y,z,w))]$
3. (Multiplication Input): $(\forall y)(\forall z)(\forall w)[\text{Num } y \ \& \ \text{Num } z \ \& \ \text{Num } w \ \& \ x = 10 \circ z \circ 3 \circ w \circ 11 \circ 1 \circ y \rightarrow (\psi(x) \equiv M(y,z,w))]$
4. (Symmetry): $(\forall y)(\forall z)(\forall w)(x = y \circ 1 \circ z \ \& \ w = z \circ 1 \circ y \ \& \ \psi(w) \rightarrow \psi(x))$
5. (Transitivity): $(\forall y)(\forall z)(\forall u)(\forall w)(\forall v)(x = y \circ 1 \circ u \ \& \ w = y \circ 1 \circ z \ \& \ v = z \circ 1 \circ u \ \& \ \psi(w) \ \& \ \psi(v) \rightarrow \psi(x))$
6. (Congruence): $(\forall y)(\forall z)(\forall w)(\forall u)[(x = 14 \circ y \circ 1 \circ 14 \circ z \ \vee$

   $x = 10 \circ y \circ 2 \circ w \circ 11 \circ 1 \circ 10 \circ z \circ 2 \circ w \circ 11 \ \vee$

   $x = 10 \circ w \circ 2 \circ y \circ 11 \circ 1 \circ 10 \circ z \circ 2 \circ w \circ 11 \ \vee$

$x = 10 \circ y \circ 3 \circ w \circ 11 \circ 1 \circ 10 \circ z \circ 3 \circ w \circ 11 \vee$

$x = 10 \circ w \circ 3 \circ y \circ 11 \circ 1 \circ 10 \circ z \circ 3 \circ w \circ 11) \& u = y \circ 1 \circ z \& \psi(u) \rightarrow \psi(x)]$

7. (Disjunction): $(\forall y)(\forall z)[x = 10 \circ y \circ 5 \circ z \circ 11 \rightarrow (\psi(x) \equiv \psi(y) \vee \psi(z))]$

8. (Conjunction): $(\forall y)(\forall z)[x = 10 \circ y \circ 6 \circ z \circ 11 \rightarrow (\psi(x) \equiv \psi(y) \& \psi(z))]$

9. (Implication): $(\forall y)(\forall z)[x = 10 \circ y \circ 7 \circ z \circ 11 \rightarrow (\psi(x) \equiv \psi(z) \vee \neg\psi(y))]$

10. (Existential Quantifier): $(\forall v)(\forall y)[\text{Var } v \& x = 10 \circ 8 \circ v \circ 11 \circ 10 \circ y \circ 11$
$\rightarrow (\psi(x) \equiv (\exists z)(\text{Inst }(x,z) \& \psi(z)))]$

11. (Universal Quantifier): $(\forall v)(\forall y)[\text{Var } v \& x = 10 \circ 9 \circ v \circ 11 \circ 10 \circ y \circ 11$
$\rightarrow (\psi(x) \equiv (\forall z)(\text{Inst}(x,z) \rightarrow \psi(z)))]$

12. (Negation): $(\forall y)[x = 4 \circ y \rightarrow (\psi(x) \equiv \neg\psi(y))]$

Formulas 1 through 6 describe the atomic sentences whose Gödel numbers lie in the set Ψ expressed by ψ: all sentences of the form $\bar{n} = \bar{n}$, all sentences of the form $\bar{n} + \bar{m} = \overline{n + m}$ and all sentences of the form $\bar{n} \cdot \bar{m} = \overline{n \cdot m}$. Also, if the Gödel number of $\tau_1 = \tau_2$ lie in Ψ, so does the number of $\tau_2 = \tau_1$; if the numbers of $\tau_1 = \tau_2$ and $\tau_2 = \tau_3$ lie in Ψ, so does the number of $\tau_1 = \tau_3$; and if the number of $\tau_1 = \tau_2$ is in Ψ, so are the numbers of $S\tau_1 = S\tau_2$, $\tau_1 + \tau = \tau_2 + \tau$, $\tau + \tau_1 = \tau_2 + \tau$, $\tau_1 \cdot \tau = \tau_2 \cdot \tau$, $\tau \cdot \tau_1 = \tau_2 \cdot \tau$. Formulas 7 through 18 describe the composite sentences whose Gödel numbers are in Ψ: Ψ contains the Gödel number of a disjunction iff it contains the number of at least one of the disjuncts; it contains the Gödel number of a conjunction iff it contains the numbers of both conjuncts; it contains the number of an existential (universal) quantification iff it contains the number of some (the numbers of all) of the instanciations; finally, Ψ contains the Gödel number of the negation of a formula iff it does not contain the number of the formula itself.

Actually, Sat ψ as defined above expresses the fact that those sentences whose Gödel numbers do lie in Ψ form a saturated set, but it does not prevent Ψ from containing numbers of non-sentences as well. To achieve this we would add the clause

$$\psi(x) \rightarrow \text{For } x \ \& \ (\forall v)(\text{Var } v \rightarrow \neg \text{ Free}(v,x)).$$

Our main purpose will be to show the provability of all formulas of the form Sat $\psi \rightarrow (\exists x)(H(x) \equiv \psi(x))$, where H and ψ are any two formulas with one free variable. From there we will be able to conclude that $\neg$ Sat F is provable for any formula F; indeed, by substituting F for ψ and $\neg F$ for H in the above, we conclude the provability of

$$\text{Sat } F \rightarrow (\exists x)(\neg F(x) \equiv F(x)),$$

from which $\neg$ Sat F follows.

§11. Auxiliaries

The proofs of the following theorems of arithmetic can be found in standard logic texts:

I. $(\forall x)(\forall y)(\forall w)(\forall v)(x = y \rightarrow (x = w \rightarrow (y = v \rightarrow w = v)))$

II. $(\forall x)(x = x)$

III. $(\forall x)(\forall y)(x = y \rightarrow y = x)$

IV. $(\forall x)(\forall y)(\forall z)(x = y \ \& \ y = z \rightarrow x = z)$

V. $(\forall x)(\forall y)(\forall z)(x = y \rightarrow (z = y \rightarrow x = z))$

VI. $(\forall x)(\forall y)(\forall z)(x = y \rightarrow x + z = y + z)$

VII. $(\forall x)(\forall y)(x + y = y + x)$

VIII. $(\forall x)(\forall y)(\forall z)(x = y \rightarrow z + x = z + y)$

IX. $(\forall x)(\forall y)(\forall z)((x + y) + z = x + (y + z))$

X. $(\forall x)(\forall y)(\forall z)(x + z = y + z \rightarrow x = y)$

XI. $(\forall x)(\forall y)(\forall z)(x = y \rightarrow x \cdot z = y \cdot z)$

XII. $(\forall x)(\forall y)(x \cdot y = y \cdot x)$

XIII. $(\forall x)(\forall y)(\forall z)(x = y \rightarrow z \cdot x = z \cdot y)$

XIV. $(\forall x)(\forall y)(\forall z)((x \cdot y) \cdot z = x \cdot (y \cdot z))$

XV. $(\forall x)(\forall y)(\forall z)((x + y) \cdot z = (x \cdot z) + (y \cdot z))$

XVI. $(\forall x)(\forall y)(\forall z)(z \cdot (x + y) = (z \cdot x) + (z \cdot y))$

XVII. $(\forall x)(\neg\, x = 1 \rightarrow (\exists y)(x = Sy))$

XVIII. $(\forall x)(\forall y)(\neg\, (x + y = y))$

XIX. $(\forall x)(\forall y)(\forall z)(x \cdot z = y \cdot z \rightarrow x = y)$

XX. $(\forall x)(\forall y)(\forall z)(z \cdot x = z \cdot y \rightarrow x = y)$

As we have mentioned earlier, we will make use of the fact that for any number c, the function $y = c^x$ is expressible and the properties of exponentiation given below can be proven from the formula expressing it.

XXI. $c^1 = c$

$(\forall x)(c^{Sx} = c^x \cdot c)$

$(\forall x)(\forall y)(x = y \rightarrow c^x = c^y)$

XXII. $(\forall x)(\forall y)(\neg\, c = 1 \;\&\; c^x = c^y \rightarrow x = y)$

Let the relation $x < y$ be defined by the formula $(\exists z)(x + z = y)$. $x \leq y$ will be defined by $x < y \quad x = y$.

XXIII. $(\forall x)(x < Sx)$

XXIV. $(\forall x)(\forall v)(\forall z)(x < y \;\&\; y < z \rightarrow x < z)$

XXV. $(\forall x)(\forall y)(\forall z)(x = y \;\&\; y < z \rightarrow x < z)$

XXVI. $(\forall x)(\forall y)(\forall z)(x < y \;\&\; y = z \rightarrow x < z)$

XXVII. $(\forall x)(\forall y)(\forall z)(x \leq y \;\&\; y \leq z \rightarrow x \leq z)$

XXVIII. $(\forall x)(1 \leq x)$

XXIX. $(\forall x)(\forall y)(\forall z)(x < y \rightarrow z + x < z + y)$

XXX. $(\forall x)(\forall y)(\forall z)(x \leq y \rightarrow z + x \leq z + y)$

XXXI. $(\forall x)(\forall y)(x < y \rightarrow Sx \leq y)$

XXXII. $(\forall x)(\forall y)(x < y \vee x = y \vee y < x)$

XXXIII. $(\forall x)(\forall y)(\neg(x < y \ \& \ y < x))$

XXXIV. $(\forall x)(\forall y)(\neg(x < y \ \& \ x = y))$

XXXV. $(\forall x)(\forall y)(x < Sy \rightarrow x < y \vee x = y)$

XXXVI. $(\forall x)(\forall y)(\forall z)(x < y \rightarrow z \cdot x < z \cdot y)$

XXXVII. $(\forall x)(\forall y)(\forall z)(\forall w)(x \leq y \ \& \ z \leq w \rightarrow x + z \leq y + w)$

XXXVIII. $(\forall x)(\forall y)(\neg\, y = 1 \rightarrow x < x \cdot y)$

XXXIX. $(\forall x)(\forall y)(c^{x+y} = c^{x} \cdot c^{y})$

XL. $(\forall x)(\forall y)(x < y \ \& \ \neg\, c = 1 \rightarrow c^{x} < c^{y})$

XLI. $(\forall x)(\forall y)(x \leq y \rightarrow c^{x} \leq c^{y})$

We let the function $z = x - y$ be defined by the formula $z + y = x$.

XLII. $(\forall x)(\forall y)(\forall z)(x < y \rightarrow z - y < z - x)$

XLIII. $(\forall x)(\forall y)(\forall z)(x = y \rightarrow x - z = y - z)$

XLIV. $(\forall x)(\forall y)(\forall z)(x < y \rightarrow x - z < y - z)$

XLV. $(\forall x)(\forall y)(\forall z)(x \leq y \rightarrow x - z \leq y - z)$

XLVI. $(\forall x)(\forall y)(\forall z)((x - y) \cdot z = (x \cdot z) - (y \cdot z))$

XLVII. $(\forall x)(\forall y)(\forall z)(x = y \rightarrow z - x = z - y)$

Let $y \mid x$ be defined by the formula $(\exists w)(y \cdot w = x)$.

XLVIII. $(\forall x)(\forall y)(\forall z)(z \mid x \ \& \ z \mid y \rightarrow z \mid x + y)$

XLIX. $(\forall x)(\forall y)(\forall z)(z \mid x \rightarrow z \mid x \cdot y)$

L. $(\forall x)(\forall y)(\forall z)(x \mid y \ \& \ y = z \rightarrow x \mid z)$

LI. $(\forall x)(\forall y)(\forall z)(x \mid y + z \ \& \ x \mid y \rightarrow x \mid z)$

LII. $(\forall x)(\forall y)(17 \mid x \cdot y \rightarrow 17 \mid x \vee 17 \mid y)$

§12. Reducing the Definition of Concatenation

We recall that concatenation was expressed by the formula

$$x \circ y = z: \quad (\exists v)\{P_{17}(v) \mathbin{\&} [S(16 \cdot y) = v \vee 16 \cdot y + 17 = 17 \cdot v \vee ((\exists w)(v + w = S(16 \cdot y)) \mathbin{\&} (\exists w)((16 \cdot y + 17) + w = 17 \cdot v)) \mathbin{\&} z = x \cdot v + y]\},$$

where $P_{17}(v)$ is shorthand for

$$(\exists v_1)[v = 17 \cdot v_1 \mathbin{\&} (\forall v_2)((\exists v_3)(v = v_2 \cdot v_3 \rightarrow v = 1 \vee (\exists v_4)(v_2 = 17 \cdot v_4)))].$$

Writing , as we did in §11, $x - y = z$ for $x = y + z$, $x < y$ for $(\exists x_1)(x + x_1 = y)$, $x \leq y$ for $x < y \vee x = y$, and $x \mid y$ for $(\exists x_1)(x \cdot x_1 = y)$, we can rewrite $P_{17}(v)$ as

$$17 \mid v \mathbin{\&} (\forall v_2)(v_2 \mid v \rightarrow v_2 = 1 \vee 17 \mid v_2)$$

and the formula expressing $x \circ y = z$ as

$$(\exists v)(P_{17}(v) \mathbin{\&} v - 1 \leq 16 \cdot y \mathbin{\&} 16 \cdot y \leq 17 \cdot (v - 1) \mathbin{\&} z = x \cdot v + y).$$

LEMMA 12.1. For all natural numbers n, m, k

a1) $\bar{n} = \bar{n}$ is provable

a2) $\neg\, \bar{n} = \bar{m}$ is provable for $n \neq m$

b1) $\bar{n} + \bar{m} = \overline{n + m}$ is provable

b2) $\neg\, \bar{n} + \bar{m} = \bar{k}$ is provable for $k \neq n + m$

c1) $\bar{n} \cdot \bar{m} = \overline{n \cdot m}$ is provable

c2) $\neg\, \bar{n} \cdot \bar{m} = \bar{k}$ is provable for $k \neq n \cdot m$.

PROOF. We will start with (b1), which we show by induction in the metalanguage. For $m = 1$, $\overline{n + m}$ is $S\bar{n}$ and, for every n, $\bar{n} + \bar{1} = S\bar{n}$ follows from Axiom (P5). Let us assume that $\bar{n} + \bar{m} = \overline{n + m}$ is provable. We have to show that so is $\bar{n} + \overline{Sm} = \overline{n + Sm}$. As $\overline{n + Sm}$ is $\overline{Sn + m}$, what should be provable is $\bar{n} + S\bar{m} = S\overline{n + m}$. The latter, though, given our inductive assumption, is a consequence of Axiom P6.

We now show (a). The provability of $\bar{n} = \bar{n}$ follows from the provability of II, §11. On the other hand, if $n \neq m$, then for some $k \in N$ either $n + k = m$ or $m + k = n$; we can assume without loss of generality that it is the former. In view of (b1), $\bar{n} + \bar{k} = \bar{m}$ must be provable; Thus $\bar{n} < \bar{m}$ is provable. Using XXXIII we can then show $\vdash \bar{n} = \bar{m}$.

To establish (b2): If $n + m \neq k$, then for some l we have $n + m = l$ and $l \neq k$. Therefore – as we have just shown – $\bar{n} + \bar{m} = \bar{l}$ and $\vdash \bar{l} = \bar{k}$ are provable. So is

$$\bar{n} + \bar{m} = \bar{l} \rightarrow (\bar{n} + \bar{m} = \bar{k} \rightarrow \bar{k} = \bar{l}),$$

by Axiom P1. Thus we can conclude $\vdash \bar{n} + \bar{m} = \bar{k}$.

The proofs of (c1) and (c2) are analogous to those of (b1) and (b2).

Consequently, for any numbers n, m, if any of the sentences $\bar{n} < \bar{m}$, $\bar{n} \leq \bar{m}$ is true, it is also provable.

LEMMA 12.2. For every natural number n and any variable v, the sentence

$$(\forall v)(v < \bar{n} \rightarrow v = \bar{1} \vee v = 2 \vee \ldots \vee v = \overline{n - 1})$$

is provable.

PROOF. We show this by induction with respect to n. If n is 1, our claim is vacuously true. Suppose that it is true for some m. We show that then

$$(\forall v)(v < \overline{m + 1} \rightarrow v = 1 \vee v = 2 \vee \ldots \vee v = \bar{m})$$

can be proven. As $\overline{m + 1}$ is $S\bar{m}$, this can be written as

$$(\forall v)(v < S\bar{m} \rightarrow v = 1 \vee v = 2 \vee \ldots \vee v = \bar{m}).$$

We know that

$$(\forall v)(v < S\bar{m} \rightarrow v < \bar{m} \vee v = \bar{m})$$

is provable (XXXV), and so - by assumption - is

$$(\forall v)(v < \bar{m} \rightarrow v = 1 \vee v = 2 \vee \ldots \vee v = \overline{m-1}.$$

From these two we conclude the desired

$$(\forall v)(v < S\bar{m} \rightarrow v = 1 \vee v = 2 \vee \ldots \vee v = \overline{m-1} \vee v = \bar{m}).$$

LEMMA 12.3. The formula $(\forall x)(P_{17}(x) \equiv (\exists y)(x = 17^y))$ is provable.

PROOF. We start with $(\forall x)(P_{17}(x) \rightarrow (\exists y)(x = 17^y))$. Let $LP(x,y)$ denote the formula

$$17^w \leq x \ \& \ 17^{Sw} > x,$$

expressing the fact that 17^w is the largest power of 17 not exceeding x. It can easily be seen that $(\forall x)[x \leq 17 \rightarrow (\exists w)(LP(x,w))]$ and $(\forall x)(\forall w_1)(\forall w_2)[LP(x,w_1) \ \& \ LP(x,w_2) \rightarrow w_1 = w_2]$ expressing, respectively, the existence and uniqueness of this largest power, are both provable; for $x \geq 17$ we can thus write $w = lp(x)$ in place of $LP(x,w)$. As $P_{17}(x)$ contains the condition that x is divisible by 17, we can prove - using XXXVIII of §11 - $(\forall x)(P_{17}(x) \rightarrow x \geq 17)$, and thus also $(\forall x)[P_{17}(x) \rightarrow (\exists w)(LP(x,w))]$.

We will prove $(\forall x)[P_{17}(x) \rightarrow (\exists y)(x = 17^y)]$ by induction on $lp(x)$. When $lp(x) = 1$, we can infer $x = 17 \cdot x_1$ for some x_1 (as x is divisible by 17) and $x_1 < 17$. This implies $\neg 17 \mid x_1$ and therefore, as we assume $P_{17}(x)$, we have to conclude $x_1 = 1$ and hence $x = 17^1$.

Assume now that our claim holds for $lp(x) = n$ and let x be such that $lp(x) = n + 1$. We can conclude that for some w_1, w_2 we have

$$x = 17^{n+1} \cdot w_1 \vee x = 17^{n+1} \cdot w_1 + w_2,$$

where $w_1 < 17$. The first disjunct again implies $w_1 = 1$ and $x = 17^{n+1}$. From the second disjunct we can infer (LI) $w_2 = 17 \cdot w_3$ for some w_3, and therefore $x = 17(17^n \cdot w_1 + w_3)$. As we can show $lp(17^n \cdot w_1 + w_3) = n$, our inductive assumption yields $17^n \cdot w_1 + w_3 = 17^y$ for some y - and thus we get $x = 17 \cdot 17^y = 17^{y+1}$.

We now establish the provability of

$$(\forall x)(\forall y)(x = 17^y \to P_{17}(x))$$

by induction on y. Using XXXVIII of §11 and Lemma 12.2 we can obtain

$$(\forall z)(z \mid 17 \to z = 1 \vee z = 2 \ \ldots \vee z = 17),$$

and therefore also

$$(\forall z)(z \mid 17 \to z = 1 \vee z = 17),$$

which implies $P_{17}(17)$.

Assume now that

$$(\forall x)(x = 17^n \to P_{17}(x))$$

can be proven; we will prove $(\forall x)(x = 17^{n+1} \to P_{17}(x))$. Clearly $17 \mid 17^{n+1}$ is provable. Let us assume $z \mid 17^{n+1}$; we can conclude (LII) $z \mid 17 \vee z \mid 17^n$ and, by our inductive assumption, infer $z = 1 \vee 17 \mid z$, which concludes our proof.

Thus the formula expressing $x \circ y = z$ reduces to

$$(\exists w)(17^w - 1 \leq 16 \cdot y \ \& \ 16 \cdot x \leq 17 \cdot (17^w - 1) \ \& \ z = x \cdot 17^w + y).$$

LEMMA 12.4. The formula

$$(\forall x)(\forall w)(\forall v)(17^w - 1 \leq x \ \& \ x \leq 17 \cdot (17^w - 1) \ \& \ 17^v - 1 \leq x \ \& \ x \leq 17 \cdot (17^v - 1) \to w = v)$$

is provable.

PROOF. Let us assume (i) $17^w - 1 \leq x$

(ii) $x \leq 17 \cdot (17^w - 1)$

$$\text{(iii) } 17^{v} - 1 \leq x$$

$$\text{(iv) } x \leq 17 \cdot (17^{v} - 1)$$

and suppose $v < w$. Then we get $v + 1 \leq w$ (by XXX) and thus also $17^{v+1} \leq 17^{w}$ (by XXXV). We further obtain, using the appropriate theorems of §11,

$$17 \cdot (17^{v} - 1 = 17^{v+1} - 17,$$
$$17^{v+1} - 17 < 17^{v+1} - 1,$$
$$17^{v+1} - 1 \leq 17^{w} - 1,$$
$$17^{v+1} - 17 < 17^{w} - 1,$$

which means $17 \cdot (17^{v} - 1) < 17^{w} - 1$. Thus given (i) we obtain $17 \cdot 17^{v-1} < x$, contrary to (iv). This proves $\neg (v < w)$. Similarly we disprove $w < v$ by showing that in this case (iii) and (ii) cannot hold together. By XXXII we conclude $w = v$.

LEMMA 12.5. The formula $(\forall w)((17^{w+1} - 1) - 17 \cdot (17^{w} - 1) = 16)$ is provable.

PROOF. This formula is equivalent to $(\forall w)(16 + 17 \cdot (17^{w} - 1) = 17^{w+1} - 1)$ and therefore to

(*) $\qquad (\forall w)[(16 + 17 \cdot (17^{w} - 1)) + 1 = 17^{w+1}]$.

From XLVI and XII of §11 we obtain $17 \cdot (17^{w} - 1) = 17^{w+1} - 17$. Therefore we can further conclude $17 \cdot (17^{w} - 1) + 17 = (17^{w+1} - 17) + 17 = 17^{w+1}$. But we also get $17 \cdot (17^{w} - 1) + 17 = 17 \cdot (17^{w} - 1) + (16 + 1) = (17 \cdot (17^{w} - 1) + 16) + 1 = (16 + 17 \cdot (17^{w} - 1)) + 1$, and hence (*).

LEMMA 12.6. The formulas $(\forall w)(16 \mid 17^{w} - 1)$ and $(\forall w)(16 \mid 17 \cdot (17^{w} - 1))$ are provable.

PROOF. The second formula can easily be obtained from the first by the appropriate theorems of §11. We prove the first formula by induction. For $w = 1$ the formula reduces to $16 \mid 17^1 - 1$, which is clearly provable. Assume $16 \mid 17^n - 1$. From Lemma 12.5 we know the provability of $17^{n+1} - 1 = 16 + 17 \cdot (17^n - 1)$. Again using §11 we get

$$16 \mid 16,$$
$$16 \mid 17^n - 1, \text{ (inductive assumption)}$$
$$16 \mid 17 \cdot (17^n - 1),$$
$$16 \mid 16 + 17 \cdot (17^n - 1),$$
$$16 \mid 17^{n+1} - 1.$$

LEMMA 12.7. The formula $(\forall x)(\exists w)(17^w - 1 \leq 16 \cdot x \;\&\; 16 \cdot x \leq 17 \cdot (17^w - 1))$ is provable.

PROOF. We prove the formula by induction. For $x = 1$ we obtain $17^1 - 1 \leq 16 \cdot 1$ and $16 \cdot 1 \leq 17 \cdot (17^1 - 1)$. Assume $17^w - 1 \leq 16 \cdot n$ and $16 \cdot n \leq 17 \cdot (17^w - 1)$ for some w. From Lemma 12.6 we know that we can prove the existence of a k for which $17 \cdot (17^w - 1) = 16 \cdot k$. From $16 \cdot n \leq 16 \cdot k$ we obtain $n \leq k$, and from Lemma 12.5 we get $17 \cdot (17^w - 1) + 16 = 17^{w+1} - 1$ and therefore $17^{w+1} - 1 = 16 \cdot k + 16 = 16 \cdot Sk$. We consider the two cases: $n = k$, and $n < k$. $n = k$ gives $Sn = Sk$ and $16 \cdot Sn = 16 \cdot Sk$, from which $16 \cdot Sn = 17^{w+1} - 1$ follows. As $17^{w+1} - 1 \leq 17 \cdot (17^{w+1} - 1)$ is easily obtainable, we get $17^{w+1} - 1 \leq 16 \cdot Sn$ and $16 \cdot Sn \leq 17 \cdot (17^{w+1} - 1)$. On the other hand, $n < k$ yields $Sn \leq k$ and $16 \cdot Sn \leq 16 \cdot k$; we conclude $16 \cdot Sn \leq 17 \cdot (17^w - 1)$. As $16 \cdot n < 16 \cdot Sn$ is provable, so is $17^w - 1 \leq 16 \cdot Sn$, and so is, finally, $17^w - 1 \leq 16 \cdot Sn$ and $16 \cdot Sn \leq 17 \cdot (17^w - 1)$.

Lemmas 12.4 and 12.7 state the provability of the uniqueness and existence of a w such that $17^w - 1 \leq 16 \cdot x$ and $16 \cdot x \leq 17 \cdot (17^w - 1)$; thus we can introduce a new function $y = l(x)$ expressed by

$$17^y \leq 16 \cdot x \;\&\; 16 \cdot x \leq 17 \cdot (17^y - 1).$$

If x and y satisfy the above formula, y will be called <u>the length of x</u> (y is the number of digits in the seventeen-adic representation of x). With this abbreviation, the formula for $x \circ y = z$ becomes

$$x \circ y = z: \quad z = x \cdot 17^{l(y)} + y.$$

§13. <u>More About the Formula Q(x,y)</u>

We recall that the formula Q(x,y) expressing the fact that y is the Gödel number of the numeral of x was

$$Q(x,y): \quad (x = 1 \;\&\; y = 15) \vee (\exists y_1)(17^x = 16 \cdot y_1 + 17 \;\&\; y = 14 \cdot y_1 + 15).$$

LEMMA 13.1. The formula $(\forall x)(\forall y)(\forall z)(Q(x,y) \;\&\; Q(x,z) \rightarrow y = z)$ is provable.

PROOF. First of all, as we can easily obtain $17^1 > 16 \cdot 1 + 17$, the appropriate theorems of §11 give us $(\forall y_1)(\neg\, 17^1 = 16 \cdot y_1 + 17)$. We can conclude $Q(1,y) \rightarrow y = 15$, and hence the uniqueness formula for this case. Let us now assume $\neg\, x = 1$ and $Q(x,y) \;\&\; Q(x,z)$. Thus we are assuming the existence of a y_1 and a y_2 such that

$$17^x = 16 \cdot y_1 + 17,$$
$$y = 14 \cdot y_1 + 15,$$
$$17^x = 16 \cdot y_2 + 17,$$
$$z = 14 \cdot y_2 + 15.$$

This gives us $16 \cdot y_1 + 17 = 16 \cdot y_2 + 17$ from which (using §11) we obtain $y_1 = y_2$, and therefore also $y = z$.

LEMMA 13.2. The formula $(\forall x)(\forall y)(Q(x,y) \to l(y) = x)$ is provable.

PROOF. For $x = 1$ this reduces to $17^1 - 1 \leq 16 \cdot 15 \leq 17 \cdot (17^1 - 1)$, which is easily provable. Let us assume $\neg x = 1$ and $Q(x,y)$, which means

$$17^x = 16 \cdot y_1 + 17 \quad \text{and} \quad y = 14 \cdot y_1 + 15$$

for some y_1. §11 lets us conclude

$$16 \cdot y = 16 \cdot (14 \cdot y_1 + 15) = 16 \cdot 14 \cdot y_1 + 16 \cdot 15 =$$
$$14 \cdot (16 \cdot y_1 + 17) + 2 = 14 \cdot 17^x + 2$$

and

$$17^x - 1 \leq 14 \cdot 17^x + 2.$$

On the other hand, we can also obtain

$$14 \cdot 17^x + 2 = 16 \cdot 17^x - 2 \cdot 17^x + 2,$$
$$16 \cdot 17^x - 2 \cdot 17^x + 2 \leq 16 \cdot 17^x - 17,$$
$$16 \cdot 17^x - 17 \leq 17 \cdot 17^x - 17,$$
$$17 \cdot 17^x - 17 = 17 \cdot (17^x - 1),$$

which finally yields $17^x - 1 \leq 16 \cdot y$ and $16 \cdot y \leq 17 \cdot (17^x - 1)$, i.e. $l(y) = x$.

LEMMA 13.3. The formula $Q(1,15)$ & $(\forall x)(\forall y)(Q(x,y) \to Q(Sx, 14 \circ y))$ is provable.

PROOF. The provability of $Q(1,15)$ is obvious. Let us assume $Q(x,y)$. Thus we assume the existence of a y_1 for which we have

$$17^x = 16 \cdot y_1 + 17,$$
$$y = 14 \cdot y_1 + 15.$$

We want to prove $Q(Sx, 14 \circ y)$, i.e. the existence of a y_2 such that

$$17^{Sx} = 16 \cdot y_2 + 17,$$

$$14 \circ y = 14 \cdot y_2 + 15.$$

By definition we have $14 \circ y = 14 \cdot 17^{l(y)} + y$. From Lemma 13.2 and the appropriate theorems of §11 we get $14 \circ y = 14 \cdot 17^x + y$. Thus we want to prove that for some y_2 we have

(*) $$17^{Sx} = 16 \cdot y_2 + 17$$

(**) $$14 \cdot 17^x + y = 14 \cdot y_2 + 15.$$

Using §11 again, we can obtain

$$16 \cdot (17 \cdot y_1 + 17) + 17 = 16 \cdot 17 \cdot y_1 + 16 \cdot 17 + 17 =$$

$$16 \cdot 17 \cdot y_1 + 17 \cdot 17 = 17 \cdot (16 \cdot y_1 + 17).$$

Together with our assumptions above, this yiel

$$16 \cdot (17 \cdot y_1 + 17) + 17 = 17^x \cdot 17 = 17^{Sx}.$$

Therefore we have proven the existence of a y_2 (namely, $17 \cdot y_1 + 17$), for which (*) holds. We can further prove

$$14 \cdot (17 \cdot y_1 + 17) + 15 = 14 \cdot ((16 \cdot y_1 + y_1) + 17) + 15 =$$

$$14 \cdot (16 \cdot y_1 + 17) + (14 \cdot y_1 + 15)$$

and therefore also

$$14 \cdot (17 \cdot y_1 + 17) + 15 = 14 \cdot 17^x + y,$$

which means that the y_2 we have chosen also fulfills (**).

COROLLARY. The formula $(\forall x)(\exists y)(Q(x,y))$ is provable.

PROOF. This is an immediate consequence of the preceding lemma.

Lemma 13.1 and this Corollary show that both the existence and the uniqueness of a y such that $Q(x,y)$ are provable for all x. Instead of writing $Q(x,y)$ we can therefore write $Q(x) = y$.

LEMMA 13.4. The formula $(\forall x_1)(\forall x_2)(Q(x_1) = Q(x_2) \rightarrow x_1 = x_2)$ is provable.

PROOF. The proof of Lemma 13.1 shows that our claim is indeed true if we assume $x_1 = 1$. Let us assume $\vdash x_1 = 1$ (and therefore $\vdash x_2 = 1$), $y = Q(x_1)$, $y = Q(x_2)$. Thus we have

(i) $17^{x_1} = 16 \cdot y_1 + 17$,

(ii) $y = 14 \cdot y_1 + 15$

for some y_1, and

(iii) $17^{x_2} = 16 \cdot y_2 + 17$,

(iv) $y = 14 \cdot y_2 + 15$

for some y_2. From (ii), (iv) and the theorems of §11 we obtain $y_1 = y_2$. But then (i) and (iii) yield $17^{x_1} = 17^{x_2}$ and therefore $x_1 = x_2$.

LEMMA 13.5. The formula $(\forall x)(\text{Num } Q(x))$ is provable.

PROOF. Immediate, as Num x is shorthand for $(\exists y)(Q(x,y))$.

LEMMA 13.6. The formula $(\forall x)(\text{Num } x \rightarrow \text{Num } 14 \cdot x)$ is provable.

PROOF. Obvious, from Lemma 13.3 and the definition of Num x.

§14. The Functions G_η

Let η be either a term or a formula. If η does not contain any free variables, then G_η will be the Gödel number of η. If η contains k free variables $v_1, \ldots, v_k$, the G_η will be the function assigning to every k-tuple $n_1, \ldots, n_k$ of natural numbers the Gödel number of $\eta(\bar{n}_1, \ldots, \bar{n}_k)$.

(Alternatively, instead of speaking of a separate function G_η for every η, we could speak of a function G having as its domain all pairs (η, ν), where η is either a term or a formula and ν is an infinite sequence of natural numbers. If k is the total number of free variables in η, the value of G on (η, ν) will be the Gödel number of the expression obtained from η by substituting the first k elements of ν for those free variables.)

For every particular η the function G_η is expressible. Indeed, if η does not contain any free variables and c is its Gödel number, then G_η is expressed by the formula $G_\eta = \bar{c}$. If η is a variable v, our formula is $G_\eta = Q(v)$. Furthermore, if τ_1, τ_2 are terms and if G_{τ_1}, G_{τ_2} are expressible, then the formulas $G_{S\tau_1} = 14 \circ G_{\tau_1}$, $G_{(\tau_1+\tau_2)} = 10 \circ G_{\tau_1} \circ 2 \circ G_{\tau_2} \circ 11$, $G_{(\tau_1 \cdot \tau_2)} = 10 \circ G_{\tau_1} \circ 3 \circ G_{\tau_2} \circ 11$, $G_{\tau_1=\tau_2} = G_{\tau_1} \circ 1 \circ G_{\tau_2}$ express the G-functions associated with combinations of τ_1 and τ_2. If now ϕ_1, ϕ_2 are formulas and G_{ϕ_1}, G_{ϕ_2} are expressible, then we get the formulas $G_{\neg\phi_1} = 4 \circ G_{\phi_1}$, $G_{(\phi_1 \vee \phi_2)} = 10 \circ G_{\phi_1} \circ 5 \circ G_{\phi_2} \circ 11$, $G_{(\phi_1 \& \phi_2)} = 10 \circ G_{\phi_1} \circ 6 \circ G_{\phi_2} \circ 11$, $G_{(\phi_1 \to \phi_2)} = 10 \circ G_{\phi_1} \circ 7 \circ G_{\phi_2} \circ 11$ to express the G-functions associated with compound formulas constructed from ϕ_1, ϕ_2.

If v is a free variable of ϕ_1, let $G_{\phi_1 - v}$ be the result of replacing Q(v) by the Gödel number of "v" in the expression on the right side of the equality representing G_{ϕ_1} (e.g. if ϕ_1 is x' = x'', then $G_{\phi_1 - x''}$ will be $Q(x') \circ 1 \circ 12 \circ 13 \circ 13$). We can then complete our description of the formulas to express G_η by noticing that if η is $(\exists v)(\phi_1)$, c is the Gödel number of v and v does not appear free in ϕ_1, then $G_\eta = 10 \circ 8 \circ \bar{c} \circ 11 \circ 10 \circ G_{\phi_1} \circ 11$ expresses G_η. If v does appear free in ϕ_1, then G_η is expressed by $G_\eta = 10 \circ 8 \circ \bar{c} \circ 11 \circ 10 \circ G_{\phi_1 - v} \circ 11$. Analogously if η is the universal quantification of ϕ_1.

We are going to prove that for any formula ψ with one free variable and any formula $F(v_1,\ldots,v_k)$ with k free variables, the formula

$$\text{Sat } \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z)[z = G_{F(v_1,\ldots,v_k)} \to (F(v_1,\ldots,v_k) \equiv \psi(z))]$$

is provable. To do so we will need some preliminary discussion.

§15. Proofs of Some Further Properties of Concatenation

LEMMA 15.1. The formula $(\forall x)(\forall y)(x = y \to x \circ z = y \circ z)$ is provable.

PROOF. Immediate, from the theorems of §11.

LEMMA 15.2. For any two numbers n,m, the sentence $l(\bar{n}) = \bar{m}$ is provable when true and refutable when false.

PROOF. Immediate, from Lemma 12.1 and §11.

LEMMA 15.3. The formula $(\forall x)(\forall y)(\forall z)(z = x \circ y \to l(z) = l(x) + l(y))$ is provable.

PROOF. Assume $z = x \circ y$. The definitions introduced earlier yield

$$z = x \cdot 17^{l(y)} + y,$$

$$17^{l(x)} - 1 \leq 16 \cdot x \text{ and } 16 \cdot x \leq 17 \cdot (17^{l(x)} - 1),$$

$$(*) \qquad 17^{l(y)} - 1 \leq 16 \cdot y \text{ and } 16 \cdot y \leq 17 \cdot (17^{l(y)} - 1).$$

Using XIII, XXXVI and the appropriate theorems concerning multiplication, we can infer

$$(17^{l(x)} - 1) \cdot 17^{l(y)} \leq 16 \cdot x \cdot 17^{l(y)} \text{ and}$$

$$16 \cdot x \cdot 17^{l(y)} \leq 17 \cdot ((17^{l(x)} - 1) \cdot 17^{l(y)}),$$

which, together with Theorems XLVI and XXXIX of §11, give

$$(**) \qquad 17^{l(x)+l(y)} - 17^{l(y)} \leq 16 \cdot x \cdot 17^{l(y)} \text{ and}$$

$$16 \cdot x \cdot 17^{l(y)} \leq 17 \cdot (17^{l(x)+l(y)} - 17^{l(y)}).$$

Adding together the inequalities of (*) and (**), which XXXVII permits us to do, we get

$$(17^{l(x)+l(y)} - 17^{l(y)}) + (17^{l(y)} - 1) \leq 16 \cdot x \cdot 17^{l(y)} + 16 \cdot y$$

and

$$16 \cdot x \cdot 17^{l(y)} + 16 \cdot y \leq 17 \cdot ((17^{l(x)+l(y)}) - 17^{l(y)}) + (17^{l(y)} - 1)),$$

which transforms into

$$17^{l(x)+l(y)} - 1 \leq 16 \cdot z \quad \text{and} \quad 16 \cdot z \leq 17 \cdot (17^{l(x)+l(y)} - 1),$$

i.e. into $l(z) = l(x) + l(y)$.

LEMMA 15.4. The formula $(\forall x)(\forall y)(\forall z)((x \circ y) \circ z = x \circ (y \circ z))$ is provable.

PROOF. The definition of concatenation and the preceding lemma yield $(x \circ y) \circ z = (x \circ y) \cdot 17^{l(z)} + z = (x \cdot 17^{l(y)} + y) \cdot 17^{l(z)} + z =$ $x \cdot 17^{l(y)+l(z)} + y \cdot 17^{l(z)} + z$, as well as $x \circ (y \circ z) = x \cdot 17^{l(y \circ z)} + y \circ z =$ $x \cdot 17^{l(y)+l(z)} + y \cdot 17^{l(z)} + z$, which proves our formula.

LEMMA 15.5. For any three numbers n, m, k, the sentence $\bar{n} \circ \bar{m} = \bar{k}$ is provable when true and refutable when false.

PROOF. The truth of the lemma follows from Lemma 12.1 and the fact (easily established by induction) that $\bar{n} = 17^{\bar{m}}$ is provable when true and refutable when false.

LEMMA 15.6 For any numbers n, m, the sentence $Q(\bar{n}) = \bar{m}$ is provable when true and refutable when false.

PROOF. From Lemma 12.1, the results in §13 and the preceding lemma.

LEMMA 15.7. The formula $(\forall x)(\forall y)(\exists z)(z = x \circ y)$ is provable.

PROOF. Immediate from Lemma 12.7 and the properties of exponentiation.

LEMMA 15.8. For every k, the formula

$$(\forall x_1)(\forall x_2)\ldots(\forall x_k)(\exists z)(x_1 \circ x_2 \circ \ldots \circ x_k = z)$$

is provable.

PROOF. From Lemma 15.7 by induction.

LEMMA 15.9. The formula $(\forall x)(\forall y)(l(x) < l(y) \rightarrow x < y)$ is provable.

PROOF. Using the properties of subtraction and inequality listed in §11, we obtain:

$$17 \cdot (17^{l(x)} - 1) = 17^{l(x)} - 17,$$
$$17^{l(x)+1} - 17 < 17^{l(x)+1} - 1,$$
$$l(x) < l(y) \rightarrow 17^{l(x)+1} \leq 17^{l(y)}.$$

Therefore we can conclude

$$l(x) < l(y) \rightarrow 17 \cdot (17^{l(x)} - 1) < 17^{l(y)} - 1.$$

As, from the definition of length, we have

$$16 \cdot x \leq 17 \cdot (17^{l(x)} - 1) \quad \text{and} \quad 17^{l(y)} \dot{-} 1 \leq 16 \cdot y,$$

we can infer $16 \cdot x < 16 \cdot y$ and therefore, using XXXVI and XI, $x < y$.

LEMMA 15.10. The formula $(\forall x)(\forall y)(\forall z)(x \circ y = x \circ z \rightarrow y = z)$ is provable.

PROOF. Assume $x \circ y = x \circ z$, i.e. $x \cdot 17^{l(y)} + y = x \cdot 17^{l(z)} + z$. Lemmas 15.3 and 15.9 then yield $l(x) + l(y) = l(x) + l(z)$, from which we conclude (using §11) $l(y) = l(z)$. Furthermore, the appropriate theorems of §11 also yield

$$17^{l(y)} = 17^{l(z)},$$
$$x \cdot 17^{l(y)} = x \cdot 17^{l(z)},$$

and therefore

$$x \cdot 17^{l(y)} + y = x \cdot 17^{l(z)} + z \rightarrow y = z.$$

LEMMA 15.11. The formula

$$(\forall x)(\forall y)(\forall z)(\forall w)(x < y \ \&\ l(z) = l(w) \rightarrow x \circ z < y \circ w)$$

is provable.

PROOF. From the facts listed in §11 we can prove

$$17^{l(z)+1} - 17 < 17^{l(z)+1} - 1,$$

and, therefore, $17 \cdot (17^{l(z)} - 1) < 16 \cdot 17^{l(z)} + 17^{l(z)} - 1$. This further implies $16 \cdot x \cdot 17^{l(z)} + 17 \cdot (17^{l(z)} - 1) < 16 \cdot (x + 1) \cdot 17^{l(z)} + (17^{l(z)} - 1)$. Therefore the assumption $x < y$, which implies $x + 1 \leq y$, gives us $16 \cdot x \cdot 17^{l(z)} + 17 \cdot (17^{l(z)} - 1) < 16 \cdot y \cdot 17^{l(z)} + (17^{l(z)} - 1)$. As we have $l(z) = l(w)$, we also get $16 \cdot z \leq 17 \cdot (17^{l(z)} - 1)$ and $17^{l(z)} - 1 \leq 16 \cdot w$. Hence we can prove

$$16 \cdot x \cdot 17^{l(z)} + 16 \cdot z < 16 \cdot y \cdot 17^{l(z)} + 16 \cdot w,$$

which is simply $16 \cdot (x \circ z) < 16 \cdot (y \circ w)$. This implies $x \circ z < y \circ w$.

COROLLARY. The formula

$$(\forall x)(\forall y)(\forall z)(\forall w)(x \circ y = z \circ w \ \&\ l(x) = l(z) \rightarrow x = z \ \&\ y = w)$$

is provable.

PROOF. From Lemma 15.3, the assumptions $x \circ y = z \circ w$ and $l(x) = l(z)$ imply $l(y) = l(w)$. Lemma 15.11 then lets us infer $x = z$ and, as an immediate conclusion, we obtain $y = w$.

PROPOSITION. The formula $(\forall x)(x \leq 17 \equiv l(x) = 1)$ is provable.

PROOF. Immediate from the definition of length and the properties of multiplication and inequality.

LEMMA 15.12. The formula

$$(\forall x)[l(x) = 1 \vee (\exists y)(\exists z)(l(y) = 1 \ \&\ x = y \circ z)]$$

is provable.

PROOF. Assume $l(x) > 1$. From $17^{l(x)} - 1 \leq 16 \cdot x \leq 17 \cdot (17^{l(x)} - 1)$ we can conclude the existence of a w such that

$$(*) \qquad w \leq 16 \;\&\; w \cdot (17^{l(x)} - 1) \leq 16 \cdot x \leq Sw \cdot (17^{l(x)} - 1).$$

According to the above Proposition, the first conjunct implies $l(w) = 1$. Let us set $z = x - w \cdot 17^{l(x)-1}$. Using the appropriate theorems of §11 and (*) above, we can show

$$w \cdot (17^{l(x)} - 1) - 16 \cdot w \cdot 17^{l(x)-1} \leq 16 \cdot z$$

and

$$16 \cdot z \leq Sw \cdot (17^{l(x)} - 1) - 16 \cdot w \cdot 17^{l(x)-1}.$$

As we have $1 \leq w$ and $w \leq 16$, we obtain

$$(17^{l(x)} - 1) - 16 \cdot 17^{l(x)-1} \leq 16 \cdot z$$

and

$$16 \cdot z \leq 17 \cdot (17^{l(x)} - 1) - 16 \cdot 17 \cdot 17^{l(x)-1},$$

which reduces to $17^{l(x)-1} - 1 \leq 16 \cdot z$ and $16 \cdot z \leq 17 \cdot (17^{l(x)-1} - 1)$. Therefore we get $l(z) = l(x) - 1$ and, as we also have $x = w \cdot 17^{l(x)-1} + z$, we can conclude $x = w \circ z$.

LEMMA 15.13. The formula

$$(\forall x)(\forall y)(\forall z)(\forall w)(x \circ y = z \circ w \;\&\; l(x) \leq l(z) \rightarrow xBz)$$

is provable.

PROOF. We perform induction on $l(x)$. First assume $l(x) = 1$, $x \circ y = z \circ w$ and $l(x) \leq l(z)$. From Lemma 15.12, we can prove the existence of a z_1 of length 1 such that for some z_2, $z = z_1 \circ z_2$. Using Lemma 15.1 we obtain $z \circ w = z_1 \circ z_2 \circ w$ and $x \circ y = z_1 \circ z_2 \circ w$. As we have $l(x) = l(z_1)$, the Corollary after Lemma 15.11 lets us conclude the provability of $x = z_1$ and therefore of $x \circ z_2 = z$, i.e. of xBz.

We now assume that our formula is provable whenever $l(x) = n$. Take $x \circ y = z \circ w$, $l(x) \leq l(z)$ and $l(x) = n + 1$. It follows from Lemma 15.12 and the preceding part of the present proof that we can prove the existence of a y of length 1 such that $x = u \circ x_1$ and $z = u \circ z_1$ for some x_1, z_1 for which we also have $l(x_1) = n - 1$, $l(z_1) = l(z) - 1 \leq n - 1$. Thus we obtain $u \circ x_1 \circ y = u \circ z_1 \circ w$ and from Lemma 15.10 follows the provability of $x_1 \circ y = z_1 \circ w$. From our inductive assumption we can conclude $x_1 B z_1$, which gives us xBz.

LEMMA 15.14. The formula

$$(\forall x)(\forall y)(\forall z)(\forall w)(x \circ y = z \circ w \ \& \ l(y) \leq l(w) \rightarrow yEw)$$

is provable.

PROOF. Analogous to the proof of Lemma 15.13.

LEMMA 15.15. The formula $(\forall x)(\forall y)(\forall z)(xPy \ \& \ yPz \rightarrow xPz)$ is provable.

PROOF. Immediate.

LEMMA 15.16. The formula

$$(\forall x)(\forall y)(\forall z)[zPx \circ y \rightarrow zPx \vee zPy \vee (\exists w)(\exists u)(z = w \circ u \ \& \ wEx \ \& \ uBy)]$$

is provable.

PROOF. Immediate.

COROLLARY. The formula $(\forall x)(\forall y)(\forall z)(l(z) = 1 \ \& \ zPx \circ y \rightarrow zPx \vee zPy)$ is provable.

PROOF. This is an immediate consequence of Lemmas 15.16 and 15.3.

LEMMA 15.17. The formula $(\forall x)(\neg\, 1PQ(x))$ is provable.

PROOF. By induction. As $l(1) = 1$, $l(15) = 1$, $\neg\, 1 = 15$ are all provable, Lemma 15.3 yields $\vdash 1P15$, i.e. $\vdash 1PQ(1)$. Let us assume $\vdash 1PQ(n)$. We want to obtain $\vdash 1PQ(Sn)$, which is equivalent to $\vdash 1P14 \circ Q(n)$ (see §12). Again, as we can prove $\vdash 1P14$, our inductive assumption together with the Corollary after Lemma 15.16 yield the desired conclusion.

LEMMA 15.18. Let a be any number of length n and let $a_1, a_2, \ldots, a_k$ be all its different parts. Then the formula

$$(\forall x)(xP\bar{a} \equiv x = \bar{a}_1 \vee x = \bar{a}_2 \vee \ldots \vee x = \bar{a}_k)$$

is provable.

PROOF. Among the a_j's $(j = 1,\ldots,k)$, let $a^i_1,\ldots,a^i_{k_i}$ $(i = 1,\ldots,n)$ be all those parts of a whose length is i, in the order of appearance. The formula $l(\bar{a}) = \bar{n}$ is provable (Lemma 15.2) and so is $(\forall x)(xP\bar{a} \to l(x) \leq l(\bar{a}))$ (Lemma 15.3 and the appropriate theorems of §11). Therefore from Lemma 12.2 we can conclude the provability of

$$(\forall x)(xP\bar{a} \to l(x) = 1 \vee l(x) = 2 \vee \ldots \vee l(x) = \bar{n}).$$

Also, from the definition of $xP\bar{a}$ we obtain

$$(*) \qquad (\forall x)[xP\bar{a} \equiv x = \bar{a} \vee (\exists y)(\exists z)(x \circ y = \bar{a} \vee z \circ x = \bar{a} \vee z \circ x \circ y = \bar{a})].$$

Using the Corollary after Lemma 15.11 and the fact that $l(\bar{a}^i_j) = \bar{i}$ is provable for every $i \leq n$ and every $j \leq k_i$, we see that the formula

$$(\forall x)(\forall y)[x \circ y = \bar{a} \to ((l(x) = 1 \to x = \bar{a}^1_1) \;\&\; (l(x) = 2 \to x = \bar{a}^2_1) \;\& \ldots \&\; (l(x) = \bar{n} \to x = \bar{a}^n_1))]$$

is provable. By the same token we obtain the provability of

$$(\forall x)(\forall z)[z \circ x = \bar{a} \to ((l(x) = 1 \to x = \bar{a}^1_{k_1}) \;\&\; (l(x) = 2 \to x = \bar{a}^2_{k_2}) \;\& \ldots \&\; (l(x) = \bar{n} \to x = \bar{a}^n_{k_n}))].$$

Similarly we can prove

$$(\forall x)(\forall y)(\forall z)(z \circ x \circ y = \bar{a} \to l(z) = 1 \vee l(z) = 2 \vee \ldots \vee l(z) = \overline{n-2})$$

and from there derive the formula expressing the fact that if x constitutes a middle part of a, then it must be equal to some a^i_j ($j = 2,\ldots,k_{i-1}$, $i = 1,\ldots,n-2$). Therefore from (*) we obtain the formula

$$(\forall x)(xP\bar{a} \to x = \bar{a}_1 \vee x = \bar{a}_2 \vee \ldots \vee x = \bar{a}_k).$$

On the other hand from Lemma 15.5 we see that the sentences $\bar{a}_1P\bar{a}$, $\bar{a}_2P\bar{a},\ldots,\bar{a}_kP\bar{a}$ are all provable; therefore, so is

$$(\forall x)(x = \bar{a}_1 \vee x = \bar{a}_2 \vee \ldots \vee x = \bar{a}_k \to xP\bar{a}).$$

COROLLARY. For any numbers n, m, the sentence $\bar{n}P\bar{m}$ is provable when true and refutable when false.

PROOF. When $l(m) < l(n)$ then we can so prove and the refutability of $\bar{n}P\bar{m}$ follows from Lemma 12.4. When $l(m) \geq l(n)$, our claim follows from Lemma 15.12 and the fact that $\bar{n} = \bar{m}$ is provable when true and refutable when false (Lemma 12.1).

LEMMA 15.19. Let F(v) be any formula for which $(\forall v)(F(v) \to \neg\, 1Pv)$ is provable and let $v_1,\ldots,v_k$ be any k variables. Let C be of the form $\bar{n}_1 \circ v_1 \circ \bar{n}_2 \circ \ldots \circ \bar{n}_k \circ v_k \circ \bar{n}_{k+1}$, where $n_1, n_2,\ldots, n_{k+1}$ are any natural numbers whose seventeen-adic representations do not contain $1 \circ 1$ and such that 1 does not start the seventeen-adic representation of n_1 or end that of n_{k+1}. Then the formula

$$(\forall x)(\forall v_1)(\forall v_2)\ldots(\forall v_k)(1 \circ 1 \circ x \circ 1 \circ 1P1 \circ 1 \circ C \circ 1 \circ 1 \equiv x = C)$$

is provable.

PROOF. Obviously $x = C \to 1 \circ 1 \circ x \circ 1 \circ 1P1 \circ 1 \circ C \circ 1 \circ 1$ is provable. Let us assume $1 \circ 1 \circ x \circ 1 \circ 1P1 \circ 1 \circ C \circ 1 \circ 1$; by definition this implies $1 \circ 1 \circ x \circ 1 \circ 1 = 1 \circ 1 \circ C \circ 1 \circ 1 \vee (\exists y)(\exists z)(1 \circ 1 \circ x \circ 1 \circ 1 \circ y = 1 \circ 1 \circ C \circ 1 \circ 1 \vee z \circ 1 \circ 1 \circ x \circ 1 \circ 1 = 1 \circ 1 \circ C \circ 1 \circ 1 \vee z \circ 1 \circ 1 \circ x \circ 1 \circ 1 \circ y = 1 \circ 1 \circ C \circ 1 \circ 1\ )$.

From Lemma 15.12 and the Corollary to Lemma 15.11 it follows that if we assume $z\circ 1\circ 1\circ x\circ 1\circ 1 = 1\circ 1\circ C\circ 1\circ 1$ or $z\circ 1\circ 1\circ x\circ 1\circ 1\circ y = 1\circ 1\circ C\circ 1\circ 1$, then we can prove that either $z = 1$ or else there exists a z_1 such that $z = 1\circ z_1$. $z = 1$ yields $1\circ 1\circ x\circ 1\circ 1 = 1\circ C\circ 1\circ 1 \vee 1\circ 1\circ x\circ 1\circ 1\circ y = 1\circ C\circ 1\circ 1$, and therefore $1\circ x\circ 1\circ 1 = C\circ 1\circ 1 \vee 1\circ x\circ 1\circ 1\circ y = C\circ 1\circ 1$, contradicting $\vdash 1B\bar{n}_1$, which we assumed to be true (and therefore provable, by the proof of Lemma 15.12). $z = 1\circ z_1$ yields $z_1\circ 1\circ 1\circ x\circ 1\circ 1 = 1\circ C\circ 1\circ 1 \vee z_1\circ 1\circ 1\circ x\circ 1\circ 1\circ y = 1\circ C\circ 1\circ 1$, which again gives us either $z_1 = 1$ (which we rule out as before) or the existence of a z_2 for which $z_1 = 1\circ z_2$, and thus $z_2\circ 1\circ 1\circ x\circ 1\circ 1 = C\circ 1\circ 1 \vee z_2\circ 1\circ 1\circ x\circ 1\circ 1\circ y = C\circ 1\circ 1$. Both disjuncts yield $1\circ 1PC$, contradicting $\vdash 1\circ 1PC$ whose provability follows from our assumptions. In an analogous manner we conclude that $1\circ 1\circ x\circ 1\circ 1\circ y = 1\circ 1\circ C\circ 1\circ 1$ leads to a contradiction, thus obtaining $1\circ 1\circ x\circ 1\circ 1 = 1\circ 1\circ C\circ 1\circ 1$, which yields $x = y$.

LEMMA 15.20. Let $F(v)$ be a formula for which $(\forall v)(F(v) \rightarrow \vdash 1Pv)$ is provable, and let $v_1,\dots, v_k$ be any k variables. For $i = 1,\dots, l$, let C_i be of the form $\bar{n}_{i_1}\circ v_1\circ \bar{n}_{i_2}\circ \dots \circ \bar{n}_{i_k}\circ v_k\circ \bar{n}_{i_{k+1}}$, where $n_{i_1},\dots, n_{i_{k+1}}$ are any natural numbers whose seventeen-adic representations do not contain $1\circ 1$ and such that 1 does not start the seventeen-adic representation of n_{i_1} or end that of $n_{i_{k+1}}$. Then the formula

$$(\forall v_1)(\forall v_2)\dots(\forall v_k)(\forall x)[\vdash 1\circ 1Px \rightarrow$$
$$1\circ 1\circ x\circ 1\circ 1P1\circ 1\circ C_1\circ 1\circ 1\circ C_2\circ \dots \circ 1\circ 1\circ C_l\circ 1\circ 1 \equiv$$
$$x = C_1 \vee x = C_2 \vee \dots \vee x = C_l)]$$

is provable.

PROOF. Let us assume $\vdash 1\circ 1Px$. Obviously $x = C_1 \vee x = C_2 \vee \dots \vee x = C_l$

provably implies $1 \circ 1 \circ x \circ 1 \circ 1P1 \circ 1 \circ C_1 \circ 1 \circ 1 \circ C_2 \circ \ldots \circ 1 \circ 1 \circ C_l \circ 1 \circ 1$. Also, if $l = 1$, our claim follows from Lemma 15.19. Suppose that our claim holds true for $l - 1$ and let us assume $1 \circ 1 \circ x \circ 1 \circ 1P1 \circ 1 \circ C_1 \circ 1 \circ 1 \circ C_2 \circ \ldots \circ 1 \circ 1 \circ C_l \circ 1 \circ 1$. By Lemma 15.16 we can obtain

$$1 \circ 1 \circ x \circ 1 \circ 1P1 \circ 1 \circ C_1 \circ 1 \circ 1 \circ C_2 \circ \ldots \circ 1 \circ 1 \circ C_{l-1} \vee$$
$$1 \circ 1 \circ x \circ 1 \circ 1P1 \circ 1 \circ C_1 \circ 1 \circ 1 \vee (\exists w)(\exists u)(1 \circ 1 \circ x \circ 1 \circ 1 = w \circ u \ \&$$
$$wE1 \circ 1 \circ C_1 \circ 1 \circ 1 \circ C_2 \circ \ldots \circ 1 \circ 1 \circ C_{l-1} \ \& \ uB1 \circ 1 \circ C_l \circ 1 \circ 1).$$

According to our inductive assumption and to Lemma 15.15, the first disjunct yields $x = C_1 \vee x = C_2 \vee \ldots \vee x = C_{l-1}$; and by Lemma 15.19 we can prove that the second disjunct is equivalent to $x = C_1$. Furthermore, given $1 \circ 1 \circ x \circ 1 \circ 1 = w \circ u \ \& \ wE1 \circ 1 \circ C_1 \circ 1 \circ 1 \circ C_2 \circ \ldots \circ 1 \circ 1 \circ C_{l-1} \ \& \ uB1 \circ 1 \circ C_l \circ 1 \circ 1$, as we have assumed $\vdash 1 \circ 1Px$ and the provability of $\vdash 1BC_l$, we obtain $u = 1 \circ 1$. This yields $1 \circ 1 \circ xE1 \circ 1 \circ C_1 \circ 1 \circ 1 \circ C_2 \circ \ldots \circ 1 \circ 1 \circ C_{l-1}$, which, again together with $\vdash 1 \circ 1Px$, $\vdash 1EC_{l-2}$ and $\vdash 1BC_{l-1}$, lets us obtain $x = C_{l-1}$.

In the next chapter we present some facts which will directly lead to the proof of the theorem described at the end of §14 – the object-language expression of the fact that a number belongs to a saturated set if and only if and only if it is the Gödel number of a true sentence.

§16. Preliminaries

LEMMA 16.1. For any term τ with k variables $v_1, \ldots, v_k$, the formula $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\exists w)(\tau = w)$ is provable.

PROOF. Immediately follows from Theorem II of §11.

LEMMA 16.2. For any three terms τ_1, τ_2, τ_3 whose variables are v_1, $\ldots, v_k$, the formula $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall w_3)[\tau_1 + \tau_2 = \tau_3 \equiv (\tau_1 = w_1 \;\&\; \tau_2 = w_2 \;\&\; \tau_3 = w_3 \rightarrow w_1 + w_2 = w_3)]$ is provable.

PROOF. Let us first assume $\tau_1 + \tau_2 = \tau_3$, $\tau_1 = w_1$, $\tau_2 = w_2$ and $\tau_3 = w_3$. Using the appropriate theorems of §11 we obtain

$$w_1 + w_2 = w_1 + \tau_2 = \tau_1 + \tau_2 = \tau_3 = w_3$$

and thus $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall w_3)[\tau_1 + \tau_2 = \tau_3 \rightarrow (\tau_1 = w_1 \;\&\; \tau_2 = w_2 \;\&\; \tau_3 = w_3 \rightarrow w_1 + w_2 = w_3)]$ is provable. On the other hand, assuming $(\forall w_1)(\forall w_2)(\forall w_3)(\tau_1 = w_1 \;\&\; \tau_2 = w_2 \;\&\; \tau_3 = w_3 \rightarrow w_1 + w_2 = w_3)$, we can conclude, using II, $\tau_1 + \tau_2 = \tau_3$; this completes the proof of our formula.

LEMMA 16.3. For any three terms τ_1, τ_2, τ_3 whose variables are v_1, $\ldots, v_k$, the formula $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall w_3)[\tau_1 \cdot \tau_2 = \tau_3 \equiv (\tau_1 = w_1 \;\&\; \tau_2 = w_2 \;\&\; \tau_3 = w_3 \rightarrow w_1 \cdot w_2 = w_3)]$ is provable.

PROOF. Analogous to that of Lemma 16.2.

LEMMA 16.4. For any two terms τ_1, τ_2 whose variables are $v_1, \ldots, v_k$, the formula $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)[S\tau_1 = \tau_2 \equiv (\tau_1 = w_1 \;\&\; \tau_2 = w_2 \rightarrow Sw_1 = w_2)]$ is provable.

PROOF. Analogous to that of Lemma 16.2.

LEMMA 16.5. For every formula F with free variables $v_1, v_2, \ldots, v_k$, the formula $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\exists z_1)(z_1 = G_F)$ is provable.

PROOF. Let j be the number of symbols appearing in F in addition to the k free variables. The formula whose provability we claim is of the form $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\exists z_1)(z_1 = p_1 \circ p_2 \circ \ldots \circ p_{j+k})$, where some of the p's are of the form $Q(v_i)$, $i = 1, \ldots, k$, and the remaining ones are the Gödel numerals of the other j symbols appearing in F. Therefore the provability of our formula follows from that of $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\exists w_1)(\exists w_2)\ldots(\exists w_k)$ $(Qv_1 = w_1 \ \&\ Qv_2 = w_2 \ \&\ldots\&\ Qv_k = w_k)$ (see Corollary after Lemma 13.3) and of $(\forall x_1)(\forall x_2)\ldots(\forall x_{k+j})(\exists z_1)(z_1 = x_1\circ x_2\circ \ldots \circ x_{k+j})$ (Lemma 15.8).

LEMMA 16.6. Let a be the Gödel number of the variable v_1. For any term or formula R with k free variables $v_1,\ldots,v_k$, the formula

(*) $$(\forall v_2)(\forall v_3)\ldots(\forall v_k)(\forall z)(\forall z_1)(\forall z_2)[z = G_{R-v_1} \rightarrow (\forall v_1)(\mathrm{Subst}(z,a,Qv_1,z_1) \ \&\ \mathrm{Subst}(z,a,Qv_1,z_2) \rightarrow z_1 = z_2)]$$

is provable.

PROOF. By induction on the length of R. If R is either a variable or the numeral 1 and b is any of the numbers 1, 2, 3, 4, 5, 6, 7, 9, 14 (call them "expression builders"), we can prove $\vdash \bar{b}PG_{R-v_1}$. Therefore we can also prove a formula expressing the fact that any sequence number which is of the form specified in the definition of $\mathrm{Subst}(z,a,Qv_1,y)$ and ends with the number of a pair whose first member is R must have as its only element either $G_{R-v_1}\circ 2\circ 2\circ Qv_1$ – if R is v_1 – or $G_{R-v_1}\circ 2\circ 2\circ G_{R-v_1}$, otherwise.

If R is a numeral different from 1 the proof of (*) will be obtained by formalizing the following inductive argument: Let us assume that our claim (uniqueness of substitution) holds for the predecessor of R. The only "expression builder" which is part of G_{R-v_1} is 14. Therefore the sequence number whose existence is required by Subst either has $G_{R-v_1}\circ 2\circ 2\circ G_{R-v_1}$ as its only element, or else the pair number $G_{R-v_1}\circ 2\circ 2\circ s$ ending it has been obtained from an earlier pair number in the sequence by preceding both its "elements" by 14. But then the first "element" of that earlier pair number must have been the number of the predecessor of R; hence our claim follows from the inductive assumption.

Suppose now that R is a composite expression and that we have established our claim for all terms and formulas with fewer logical constants than R contains. We will outline the proof using a concrete example; let us say R is $(v_1 = 2 \vee x' + 2 = 3)$, where v_1 is different from x'. First of all, we can obviously prove a formula expressing the fact that the first "element" of any pair number in any sequence number of the form specified by Subst must be part of the first "element" of any pair occurring later in that sequence. In particular, the first pair in the sequence described by Subst(G_{R-v_1},a,Qv_1,y) must have as its first element a variable or a numeral which is part of R. Thus for our specific R we can prove that the first element of that sequence number must be one of $a \circ 2 \circ 2 \circ Qv_1$, $15 \circ 2 \circ 2 \circ 15$, $14 \circ 15 \circ 2 \circ 2 \circ 15$, $12 \circ 13 \circ 2 \circ 2 \circ 12 \circ 13$ and $14 \circ 14 \circ 15 \circ 2 \circ 2 \circ 14 \circ 14 \circ 15$ and that any of these may occur in the sequence at any point. By the same token we can prove that the only expression builders used in the sequence are 1, 5, 2 and 14. Therefore there is only a finite number of sequence numbers of the kind described in Subst that we can build using the elements we have just listed, if the first "element" of the last pair number in the sequence number cannot exceed G_{R-v_1} in length. After listing all those sequence numbers we find out that only the one whose penultimate two elements are the pair encodings beginning with the numbers of $v_1 = 2$ and $x' + 2 = 3$ ends with a pair number beginning with G_{R-v_1}. That our uniqueness formula for G_{R-v_1} can be inferred follows from our inductive assumption of that formula's provability for terms and formulas with fewer logical constants.

LEMMA 16.7. Let a be the Gödel number of the variable v_1. For any term or formula R with k free variables $v_1, \ldots, v_k$, the formula

(*) $(\forall v_2)\ldots(\forall v_k)(\forall z)(\forall z_1)[z = G_{R-v_1} \rightarrow (\forall v_1)(z_1 = G_R \rightarrow \mathrm{Subst}(z,a,Qv_1,z_1))]$

is provable.

PROOF. By induction on the length of R. First let R be a numeral $\bar{n}$. Let m be $1\circ 1\circ Q(n)\circ 2\circ 2\circ Q(n)\circ 1\circ 1$. From Lemma 15.5 and the Corollary after Lemma 15.12 we conclude that $1\circ 1B\bar{m}$, $1\circ 1E\bar{m}$, $\vdash 1\circ 1 = \bar{m}$ and $\vdash 1\circ 1\circ 1P\bar{m}$ are all provable; thus Seq $\bar{m}$ is provable. As a consequence of Lemmas 15.20 and 15.16 we also obtain the provability of $(\forall x)(x \varepsilon \bar{m} \equiv x = Q(\bar{n})\circ 2\circ 2\circ Q(\bar{n}))$. As for this particular R both G_{R-v_1} and G_R are equal to Q(n), the above remarks together with the provability of Num $Q(\bar{n})$ establish the provability of (*) for this R.

We proceed analogously if R is a variable different from v_1, with Gödel number b (we let m be $1\circ 1\circ b\circ 2\circ 2\circ b\circ 1\circ 1$), when R is v_1 (let m be $1\circ 1\circ a\circ 2\circ 2\circ Qv_1\circ 1\circ 1$) or when R is a quantifier formula where the quantification is with respect to a variable different from v_1 (let m be $1\circ 1\circ G_{R-v_1}\circ 2\circ 2\circ G_{R-v_1}\circ 1\circ 1$).

Suppose now that we can prove (*) for some two expressions R_1, R_2 (terms or formulas) by actually exhibiting, as we did above, two sequence numbers of the kind described by Subst whose last elements are, respectively, the "encodings" of the pairs $(G_{R_1-v_1}, G_{R_1})$ and $(G_{R_2-v_1}, G_{R_2})$ and by proving that these sequences are indeed of the kind desired. It is clear, then, that by precisely the same methods we can prove that the sequence number obtained by the following procedure is also of the kind desired:

delete the $1 \circ 1$ at the end of one sequence number, adjoin the other one (by means of $\circ$) at the end and to the result adjoin the encoding, followed by $1 \circ 1$, of any one of the pairs (G_{R-v_1}, G_R) in which R has been built up from R_1, R_2 by any one of the "term building" or "formula building" operations.

This is the induction step which completes our proof.

LEMMA 16.8. For any formula F with k free variables $v_1, \ldots, v_k$, the formula $(\forall v_2)\ldots(\forall v_k)(\forall z)(z_1)[z = G_{(\forall v_1)F} \vee z = G_{(\exists v_1)F} \to (\forall v_1)(\mathrm{Inst}_1(z, z_1, Qv_1) \equiv z_1 = G_F)]$ is provable.

PROOF. Immediate from the definition of Inst_1 and the two preceding lemmas.

§17. Main Theorem on Saturated Sets

THEOREM 17.1. Let ψ be any formula with one free variable, and let F be a formula with k free variables $v_1, \ldots v_k$. Then the formula

$$\mathrm{Sat}\,\psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z)[z = G_F \to (F(v_1, \ldots, v_k) \equiv \psi(z))]$$

is provable.

PROOF. A. We first establish our claim for an atomic formula F of the form $v_1 = v_2$; G_F is then equal to $Q(v_1) \circ 1 \circ Q(v_2)$. In view of the Identity Input clause of $\mathrm{Sat}\,\psi$ we can prove

$$\mathrm{Sat}\,\psi \to (\forall v_1)(\forall v_2)(\forall z)\{\mathrm{Num}\ Qv_1\ \&\ \mathrm{Num}\ Qv_2 \to [z = Qv_1 \circ 1 \circ Qv_2 \to (\psi(z) \equiv Q(v_1) = Q(v_2))]\}.$$

Therefore, by Lemma 13.5 we can obtain

$$\mathrm{Sat}\,\psi \to (\forall v_1)(\forall v_2)(\forall z)[z = Qv_1 \circ 1 \circ Qv_2 \to (\psi(z) \equiv Q(v_1) = Q(v_2))].$$

According to Lemma 13.4, the formula $(\forall v_1)(\forall v_2)(Qv_1 = Qv_2 \rightarrow v_1 = v_2)$ is provable; therefore, so is

$$\text{Sat } \psi \rightarrow (\forall v_1)(\forall v_2)(\forall z)[z = Qv_1 \circ 1 \circ Qv_2 \rightarrow (\psi(z) \equiv v_1 = v_2)],$$

which is what we wanted to show.

B. We let F be an atomic formula of the form $(v_1 + v_2) = v_3$; that makes G_F equal to $10 \circ Qv_1 \circ 2 \circ Qv_2 \circ 11 \circ 1 \circ Qv_3$. As Sat ψ contains the Addition Input clause, one can prove

(B1) $$\text{Sat } \psi \rightarrow (\forall v_1)(\forall v_2)(\forall v_3)(\forall z)\{\text{Num } Qv_1 \ \& \ \text{Num } Qv_2 \ \& \ \text{Num } Qv_3 \rightarrow [z = 10 \circ Qv_1 \circ 2 \circ Qv_2 \circ 11 \circ 1 \circ Qv_3 \rightarrow (\psi(z) \equiv (\exists x_1)(\exists x_2)(\exists x_3) (Qv_1 = Qx_1 \ \& \ Qv_2 = Qx_2 \ \& \ Qv_3 = Qx_3 \ \& \ x_3 = x_1 + x_2))] .$$

From Lemma 13.4 follows the provability of

$$(\forall v_1)(\forall v_2)(\forall v_3)[(\exists x_1)(\exists x_2)(\exists x_3)(Qv_1 = Qx_1 \ \& \ Qv_2 = Qx_2 \ \& \ Qv_3 = Qx_3 \ \& \ x_3 = x_1 + x_2) \equiv v_3 = v_1 + v_2)].$$

Therefore, as a consequence of Lemma 13.5 and of (B1) we can obtain

$$\text{Sat } \psi \rightarrow (\forall v_1)(\forall v_2)(\forall v_3)(\forall z)[z = 10 \circ Qv_1 \circ 2 \circ Qv_2 \circ 11 \circ 1 \circ Qv_3 \rightarrow (\psi(z) \equiv v_3 = v_1 + v_2)],$$

which was our claim.

C. The proof proceeds analogously if F is of the form $(v_1 \cdot v_2) = v_3$. We use the Multiplication Input clause of Sat ψ.

D. Let F be of the form $Sv_1 = v_2$. In this case G_F is $14 \circ Qv_1 \circ 1 \circ Qv_2$. As Sat ψ contains the Identity Input clause, the following is provable:

(D1) $$\text{Sat } \psi \rightarrow (\forall v_1)(\forall v_2)(\forall z)[\text{Num } 14 \circ Qv_1 \ \& \ \text{Num } Qv_2 \rightarrow z = 14 \circ Qv_1 \circ 1 \circ Qv_2 \rightarrow (\psi(z) \equiv 14 \circ Qv_1 = Qv_2)].$$

Lemmas 13.3 and 13.4 give us the provability of

$$(\forall v_1)(\forall v_2)(14 \circ Qv_1 = Qv_2 \equiv Sv_1 = v_2).$$

Hence from (D1), using Lemmas 13.5 and 13.6, we get

$$\text{Sat}\ \psi \to (\forall v_1)(\forall v_2)(\forall z)[z = 14 \circ Qv_1 \circ 1 \circ Qv_2 \to (\psi(z) \equiv Sv_1 = v_2)],$$

which is what we were aiming for.

Let us now assume that our claim holds true for atomic formulas with fewer than n function symbols. Let F be an atomic formula with n function symbols and k free variables.

E. F is of the form $(\tau_1 + \tau_2) = \tau_3$. It follows from our inductive assumption that the formula

(E1) $$\text{Sat}\ \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall w_3)(\forall z_1)(\forall z_2)(\forall z_3)$$
$$[z_1 = G_{\tau_1} \circ 1 \circ Qw_1\ \&\ z_2 = G_{\tau_2} \circ 1 \circ Qw_2\ \&\ z_3 = G_{\tau_3} \circ 1 \circ Qw_3 \to$$
$$((\psi(z_1) \equiv \tau_1 = w_1)\ \&\ (\psi(z_2) \equiv \tau_2 = w_2)\ \&\ (\psi(z_3) \equiv \tau_3 = w_3))]$$

is provable; it also follows from part B above that we can prove

(E2) $$\text{Sat}\ \psi \to (\forall w_1)(\forall w_2)(\forall w_3)(\forall z_4)[z_4 = 10 \circ Qw_1 \circ 2 \circ Qw_2 \circ 11 \circ 1 \circ Qw_3 \to$$
$$(\psi(z_4) \equiv (w_1 + w_2) = w_3)].$$

From Lemma 16.2 follows the provability of

(E3) $$(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall w_3)\{[\tau_1 + \tau_2 = \tau_3 \equiv (\tau_1 = w_1\ \&$$
$$\tau_2 = w_2\ \&\ \tau_3 = w_3 \to w_1 + w_2 = w_3)]\ \&\ [\tau_1 = w_1\ \&\ \tau_2 = w_2\ \&\ \tau_3 = w_3$$
$$\to (\tau_1 + \tau_2 = \tau_3 \equiv w_1 + w_2 = w_3)]\}.$$

The provability of the last three formulas implies the provability of

$$\text{Sat}\ \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall w_3)(\forall z_1)(\forall z_2)(\forall z_3)(\forall z_4)(\forall z)$$
$$\{z_1 = G_{\tau_1} \circ 1 \circ Qw_1\ \&\ z_2 = G_{\tau_2} \circ 1 \circ Qw_2\ \&\ z_3 = G_{\tau_3} \circ 1 \circ Qw_3\ \&$$
$$z_4 = 10 \circ Qw_1 \circ 2 \circ Qw_2 \circ 11 \circ 1 \circ Qw_3\ \&\ z = 10 \circ G_{\tau_1} \circ 2 \circ G_{\tau_2} \circ 11 \circ 1 \circ G_{\tau_3}$$
$$\to [\tau_1 + \tau_2 = \tau_3 \equiv (\tau_1 = w_1\ \&\ \tau_2 = w_2\ \&\ \tau_3 = w_3 \to \psi(z_4))]\ \&$$
$$[\tau_1 = w_1\ \&\ \tau_2 = w_2\ \&\ \tau_3 = w_3 \to (\psi(z_4) \equiv \psi(z))]\},$$

which means that the following is provable as well:

(E4) $\quad$ $\text{Sat}\ \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall w_3)(\forall z)$
$[z = 10 \circ G_{\tau_1} \circ 2 \circ G_{\tau_2} \circ 11 \circ 1 \circ G_{\tau_3} \to (\tau_1 + \tau_2 = \tau_3 \equiv (\tau_1 = w_1\ \&$
$\tau_2 = w_2\ \&\ \tau_3 = w_3 \to \psi(z)))]$.

From Lemma 16.1 we conclude the provability of

$$(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\exists w_1)(\exists w_2)(\exists w_3)(\tau_1 = w_1\ \&\ \tau_2 = w_2\ \&\ \tau_3 = w_3)$$

which, together with (E4), yields

$$\text{Sat}\ \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z)[z = 10 \circ G_{\tau_1} \circ 2 \circ G_{\tau_2} \circ 11 \circ 1 \circ G_{\tau_3} \to (\psi(z) \equiv \tau_1 + \tau_2 = \tau_3)],$$

which concludes our proof.

F. For F of the form $(\tau_1 \cdot \tau_2) = \tau_3$ the proof is analogous; we use Lemma 16.3 and part C above in place of Lemma 16.2 and part B.

G. Let F be of the form $S\tau_1 = \tau_2$. The provability of the following is given by our inductive assumption:

(G1) $\quad$ $\text{Sat}\ \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall z_1)(\forall z_2)[z_1 = G_{\tau_1} \circ 1 \circ Qw_1$
$\&\ z_2 = G_{\tau_2} \circ 1 \circ Qw_2 \to (\psi(z_1) \equiv \tau_1 = w_1)\ \&\ (\psi(z_2) \equiv \tau_2 = w_2)]$.

We also know from part D above that we can prove

(G2) $\quad$ $\text{Sat}\ \psi \to (\forall w_1)(\forall w_2)(\forall z_3)[z_3 = 14 \circ Qw_1 \circ 1 \circ Qw_2 \to (\psi(z_3) \equiv Sw_1 = w_2)]$.

Furthermore, Lemma 16.4 assures the provability of

$$(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)[S\tau_1 = \tau_2 \equiv (\tau_1 = w_1\ \&\ \tau_2 = w_2 \to Sw_1 = w_2)].$$

From the three formulas above we can obtain

$$\text{Sat}\ \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall z_3)(\forall z)$$
$$[z_3 = 14 \circ Qw_1 \circ 1 \circ Qw_2\ \&\ z = 14 \circ G_{\tau_1} \circ 1 \circ G_{\tau_2} \to (S\tau_1 = \tau_2 \equiv$$
$$(\tau_1 = w_1\ \&\ \tau_2 = w_2 \to \psi(z_3)))\ \&\ (\tau_1 = w_1\ \&\ \tau_2 = w_2 \to (\psi(z_3) \equiv \psi(z)))].$$

Hence one can also prove

(G4) $\text{Sat}\ \psi \rightarrow (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall w_1)(\forall w_2)(\forall z)[z = 14 \circ G_{\tau_1} \circ 1 \circ G_{\tau_2} \rightarrow (S\tau_1 = \tau_2 \equiv (\tau_1 = w_1 \,\&\, \tau_2 = w_2 \rightarrow \psi(z)))]$.

Lemma 16.1 gives us the provability of

$$(\forall v_1)(\forall v_2)\ldots(\forall_k)(\exists w_1)(\exists w_2)(\tau_1 = w_1 \,\&\, \tau_2 = w_2).$$

This together with (G4) gives

$$\text{Sat}\ \psi \rightarrow (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z)[z = 14 \circ G_{\tau_1} \circ 1 \circ G_{\tau_2} \rightarrow (\psi(z) \equiv S\tau_1 = \tau_2)],$$

which is the desired formula.

Thus we have established our claim for all atomic formulas. Let us assume that our Theorem holds true for formulas with fewer than n logical connectives, and that F is a formula with n logical connectives and k free variables $v_1,\ldots,v_k$.

H. F is of the form $\neg$ f. From our inductive assumption follows the provability of

$$\text{Sat}\ \psi \rightarrow (\forall v_1)(\forall v_2)\ldots(v_k)(\forall z_1)[z_1 = G_f \rightarrow (\psi(z_1) \equiv f)],$$

which is equivalent to

$$\text{Sat}\ \psi \rightarrow (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z_1)[z_1 = G_f \rightarrow (\neg\, \psi(z_1) \equiv \neg\, f)].$$

As Sat ψ contains the Negation clause, we can prove

$$\text{Sat}\ \psi \rightarrow (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z_1)(\forall z)[z_1 = G_f \,\&\, z = 14 \circ z_1 \rightarrow (\psi(z) \equiv \neg\, \psi(z_1))].$$

The last two formulas give

$$\text{Sat}\ \psi \rightarrow (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z)[z = 14 \circ G_f \rightarrow (\psi(z) \equiv \neg\, f)],$$

which is the formula whose provability we wanted to show.

I. Let F be of the form $(f_1 \vee f_2)$. From our inductive assumption, the following is provable:

$$\text{Sat } \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z_1)(\forall z_2)[z_1 = G_{f_1} \;\&\; z_2 = G_{f_2} \to (\psi(z_1) \equiv f_1) \;\&\; (\psi(z_2) \equiv f_2)].$$

Therefore we can also prove

(I1) $$\text{Sat } \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z_1)(\forall z_2)[z_1 = G_{f_1} \;\&\; z_2 = G_{f_2} \to (\psi(z_1) \vee \psi(z_2) \equiv f_1 \vee f_2)].$$

As Sat ψ contains the Disjunction clause, one can prove

$$\text{Sat } \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z_1)(\forall z_2)(\forall z)[z_1 = G_{f_1} \;\&\; z_2 = G_{f_2} \;\&\; z = 10 \circ G_{f_1} \circ 5 \circ G_{f_2} \circ 11 \to (\psi(z) \equiv \psi(z_1) \vee \psi(z_2))],$$

which, together with (I1), yields

$$\text{Sat } \psi \to (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z)[z = 10 \circ G_{f_1} \circ 5 \circ G_{f_2} \circ 11 \to (\psi(z) \equiv f_1 \vee f_2)].$$

J. For F of the form $(f_1 \;\&\; f_2)$ we proceed analogously, using the Conjunction clause of Sat ψ.

K. For F of the form $(f_1 \to f_2)$ the proof is again analogous. We use the Implication clause of Sat ψ.

L. Let F be of the form $(\exists v_1)(f)$. If v_1 does not occur free in f, then we can prove

(L1) $$(\forall v_2)(\forall v_3)\ldots(\forall v_k)(f \equiv (\exists v_1) f).$$

From our inductive assumption, the formula

$$\text{Sat } \psi \to (\forall v_2)(\forall v_3)\ldots(\forall v_k)(\forall z_1)[z_1 = G_f \to (\psi(z_1) \equiv f)]$$

is provable. This together with Lemma 16.8 implies the provability of

$$\text{Sat } \psi \to (\forall v_2)(\forall v_3)\ldots(\forall v_k)(\forall z)(\forall z_1)[z = G_F \;\&\; \text{Inst}(z,z_1) \to (\psi(z_1) \equiv f)].$$

From (L1), this implies the provability of

$$\text{Sat } \psi \to (\forall v_2)(\forall v_3)\ldots(\forall v_k)(\forall z)(\forall z_1)[z = G_F \;\&\; \text{Inst}(z,z_1) \to (\psi(z_1) \equiv (\exists v_1) f)].$$

As Sat ψ contains the Existential Quantifier clause, it follows that

$$\text{Sat } \psi \rightarrow (\forall v_2)(\forall v_3)\ldots(\forall v_k)(\forall z)[z = G_F \rightarrow (\psi(z) \equiv (\exists v_1) f)]$$

is provable.

Now suppose v_1 does occur free in f. Again, from our inductive assumption follows the provability of

$$\text{Sat } \psi \rightarrow (\forall v_1)(\forall v_2)\ldots(\forall v_k)(\forall z_1)[z_1 = G_f \rightarrow (\psi(z_1) \equiv f)].$$

Therefore, in view of Lemma 16.5, one can also prove

$$\text{Sat } \psi \rightarrow (\forall v_2)(\forall v_3)\ldots(\forall v_k)[(\exists v_1)(f) \equiv (\exists v_1)(\exists z_1)(z_1 = G_f \ \& \ \psi(z_1))].$$

Lemmas 16.5 and 16.8 allow us to infer the provability of

$$\text{Sat } \psi \rightarrow (\forall v_2)(\forall v_3)\ldots(\forall v_k)(\forall z)[z = G_F \rightarrow ((\exists v_1)(f) \equiv$$
$$(\exists z_1)(\text{Inst}(z,z_1) \ \& \ \psi(z_1)))].$$

As Sat ψ contains the Existential Quantifier clause, the provability of the above formula implies the provability of

$$\text{Sat } \psi \rightarrow (\forall v_2)(\forall v_3)\ldots(\forall v_k)(\forall z)(z = G_F \rightarrow (F \equiv \psi(z))),$$

which is precisely what we wanted.

M. For F of the form $(\forall v_1)(f)$ the proof is analogous; we use the Universal Quantifier clause of Sat ψ.

THEOREM 17.2. For any two formulas H, ψ with one free variable, the formula Sat $\psi \rightarrow (\exists v)(H(v) \equiv \psi(v))$ is provable.

PROOF. Let v, w be any two variables with Gödel numbers a and b, respectively. Let D(v,w) denote the formula

$$D(v,w): \quad w = 10 \circ 9 \circ a \circ 11 \circ 10 \circ a \circ 1 \circ v \circ 7 \circ v \circ 11.$$

It follows from Theorem 17.1 that the formula

$$\text{Sat } \psi \rightarrow (\forall x)(\forall z)\{z = G_{(\forall v)(v=x\rightarrow(\forall w)(D(v,w)\rightarrow Hw))} \rightarrow$$
$$(\forall v)[(v = x \rightarrow (\forall w)(D(v,w) \rightarrow Hw)) \equiv \psi(z)]\}$$

is provable. In particular, if h is the Gödel number of

$$(\forall v)[v = x \to (\forall w)(D(v,w) \to Hw)],$$

the formula

(*) $$\text{Sat } \psi \to (\forall z)\{z = G_{(\forall v)(v=\bar{h}\to(\forall w)(D(v,w)\to Hw))} \to (\forall v)[(v = \bar{h} \to (\forall w)(D(v,w) \to Hw)) \equiv \psi(z)]\}$$

is provable. Let p be the Gödel number of

$$(\forall v)[v = \bar{h} \to (\forall w)(D(v,w) \to Hw)].$$

It follows from Lemma 15.5 that we can prove the sentence

$$\bar{p} = G_{(\forall v)(v=\bar{h}\to(\forall w)(D(v,w)\to Hw))}.$$

This and the provability of (*) give us the provability of

$$\text{Sat } \psi \to (\forall v)[(v = \bar{h} \to (\forall w)(D(v,w) \to Hw)) \equiv \psi(\bar{p})],$$

and therefore of

(**) $$\text{Sat } \psi \to [(\forall w)(D(\bar{h},w) \to Hw) \equiv \psi(\bar{p})].$$

Again using Lemma 15.5 we observe that the sentence $D(\bar{h},\bar{p})$ is provable; and, as can immediately be seen, so is $(\forall w)(D(\bar{h},w) \to w = \bar{p})$. This implies the provability of

$$H\bar{p} \equiv (\forall w)(D(\bar{h},w) \to Hw)$$

which, together with (**), yields Sat $\psi \to (H\bar{p} \equiv \psi(\bar{p}))$. This, finally, gives us the provability of Sat $\psi \to (\exists v)(Hv \equiv \psi(v))$.

THEOREM 17.3. For every formula F with one free variable, the formula $\neg$ Sat F is provable. In particular, we can prove $\neg$ Sat Prov.

PROOF. Taking F for ψ in Theorem 17.2, and $\neg$ F for H, we conclude the provability of Sat F $\to (\exists x)(\neg Fx \equiv Fx)$, and therefore of $\neg$ Sat F.

Notice that if x is the Gödel number of a formula $F_x(v)$, then D(x,y) expresses the fact that y is the Gödel number of the formula $(\forall v)(v = x \to F_x(v))$, logically equivalent to the diagonalization of F_x. Therefore, if we let θ denote the set expressed by H, $(\forall w)(D(x,w) \to Hw)$ holds if and only if the diagonalization of F_x belongs to θ; i.e. iff x is in θ^*. Thus the results of this chapter can be summarized as follows: A saturated set Ψ expressed by a formula ψ contains the Gödel number of a sentence if and only if the sentence itself holds. Let θ be any expressible set and let H(x) be the formula expressing it. Then the formula $H^*(x)$: $(\forall w)(D(x,w) \to H(w))$ expresses θ^*. Let h be the Gödel number of $H^*(x)$. Then Ψ contains the Gödel number p of $H^*(\bar{h})$ if and only if $H^*(\bar{h})$ holds, i.e. iff $H(\bar{p})$ holds. In other words, $\psi(\bar{p})$ is equivalent to $H(\bar{p})$. As this is true for every formula H, in particular it holds if H is $\neg\psi$. But this leads to a contradiction; therefore the existence of a formula ψ to express a saturated set Ψ is impossible.

§18. Further Consequences

We observe that by exactly the same kind of inductive argument as the ones employed above, using Lemma 15.20, we can obtain the provability of $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\text{Term } G_R)$ and of $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\text{For } G_F)$ for every term R and every formula F with k free variables $v_1, \ldots, v_k$. Also, if F is an axiom of arithmetic (or a logical axiom), the formula $(\forall v_1)(\forall_2)\ldots(\forall v_k)$ $(\text{ArAx } G_F)$ (or $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\text{Log Ax } G_F)$) will be provable; and if F can be obtained from F_1 and F_2 by one of the rules of inference, then we can prove $(\forall v_1)(\forall v_2)\ldots(\forall v_k)(\text{Inf}(G_{F_1}, G_{F_2}, G_F))$.

We also want to point out the provability of the formula

$$(\infty) \qquad (\forall x)(\forall y)(\text{Prov } x \;\&\; \text{Prov } 10 \circ x \circ 7 \circ y \circ 11 \to \text{Prov } y),$$

of which we will make extensive use. Indeed, the definition of Prov x implies the provability of (∀x)[Prov x → (∃w)(Proof(w ∘ 1 ∘ 1,x))] and of (∀x)(∀y)[Prov 10 ∘ x ∘ 7 ∘ y ∘ 11 → (∃z)(Proof(z ∘ 1 ∘ 1,10 ∘ x ∘ 7 ∘ y ∘ 11))]. As

(∀x)(∀y)(For x & For y → Inf(x,10 ∘ x ∘ 7 ∘ y ∘ 11,y))

is provable, so is

(∀w)(∀z)[Proof(w ∘ 1 ∘ 1,x) & Proof(z ∘ 1 ∘ 1,10 ∘ x ∘ 7 ∘ y ∘ 11) →
Proof(w ∘ z ∘ 1 ∘ 1 ∘ y ∘ 1 ∘ 1,y)],

which allows us to obtain (∞).

THEOREM 18.1. The following formulas are provable:

1. (∀x)(∀y_1)(∀y_2)[Num y_1 & Num y_2 & x = y_1 ∘ 1 ∘ y_2 → (y_1 = y_2 → Prov x)]
2. (∀z)(∀w)(Prov 10 ∘ Qz ∘ 2 ∘ Qw ∘ 11 ∘ 1 ∘ Q(z + w))
3. (∀x)(∀y)(∀z)(∀w)[Num y & Num z & Num w & x = 10 ∘ z ∘ 2 ∘ w ∘ 11 ∘ 1 ∘ y →
(A(y,z,w) → Prov x)]
4. (∀x)(∀y_1)(∀y_2)[Num y_1 & Num y_2 & x = y_1 ∘ 1 ∘ y_2 → (⌐ y_1 = y_2 →
Prov 4 ∘ x)]
5. (∀x)(∀y)(∀z)(∀w)[Num y & Num z & Num w & x = 10 ∘ z ∘ 2 ∘ w ∘ 11 ∘ 1 ∘ y →
(⌐ A(y,z,w) → Prov 4 ∘ x)]
6. (∀x)(∀y)(∀z)(∀w)[Num y & Num z & Num w & x = 10 ∘ z ∘ 3 ∘ w ∘ 11 ∘ 1 ∘ y →
(M(y,z,w) → Prov x)]
7. (∀x)(∀y)(∀z)(∀w)[Num y & Num z & Num w & x = 10 ∘ z ∘ 3 ∘ w ∘ 11 ∘ 1 ∘ y →
(⌐ M(y,z,w) → Prov 4 ∘ x)]
8. (∀y)(∀z)(Prov y ∘ 1 ∘ z → Prov z ∘ 1 ∘ y)
9. (∀y)(∀z)(∀u)(Prov y ∘ 1 ∘ z & Prov z ∘ 1 ∘ u → Prov y ∘ 1 ∘ u)
10. (∀y)(∀z)(∀w)(Prov y ∘ 1 ∘ z → Prov 14 ∘ y ∘ 1 ∘ 14 ∘ z & Prov 10 ∘ y ∘ 2 ∘ w ∘
11 ∘ 1 ∘ 10 ∘ z ∘ 2 ∘ w ∘ 11 & Prov 10 ∘ w ∘ 2 ∘ y ∘ 11 ∘ 1 ∘ 10 ∘ z ∘ 2 ∘ w ∘ 11 &

$\mathrm{Prov}\ 10 \circ y \circ 3 \circ w \circ 11 \circ 1 \circ 10 \circ z \circ 3 \circ w \circ 11\ \&\ \mathrm{Prov}\ 10 \circ w \circ 3 \circ y \circ 11 \circ 1 \circ 10 \circ z \circ 3 \circ w \circ 11)$

11. $(\forall y)(\forall z)(\mathrm{Prov}\ y \vee \mathrm{Prov}\ z \rightarrow \mathrm{Prov}\ 10 \circ y \circ 5 \circ z \circ 11)$

12. $(\forall y)(\forall z)(\mathrm{Prov}\ 10 \circ y \circ 6 \circ z \circ 11 \rightarrow \mathrm{Prov}\ y\ \&\ \mathrm{Prov}\ z)$

13. $(\forall y)(\forall z)(\mathrm{Prov}\ y\ \&\ \mathrm{Prov}\ z \rightarrow \mathrm{Prov}\ 10 \circ y \circ 6 \circ z \circ 11)$

14. $(\forall y)(\forall z)(\mathrm{Prov}\ 10 \circ y \circ 7 \circ z \circ 11 \equiv \mathrm{Prov}\ 10 \circ z \circ 5 \circ 4 \circ y \circ 11)$

15. $(\forall y)(\forall v)(\forall z)(\forall w)(\mathrm{Subst}(y,v,w,z)\ \&\ \mathrm{Prov}\ z \rightarrow \mathrm{Prov}\ 10 \circ 8 \circ v \circ 11 \circ 10 \circ y \circ 11)$

16. $(\forall y)(\forall v)[\mathrm{Prov}\ 10 \circ 9 \circ v \circ 11 \circ 10 \circ y \circ 11 \rightarrow (\forall w)(\forall z)(\mathrm{Subst}(y,v,w,z) \rightarrow \mathrm{Prov}\ z)]$

PROOF. 1. Assume Num y_1, Num y_2, $x = y_1 \circ 1 \circ y_2$ and $y_1 = y_2$. According to Lemma 15.1 the last two assumptions yield $x = y_2 \circ 1 \circ y_2$.

Let us consider any complete proof of Theorem II of §11, i.e. of $(\forall x')(x' = x')$. Let p be the sequence number of this proof and let p_1 be obtained from p by appending to it $10 \circ 10 \circ 9 \circ 12 \circ 13 \circ 11 \circ 10 \circ 12 \circ 13 \circ 1 \circ 12 \circ 13 \circ 11 \circ 7 \circ y_2 \circ 1 \circ y_2 \circ 11$ (which is the number of an instance of L4), followed by the separator, followed by $y_2 \circ 1 \circ y_2 \circ 1 \circ 1$. It follows from our preceding discussion that the fact that the resulting sequence number is the number of a proof of $y_2 \circ 1 \circ y_2$ is provable; therefore so is $(\forall y_2)(\mathrm{Num}\ y_2 \rightarrow \mathrm{Prov}\ y_2 \circ 1 \circ y_2)$, from which we obtain (1).

2. By induction on w. Assume, first, $w = 1$. As $Q1 = 15$, $z + 1 = Sz$ and $Q(Sz) = 14 \circ Qz$ are all provable, our task is to establish the provability of $\mathrm{Prov}\ 10 \circ Qz \circ 2 \circ 15 \circ 11 \circ 1 \circ 14 \circ Qz$. Let p be the Gödel number of P5, let p_1 denote $10 \circ Qz \circ 2 \circ 15 \circ 11 \circ 1 \circ 14 \circ Qz$, and let p_2 be the number obtained from p by preceding it with $1 \circ 1$ and appending to it $10 \circ p \circ 7 \circ p_1 \circ 11$ (an instance of L4), followed by $1 \circ 1 \circ p_1$. We can prove that p_2 is a sequence number of a proof of p_1; therefore (2) is provable when $w = 1$.

Let r_1 denote $10 \circ Qz \circ 2 \circ Qn \circ 11 \circ 1 \circ Q(z + n)$ and let r_2 denote $10 \circ Qz \circ 2 \circ 14 \circ Qn \circ 1 \circ 1 \circ 14 \circ Q(z + n)$. As r_2 can be proven to be equal to $10 \circ Qz \circ 2 \circ Q(Sn) \circ 1 \circ 1 \circ 14 \circ Q(z + Sn)$, our goal now will be to show that Prov r_2 can be inferred from Prov r_1. Let us assume Prov r_1; this yields $(\exists x)(\mathrm{Proof}(x,r_1))$. Let p be the Gödel number of P6 and let p_1 be obtained from p by appending to it $1 \circ 1$ followed by $10 \circ p \circ 7 \circ r_2$ (an instance of L4), followed by $1 \circ 1 \circ r_2 \circ 1 \circ 1$. Then, as $(\forall x)(\mathrm{Proof}(x,r_1) \rightarrow \mathrm{Proof}(x \circ p_1,r_2))$ is provable, so is - by our inductive assumption - Prov r_2; which concludes our proof.

As an immediate corollary of the provability of (2) we obtain the provability of (3).

It will be noticed that the proofs of (1) and (2) were obtained by replicating within the object language the metalinguistic arguments used in proving (a1) and (b1) of Lemma 12.1. Proofs of (4), (5), (6) and (7) can be obtained by similarly replicating the arguments used to establish (a2), (b2), (c1) and (c2) of the same Lemma.

8. From Prov $y \circ 1 \circ z$ we can infer $(\exists x)$ $\mathrm{Proof}(x \circ 1 \circ 1, y \circ 1 \circ z)$. Let p be the Gödel number of the formula $(\forall x')((\forall x'')((x' = x'' \rightarrow x'' = x')))$ (III of §11) and let p_1 be the sequence number of any proof of this formula. Let p_2 be obtained from p_1 by appending to it $10 \circ p \circ 7 \circ 10 \circ 9 \circ 12 \circ 13 \circ 13 \circ 11 \circ 10 \circ 10 \circ y \circ 1 \circ 12 \circ 13 \circ 13 \circ 7 \circ 12 \circ 13 \circ 13 \circ 1 \circ y \circ 11 \circ 11 \circ 11$ (an instance of L4) followed by $1 \circ 1$, followed by $10 \circ 10 \circ 9 \circ 12 \circ 13 \circ 13 \circ 11 \circ 10 \circ 10 \circ y \circ 1 \circ 12 \circ 13 \circ 13 \circ 7 \circ 12 \circ 13 \circ 13 \circ 1 \circ y \circ 11 \circ 11 \circ 7 \circ y \circ 1 \circ z \circ 11$ (also an instance of L4), followed by $1 \circ 1 \circ y \circ 1 \circ z \circ 1 \circ 1$. The formula $(\forall x)(\forall y)(\forall z)$ $[\mathrm{Proof}(x \circ 1 \circ 1, y \circ 1 \circ z) \rightarrow \mathrm{Proof}(x \circ p_2, z \circ 1 \circ y)]$ is provable; which yields a proof of (8).

We proceed analogously to establish the provability of (9) and (10), using IV of §11 for (9) and VI, VII, XI and XII for (10).

The provability of (11) follows from the fact that $(F \to (F \vee G))$ and $(G \to (F \vee G))$ are both provable for any two formulas F, G; therefore we can prove $(\forall y)(\forall z)(\text{Prov } 10 \circ y \circ 7 \circ 10 \circ y \circ 5 \circ z \circ 11 \circ 11 \;\&\; \text{Prov } 10 \circ z \circ 7 \circ 10 \circ y \circ 5 \circ z \circ 11 \circ 11)$, which yields (11) by an application of (∞) on page 73. By the same argument the provability of (12) and (13) follows from the provability of $((F \;\&\; G) \to F)$, $((F \;\&\; G) \to G)$ (for (12)) and of $(F \to (G \to (F \;\&\; G)))$ (for (13)). The provability of (14) follows from the fact that $((F \to G) \equiv (G \vee \neg F))$ is provable for all formulas F, G; the provability of (15) follows from the provability of $(F(\bar{n}) \to (\exists u)(F(u)))$ for all formulas F, all variables u and all natural numbers n; and, finally, the provability of (16) is a consequence of the provability of $((\forall u)(F(u)) \to F(\bar{n}))$.

We now introduce the four formulas

Consist: $(\forall x)(\neg(\text{Prov } x \;\&\; \text{Prov } 4 \circ x))$

ω-Consist: $(\forall v)(\forall x)[(\forall w)(\forall y)(\text{Subst}(x,v,Qw,y) \to \text{Prov } y) \to \neg \text{Prov}(10 \circ 8 \circ v \circ 11 \circ 10 \circ 4 \circ x \circ 11)]$

Compl: $(\forall x)(\text{Prov } x \vee \text{Prov } 4 \circ x)$

ω-Compl: $(\forall v)(\forall x)[(\forall w)(\forall y)(\text{Subst}(x,v,Qw,y) \to \text{Prov } y) \to \text{Prov}(10 \circ 9 \circ v \circ 11 \circ 10 \circ x \circ 11)]$,

expressing, respectively, the consistency, ω-consistency, completeness and ω-completeness of Peano Arithmetic.

THEOREM 18.2. The formula

$$\text{Compl} \to (\forall y)(\forall z)(\text{Prov } 10 \circ y \circ 5 \circ z \circ 11 \to \text{Prov } y \vee \text{Prov } z)$$

is provable.

PROOF. Let us assume Compl, Prov $10 \circ y \circ 5 \circ z \circ 11$ and $\neg$ Prov y. The first and last of these yield Prov $4 \circ y$. Our claim then follows from the provability of $((F \vee G) \to (\neg F \to G))$ by an application of(∞) on page 73, as in the proof of Theorem 18.1.

THEOREM 18.3. The formula

$$\text{Compl} \to (\forall y)(\forall z)(\text{Prov } 10 \circ y \circ 7 \circ z \circ 11 \to \text{Prov } z \vee \neg \text{ Prov } y)$$

is provable.

PROOF. This is a direct consequence of Theorems 18.1 (see parts (11) and (14)) and 18.2.

THEOREM 18.4. The formula

(*) $$\omega\text{-Consist} \;\&\; \text{Compl} \to (\forall v)(\forall y)[\text{Var } v \;\&\; \text{Prov } 10 \circ 8 \circ v \circ 11 \circ 10 \circ y \circ 11 \to (\exists w)(\exists z)(\text{Subst}(y,v,Qw,z) \;\&\; \text{Prov } z)]$$

is provable.

PROOF. As the formula $((\exists v)(F) \equiv (\exists v) \neg\neg(F))$ is provable for all formulas F and all variables v, we can show by an argument analogous to the previous ones that

(**) $$(\forall v)(\forall y)[\text{Var } v \to (\text{Prov } 10 \circ 8 \circ v \circ 11 \circ 10 \circ y \circ 11 \equiv \text{Prov } 10 \circ 8 \circ v \circ 11 \circ 10 \circ 4 \circ 4 \circ y \circ 11)]$$

is also provable. From the definition of Compl we obtain the provability of

$$\text{Compl} \to (\forall y)(\forall v)[(\forall w)(\forall z)(\text{Subst}(y,v,Qw,z) \to \neg \text{ Prov } z) \to (\forall w)(\forall z)(\text{Subst}(y,v,Qw,z) \to \text{Prov } 4 \circ z)].$$

Therefore, by the definition of ω-Consist we obtain

$$\omega\text{-Consist} \;\&\; \text{Compl} \to (\forall y)(\forall v)[(\forall w)(\forall z)(\text{Subst}(y,v,Qw,z) \to \neg \text{ Prov } z) \to \neg \text{ Prov } 10 \circ 8 \circ v \circ 11 \circ 10 \circ 4 \circ 4 \circ y \circ 11)].$$

Together with (**), this yields

$$\omega\text{-Consist} \,\&\, \text{Compl} \rightarrow (\forall y)(\forall v)[(\forall w)(\forall z)(\text{Subst}(y,v,Qw,z) \rightarrow \neg\, \text{Prov}\ z)$$

$$\rightarrow \neg\, \text{Prov}\ 10 \circ 8 \circ v \circ 11 \circ 10 \circ y \circ 11],$$

which is equivalent to (*).

THEOREM 18.5. The formula

$$\text{Consist} \,\&\, \text{Compl} \rightarrow (\forall x)(\text{Prov}\ 4 \circ x \equiv \neg\, \text{Prov}\ x)$$

is provable.

PROOF. Immediate.

THEOREM 18.6. The formula

$$\omega\text{-Consist} \,\&\, \omega\text{-Compl} \,\&\, \text{Consist} \,\&\, \text{Compl} \rightarrow \text{Sat Prov}$$

is provable.

PROOF. This is an immediate consequence of Theorems 18.1 through 18.5.

THEOREM 18.7. The formula

$$\omega\text{-Consist} \,\&\, \text{Compl} \rightarrow \omega\text{-Compl} \,\&\, \text{Consist}$$

is provable.

PROOF. As $((F \,\&\, \neg F) \rightarrow G)$ is provable for any two formulas F, G, we can show by an argument analogous to the ones employed above that $(\forall y)(\forall z)(\text{Prov}\ y \,\&\, \text{Prov}\ 4 \circ y \rightarrow \text{Prov}\ z)$ is provable. Therefore we can also prove

(*) $\neg\text{Consist} \rightarrow (\forall z)(\text{For}\ z \rightarrow \text{Prov}\ z).$

To obtain ω-Consist $\rightarrow$ Consist, let us consider the formula $x' = x'$. By what we said earlier, For $12 \circ 13 \circ 1 \circ 12 \circ 13$ is provable. So is

$$\omega\text{-Consist} \rightarrow (\exists w)(\exists y)(\text{Subst}(12 \circ 13 \circ 1 \circ 12 \circ 13, 12 \circ 13, Qw, y) \,\&$$

$$\text{Prov}\ y\ ) \vee \neg\, \text{Prov}\ 10 \circ 8 \circ 12 \circ 13 \circ 11 \circ 10 \circ 4 \circ 12 \circ 13 \circ 1 \circ 12 \circ 13 \circ 11,$$

which yields ω-Consist $\rightarrow (\exists x)(\text{For}\ x \,\&\, \neg\, \text{Prov}\ x)$. As (*) is provable, we obtain

(**) ω-Consist $\rightarrow$ Consist.

Next we show the provability of ω-Consist & Compl $\rightarrow$ ω-Compl. As $(\neg(\exists v)(\neg F) \rightarrow (\forall v)(F))$ is provable for all formulas F and all variables v, so is

(***) $(\forall x)(\forall v)[\text{Var } v \,\&\, \text{For } x \rightarrow (\text{Prov } 4 \circ 10 \circ 8 \circ v \circ 11 \circ 10 \circ 4 \circ x \circ 11 \rightarrow \text{Prov } 10 \circ 9 \circ v \circ 11 \circ 10 \circ x \circ 11)]$.

From the definition of Compl we obtain

$$\text{Compl} \rightarrow (\forall x)(\forall v)(\text{Var } v \,\&\, \text{For } x \,\&\, \neg\, \text{Prov } 10 \circ 8 \circ v \circ 11 \circ 10 \circ 4 \circ x \circ 11 \rightarrow \text{Prov } 4 \circ 10 \circ 8 \circ v \circ 11 \circ 10 \circ 4 \circ x \circ 11).$$

Together with the definition of ω-Consist, this gives us

$$\omega\text{-Consist} \,\&\, \text{Compl} \rightarrow (\forall x)(\forall v)[(\forall w)(\forall y)(\text{Subst}(x,v,Qw,y) \rightarrow \text{Prov } y) \rightarrow \text{Prov } 4 \circ 10 \circ 8 \circ v \circ 11 \circ 10 \circ 4 \circ x \circ 11],$$

and combining it with (***), we get

$$\omega\text{-Consist} \,\&\, \text{Compl} \rightarrow (\forall x)(\forall v)[(\forall w)(\forall y)(\text{Subst}(x,v,w,y) \rightarrow \text{Prov } y) \rightarrow \text{Prov } 10 \circ 9 \circ v \circ 11 \circ 10 \circ x \circ 11],$$

which is

(****) ω-Consist & Compl $\rightarrow$ ω-Compl.

(**) and (****) yield the desired formula ω-Consist & Compl $\rightarrow$ ω-Compl & Consist.

THEOREM 18.8. The formula ω-Consist & Compl $\rightarrow$ Sat Prov is provable.

PROOF. Immediate, from Theorems 18.6 and 18.7.

THEOREM 18.9. The formula $\neg$ (ω-Consist & Compl) is provable.

PROOF. Immediate, from Theorems 17.3 and 18.8.

APPENDIX

As we have explained in the Introduction, Gödel's original proof rests on representing the set of Gödel numbers of all theorems - and, further, the set Ref^* - rather than expressing it. We will show how to construct the formula needed for this proof and see how it differs from the one employed by us.

We say that a set A is <u>representable</u> if there exists a formula F with one free variable such that for all n

$F(\bar{n})$ is provable iff $n \varepsilon A$.

The formula F is then said to <u>represent</u> A. If, in addition, the negation of F represents the complement of A, i.e. if for all n we also have

$\neg F(\bar{n})$ is provable iff $n \notin A$,

then F is said to <u>totally represent</u> A.

In general, if R is any k-nary relation on N, then the formula F represents R if for any $n_1,\ldots n_k$ in N

$F(\bar{n}_1,\ldots \bar{n}_k)$ is provable iff R holds between $n_1,\ldots n_k$,

and totally represents R if it represents R and also

$\neg F(\bar{n}_1,\ldots,\bar{n}_k)$ is provable iff R does not hold between $n_1,\ldots,n_k$.

It is a consequence of Gödel's Theorem that expressibility and representability do not coincide. For some numbers n $F(\bar{n})$ might be true without our being able to prove it. We will show, however, that under appropriate assumptions formulas of a certain type are provable for precisely those natural numbers for which they are true; in other words, those formulas represent the sets (or relations) which they express.

If F is a formula and v, u are variables, we will use the notation $(\exists v < u)(F)$ as shorthand for $(\exists v)(v < u \& F)$, and the notation $(\forall v < u)(F)$ as shorthand for $(\forall v)(v < u \rightarrow F)$. We call $(\exists v < u)$ and $(\forall v < u)$ restricted quantifiers, and the above formulas containing them restricted quantifications of F.

A formula is constructive arithmetic (c.a.) if all its quantifiers are restricted. An e.c.a. formula is an unrestricted existential quantification of a constructive arithmetic formula.

We will now show the following:

THEOREM 1. If arithmetic is consistent, then every c.a. formula totally represents the relation it expresses.

PROOF. Assuming the consistency of arithmetic, we have to show that if $F(v_1,\ldots v_k)$ is a c.a. formula, then $F(\bar{n}_1,\ldots,\bar{n}_k)$ is true precisely for those k-tuples $n_1,\ldots n_k$ of natural numbers for which it is provable, and false precisely for those for which it is refutable.

First let us observe that if arithmetic is consistent, then it suffices if we show that

If $F(\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable

and

If $F(\bar{n}_1,\ldots,\bar{n}_k)$ is false, then $\neg F(\bar{n}_1,\ldots,\bar{n}_k)$ is provable.

To see how our claim follows from these two conditions, let us suppose that $F(\bar{n}_1,\ldots,\bar{n}_k)$ is provable. If arithmetic is consistent, $\neg F(\bar{n}_1,\ldots,\bar{n}_k)$ cannot be provable at the same time, and $F(\bar{n}_1,\ldots,\bar{n}_k)$ cannot therefore be false. Thus if $F(\bar{n}_1,\ldots,\bar{n}_k)$ is provable, it must also be true.

Next we observe that for formulas of the form $u = v$, $u + v = w$ and

$u \cdot v = w$ our theorem coincides with Lemma 12.1. Let i_0 denote the i-function of the standard model. We show

A. For every pure term τ, the sentence $\tau = \overline{i_0(\tau)}$ is provable.

If τ is a numeral, then $\overline{i_0(\tau)}$ is just τ, and the fact that $\tau = \tau$ is provable follows from Lemma 12.1. Suppose now that our claim holds for two terms τ_1, τ_2; so that $\tau_1 = \overline{i_{}(\tau_1)}$ and $\tau_2 = \overline{i_0(\tau_2)}$ are both provable. We show that then $S\tau_1 = \overline{i_0(S\tau_1)}$, $\tau_1 + \tau_2 = \overline{i_0(\tau_1 + \tau_2)}$ and $\tau_1 \cdot \tau_2 = \overline{i_0(\tau_1 \cdot \tau_2)}$ are also provable. First we remark that

$$\overline{i_0(S\tau_1)} = \overline{i_0(\tau_1) + 1} = S\overline{i_0(\tau_1)},$$
$$\overline{i_0(\tau_1 + \tau_2)} = \overline{i_0(\tau_1) + i_0(\tau_2)},$$
$$\overline{i_0(\tau_1 \cdot \tau_2)} = \overline{i_0(\tau_1) \cdot i_0(\tau_2)}.$$

If $\tau_1 = \overline{i_0(\tau_1)}$ is provable, then so is $S\tau_1 = S\overline{i_0(\tau_1)}$, by Axiom P6. Using the properties of equality listed in §11, we can easily obtain $S\tau_1 = \overline{i_0(S\tau_1)}$. Furthermore, the assumption we made about τ_1 and τ_2 lets us prove $\tau_1 + \tau_2 = \overline{i_0(\tau_1)} + \tau_2$ and $\overline{i_0(\tau_1)} + \tau_2 = \overline{i_0(\tau_1)} + \overline{i_0(\tau_2)}$ (by VI and XI), as well as $\tau_1 \cdot \tau_2 = \overline{i_0(\tau_1)} \cdot \tau_2$ and $\overline{i_0(\tau_1)} \cdot \tau_2 = \overline{i_0(\tau_1)} \cdot \overline{i_0(\tau_2)}$ (by VIII and XIII). Again using the appropriate properties of equality we get $\tau_1 + \tau_2 = \overline{i_0(\tau_1)} + \overline{i_0(\tau_2)}$ and $\tau_1 \cdot \tau_2 = \overline{i_0(\tau_1)} \cdot \overline{i_0(\tau_2)}$. As $\overline{i_0(\tau_1)} + \overline{i_0(\tau_2)} = \overline{i_0(\tau_1) + i_0(\tau_2)}$ and $\overline{i_0(\tau_1)} \cdot \overline{i_0(\tau_2)} = \overline{i_0(\tau_1) \cdot i_0(\tau_2)}$ are both provable (Lemma 12.1), we can obtain $\tau_1 + \tau_2 = \overline{i_0(\tau_1 + \tau_2)}$ and $\tau_1 \cdot \tau_2 = \overline{i_0(\tau_1 \cdot \tau_2)}$. Thus we have inductively established (A).

B. Our theorem holds if F is an atomic formula. That is, for every atomic formula $F(v_1,\ldots,v_k)$, for any natural numbers $n_1,\ldots,n_k$,

If $F(\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable;

If $\neg F(\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable.

Indeed, an atomic formula must be of the form $\tau_1 = \tau_2$, where τ_1,τ_2 are terms. Let $n_1,\ldots n_k$ be any k natural numbers. $F(\bar{n}_1,\ldots,\bar{n}_k)$ will be of the form $\pi_1 = \pi_2$, where π_1 and π_2 are the pure terms obtained from τ_1, τ_2 by substituting $\bar{n}_1,\ldots, \bar{n}_k$ for the free variables $v_1,\ldots,v_k$. For $\pi_1 = \pi_2$ to be true means that $i_0(\pi_1)$ and $i_0(\pi_2)$ are the same natural number - we call it n. It follows from (A) above that $\pi_1 = \bar{n}$ and $\pi_2 = \bar{n}$ are both provable. Therefore, using V of §11, we can prove $\pi_1 = \pi_2$.

If, on the other hand, $\pi_1 = \pi_2$ is false (i.e. $\neg F(\bar{n}_1,\ldots,\bar{n}_k)$ is true), then $i_0(\pi_1)$ does not equal $i_0(\pi_2)$. Therefore, by Lemma 12.1, $\neg\, \overline{i_0(\pi_1)} = \overline{i_0(\pi_2)}$ is provable. As $\pi_1 = \overline{i_0(\pi_1)}$ and $\pi_2 = \overline{i_0(\pi_2)}$ are also provable, the desired provability of $\neg\, \pi_1 = \pi_2$ follows from the provability (via the properties of equality) of

$$\pi_1 = \overline{i_0(\pi_1)} \rightarrow (\pi_2 = \overline{i_0(\pi_2)} \rightarrow (\pi_1 = \pi_2 \rightarrow \overline{i_0(\pi_1)} = \overline{i_0(\pi_2)})).$$

C. Assuming that we have established the truth of our theorem for the c.a. formulas $F(v_1,\ldots v_k)$ and $G(w_1,\ldots,w_j)$, we will show that then it must also hold for the c.a. formulas $\neg F(v_1,\ldots,v_k)$, $F(v_1,\ldots,v_k) \vee G(w_1,\ldots w_j)$ and $F(v_1,\ldots,v_k) \,\&\, G(w_1,\ldots,w_j)$.

We start with negation : we have assumed that for any k natural numbers $n_1,\ldots, n_k$,

If $F(\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable;

(*) If $\neg F(\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable.

The first of these can be rephrased as

If $\neg\neg F(\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable,

which, together with (*), is what we want to show.

Concerning disjunction: If $n_1,\ldots, n_k, m_1,\ldots, m_j$ are any k + j natural numbers, then $F(\bar{n}_1,\ldots,\bar{n}_k) \vee G(\bar{m}_1,\ldots,\bar{m}_j)$ is true iff at least one of the disjuncts is true. But whichever disjunct is true, it will also be provable; and so will the disjunction. Furthermore, the disjunction is false iff both disjuncts are false. In that case both $\neg F(\bar{n}_1,\ldots,\bar{n}_k)$ and $\neg G(\bar{m}_1,\ldots,\bar{m}_j)$ are provable, which makes their conjunction, and hence $\neg(F(\bar{n}_1,\ldots,\bar{n}_k) \vee G(\bar{m}_1,\ldots,\bar{m}_j))$, provable as well.

The proof is analogous for conjunction.

D. Suppose that our claim holds for the c.a. formula $F(v,v_1,\ldots,v_k)$ with k + 1 free variables. We show that then it also holds for $(\exists v < w)F(v,v_1,\ldots,v_k)$ and for $(\forall v < w)F(v,v_1,\ldots,v_k)$, i.e. that for all k+1-tuples $m, n_1,\ldots,n_k$ of natural numbers we have

If $(\exists v < \bar{m})F(v,\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable;

If $\neg(\exists v < \bar{m})F(v,\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable,

as well as

If $(\forall v < \bar{m})F(v,\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable;

If $\neg(\forall v < \bar{m})F(v,\bar{n}_1,\ldots,\bar{n}_k)$ is true, then it is provable.

We first concern ourselves with the existential formula. Suppose that $(\exists v < \bar{m})F(v,\bar{n}_1,\ldots,\bar{n}_k)$ is true. Then there exists a number a smaller than m such that $F(\bar{a},\bar{n}_1,\ldots,\bar{n}_k)$ is true. $a < m$ means that for some b, $\bar{a} + \bar{b} = \bar{m}$ is true; which makes it - and therefore $\bar{a} < \bar{m}$ - provable. Also, we have assumed that $F(\bar{a},\bar{n}_1,\ldots,\bar{n}_k)$ is provable. Hence, so is

$$\bar{a} < \bar{m} \;\&\; F(\bar{a},\bar{n}_1,\ldots,\bar{n}_k)$$

and, finally,

$$(\exists v)(v < \bar{m} \;\&\; F(v,\bar{n}_1,\ldots,\bar{n}_k)).$$

Suppose now that $(\exists v < \bar{m})F(v,\bar{n}_1,\ldots,\bar{n}_k)$ is false. This means that the sentences $F(1,\bar{n}_1,\ldots,\bar{n}_k)$, $F(2,\bar{n}_1,\ldots,\bar{n}_k),\ldots$, $F(\overline{m-1},\bar{n}_1,\ldots,\bar{n}_k)$ are all false. It follows that their negations are provable, and so are

$$(\forall v)(v = 1 \rightarrow \neg F(v,\bar{n}_1,\ldots,\bar{n}_k)),$$

$$(\forall v)(v = 2 \rightarrow \neg F(v,\bar{n}_1,\ldots,\bar{n}_k)),$$

$$\ldots$$

$$(\forall v)(v = \overline{m-1} \rightarrow \neg F(v,\bar{n}_1,\ldots,\bar{n}_k)).$$

Therefore, so is

$$(\forall v)(v = 1 \vee v = 2 \vee \ldots \vee v = \overline{m-1} \rightarrow \neg F(v,\bar{n}_1,\ldots,\bar{n}_k)).$$

From Lemma 12.2 we can then conclude the provability of

$$(\forall v)(v < \bar{m} \rightarrow \neg F(v,\bar{n}_1,\ldots,\bar{n}_k)),$$

which is equivalent to the provability of

$$\neg (\exists v)(v < \bar{m}\ \&\ F(v,\bar{n}_1,\ldots,\bar{n}_k)).$$

To show that our claim transfers from the c.a. formula $F(v,v_1,\ldots,v_k)$ to $(\forall v < w)\ F(v,v_1,\ldots,v_k)$, we notice that from what we have already established it does transfer to $\neg F(v,v_1,\ldots,v_k)$; thence to $(\exists v < w) \neg F(v,v_1,\ldots,v_k)$ and thence to $\neg (\exists v < w) \neg F(v,v_1,\ldots,v_k)$. But the latter is equivalent to $(\forall v < w)\ F(v,v_1,\ldots,v_k)$.

This completes the proof of Theorem 1.

THEOREM 2. If arithmetic is ω-consistent, then every e.c.a. formula represents the relation it expresses.

PROOF. Let $F(v,v_1,\ldots,v_k)$ be any c.a. formula. We want to show that for all $n_1,\ldots, n_k$ in N

$$(\exists v)\ F(v,\bar{n}_1,\ldots,\bar{n}_k) \text{ is true iff it is provable.}$$

Suppose, then, that $(\exists v)\ F(v,\bar{n}_1,\ldots,\bar{n}_k)$ is true. Then for some $n \in N$, $F(\bar{n},\bar{n}_1,\ldots,\bar{n}_k)$ is true. As we have assumed that arithmetic is consistent and as F is a c.a. formula, it follows from Theorem 1 that $F(\bar{n},\bar{n}_1,\ldots,\bar{n}_k)$ must be provable. Therefore so is $(\exists v)\ F(v,\bar{n}_1,\ldots,\bar{n}_k)$.

Assume now that our e.c.a. formula is provable. It follows from ω-consistency that for some $n \in N$, $\vdash F(\bar{n},\bar{n}_1,\ldots,\bar{n}_k)$ cannot be proven. As F is c.a., it must then be the case that $F(\bar{n},\bar{n}_1,\ldots,\bar{n}_k)$ is provable. Hence it must be true - and so is $(\exists v)\ F(v,\bar{n}_1,\ldots,\bar{n}_k)$.

Theorems 1 and 2 can be generalized to cases when the quantifiers are restricted not necessarily by variables, but by functions of a certain kind.

LEMMA A. Let R be a binary relation whose domain is all of N. Let $F(v,w)$ be a formula with two free variables expressing R. If F represents R and if, in addition, the formula

$$(\forall w_1)(\forall w_2)(F(\bar{n},w_1)\ \&\ F(\bar{n},w_2) \rightarrow w_1 = w_2)$$

is provable for every natural number n, then F totally represents R.

PROOF. Knowing that F represents the relation it expresses and assuming, as we did before, that arithmetic is consistent, we have to show that for all $n, m \in N$

$$\text{If } \vdash F(\bar{n},\bar{m}) \text{ is true, then it is provable.}$$

So suppose that $\vdash F(\bar{n},\bar{m})$ holds. As R has all of N for its domain, $F(\bar{n},\bar{j})$ has to hold for some j different from m. Therefore $F(\bar{n},\bar{j})$ is provable and - by what has been established earlier - so is $\vdash \bar{j} = \bar{m}$. From our assumption,

$$F(\bar{n},\bar{j})\ \&\ F(\bar{n},\bar{m}) \rightarrow \bar{j} = \bar{m}$$

can be proven; therefore we can prove $\vdash F(\bar{n},\bar{m})$.

We say that the formula $F(v,w)$ with two free variables represents (totally represents) a function $f: N \rightarrow N$ iff F represents (totally represents) the relation $f(n) = m$.

If $F(v,w)$ expresses the function f and if P is a formula, we will use the notation $(\exists u < f(v))\ P$ and $(\forall u < f(v))\ P$ as shorthand for $(\exists w)(u < w)(F(v,w)\ \&\ P)$ and $(\exists w)(F(v,w)\ \&\ (\forall u < w)\ P)$, respectively.

THEOREM 3. Let $F(v,w)$ be a formula representing a function $f\colon N \to N$ and such that

$$(\forall w_1)(\forall w_2)(F(\bar{n},w_1)\ \&\ F(\bar{n},w_2) \to w_1 = w_2)$$

is provable for each number n. Then, if $P(v_1,\ldots,v_k,u)$ totally represents the relation it expresses, so do $(\exists u < f(v))\ P(v_1,\ldots,v_k,u)$ and $(\forall u < f(v))\ P(v_1,\ldots,v_k,u)$.

PROOF. Assuming - as before - that arithmetic is consistent, we have to show that for any $n_1,\ldots,n_k,n$ in N

If $(\exists u < f(n))\ P(\bar{n}_1,\ldots,\bar{n}_k,u)$ is true, then it is provable;

If $\neg\ (\exists u < f(n))\ P(\bar{n}_1,\ldots,\bar{n}_k,u)$ is true, then it is provable,

and

If $(\forall u < f(n))\ P(\bar{n}_1,\ldots,\bar{n}_k,u)$ is true, then it is provable;

If $\neg\ (\forall u < f(n))\ P(\bar{n}_1,\ldots,\bar{n}_k,u)$ is true, then it is provable.

Suppose, then, that the existential formula is true. Then, if m is the number such that $f(n) = m$, there exists some $j < m$ such that $P(\bar{n}_1,\ldots\bar{n}_k,\bar{j})$ holds. From the assumptions we have made about F and P it follows that $F(\bar{n},\bar{m})$ and $P(\bar{n}_1,\ldots,\bar{n}_k,\bar{j})$ will be provable; also, as we have argued before, one can prove $\bar{j} < \bar{m}$. Thus

$$F(\bar{n},\bar{m})\ \&\ \bar{j} < \bar{m}\ \&\ P(\bar{n}_1,\ldots,\bar{n}_k,\bar{j})$$

is provable, and so is

$$(\exists w)(\exists u)(F(\bar{n},w)\ \&\ u < w\ \&\ P(\bar{n}_1,\ldots,\bar{n}_k,u)),$$

which is our existential formula.

Suppose now that the negation of $(\exists u < f(n))\ P(\bar{n}_1,\ldots,\bar{n}_k,u)$ is true. That means that if $j = f(n)$, then all of $\neg P(\bar{n}_1,\ldots,\bar{n}_k,1)$, $\neg P(\bar{n}_1,\ldots,\bar{n}_k,2)$. $\ldots$, $\neg P(\bar{n}_1,\ldots,\bar{n}_k,\overline{j-1})$ are true. Therefore they are all provable, and so is

$$(\forall u)(u = 1 \vee u = 2 \vee \ldots \vee u = \overline{j-1} \rightarrow \neg P(\bar{n}_1,\ldots,\bar{n}_k,u)).$$

In view of Lemma 12.2, this implies the provability of

$$(\forall u)(u < \bar{j} \rightarrow \neg P(\bar{n}_1,\ldots,\bar{n}_k,u)).$$

It follows from our assumptions that we can prove $F(\bar{n},\bar{j})$ and $(\forall w)(F(\bar{n},w) \rightarrow w = \bar{j})$. Therefore

$$(\forall w)(\forall u)(F(\bar{n},w)\ \&\ u < w \rightarrow u < \bar{j})$$

is provable and, consequently, so is

$$(\forall w)(\forall u < w)(F(\bar{n},w) \rightarrow \neg P(\bar{n}_1,\ldots,\bar{n}_k,u)).$$

To establish our claim for the restricted universal quantification, suppose that

$$(*) \qquad (\exists w)(F(\bar{n},w)\ \&\ (\forall u < w)\ P(\bar{n}_1,\ldots,\bar{n}_k,u))$$

holds. Let $j = f(n)$. Then $F(\bar{n},\bar{j})$ is provable, and so is $(\exists w)\ F(\bar{n},w)$. From previous considerations we know that $(\forall u < \bar{j})\ P(\bar{n}_1,\ldots,\bar{n}_k,u)$ is provable. Therefore (*) is provable. On the other hand, if (*) is false and if $j = f(n)$, we can prove $F(\bar{n},\bar{j})$ as well as $\neg\ (\forall u < \bar{j})\ P(\bar{n}_1,\ldots,\bar{n}_k,u)$. This, together with the provability of $(\forall w)(F(\bar{n},w) \rightarrow w = \bar{j})$, establishes the provability of

$$(\forall w)(F(\bar{n},w) \rightarrow \neg\ (\forall u < w)\ P(\bar{n}_1,\ldots,\bar{n}_k,u)).$$

THEOREM 4. If arithmetic is ω-consistent and if $F(v,v_1,\ldots,v_k)$ totally represents the relation it expresses, then $(\exists v)\ F(v,v_1,\ldots,v_k)$ represents the relation it expresses.

PROOF. Analogous to that of Theorem 2.

A function $f\colon N \to N$ which is represented by a formula $F(v,w)$ such that

$$(\forall w_1)(\forall w_2)(F(\bar{n},w_1) \;\&\; F(\bar{n},w_2) \to w_1 = w_2)$$

is provable for each n, will be called <u>functionally representable</u>. Thus Theorem 3 says that a formula all of whose quantifiers are restricted by functionally representable functions totally represents the relation it expresses. Theorem 4 says that an existential quantification of such a formula represents the relation it expresses. In particular, if all the functions restricting the quantifiers are identity functions, we obtain Theorems 1 and 2.

The following consequence of the preceding theorems will prove useful:

COROLLARY. If arithmetic is ω-consistent, then the composition of functionally representable functions is functionally representable.

PROOF. Let f, g be functionally representable and let $F(v,w)$ and $G(v,w)$ be formulas representing them. By the Lemma preceding Theorem 3, F and G totally represent f,g. Therefore, by Theorem 4, the formula

$$(\exists z)(F(x,z) \;\&\; G(z,y))$$

represents the relation $g(f(x)) = y$. It remains to show that, given any $n \in N$, the sentence

$$(*) \qquad (\forall y_1)(\forall y_2)[(\exists z_1)(F(\bar{n},z_1) \;\&\; G(z_1,y_1)) \;\&\; (\exists z_2)(F(\bar{n},z_2) \;\&\; G(z_2,y_2)) \to y_1 = y_2]$$

is provable. Let m, k be such that $f(n) = m$, $g(m) = k$. As F and G functionally represent f and g, we can prove

$$(\forall y_1)(\forall y_2)[(\exists z)(F(\bar{n},z) \;\&\; G(z,y_1)) \;\&\; (\exists z)(F(\bar{n},z) \;\&\; G(z,y_2)) \to G(\bar{m},y_1) \;\&\; G(\bar{m},y_2)],$$

as well as

$$(\forall y_1)(\forall y_2)(G(\bar{m},y_1) \;\&\; G(\bar{m},y_2) \rightarrow y_1 = y_2).$$

Those two sentences let us prove (*).

Theorem 3 as well as the above Corollary could have been formulated for functions of more than one variable, with proofs practically unchanged. In particular, as the functions $x \cdot y$, $x + y$, $x + 1$ and 17^x are all functionally representable, so are $17^{x \cdot y}$, 17^{x+y} and 17^{x+1}.

We have established certain syntactic features which guarantee that the formula possessing them represents the relation which it expresses. Our aim is to construct such formulas for all the relations which before we have found expressible. We do so under the assumption that arithmetic is ω-consistent.

Let $P_{17}(v)$ now be the formula

$$P_{17}(v): \quad (\exists y < v)(v = 17 \cdot y) \;\&\; (\forall x < v)[(\exists y < v)(v = y \cdot x) \rightarrow x = 1 \vee (\exists w < v)(x = 17 \cdot w)]$$

and let L denote the formula

$$L: \quad S(16 \cdot y) = v \vee 16 \cdot y + 17 = 17 \cdot v \vee (\exists w < 16 \cdot y)(v + w = S(16 \cdot y)) \;\&\; (\exists w < 16 \cdot y + 17)(16 \cdot y + 17 + w = 17 \cdot v).$$

Then $x \circ y = z$ is represented by

$$x \circ y = z: \quad (\exists v < y)(P_{17}(v) \;\&\; L \;\&\; z = x \cdot v + y),$$

and for $y = x_1 \circ \ldots \circ x_k$ we obtain

$$y = x_1 \circ \ldots \circ x_k: \quad (\exists y_1 < y)(\exists y_2 < y)\ldots(\exists y_{k-2} < y)(y_1 = x_1 \circ x_2 \;\&\; y_2 = x_2 \circ x_3 \;\&\ldots\&\; y_{k-2} = x_{k-2} \circ x_{k-1} \;\&\; y = y_{k-2} \circ x_k).$$

We can now also represent the relations:

x begins y

$$xBy: \quad x = y \vee (\exists z < y)(x \circ z = y)$$

x ends y

xEy: $x = y \vee (\exists z < y)(z \circ x = y)$

x is part of y

xPy: $xBy \vee xEy \vee (\exists z_1 < y)(\exists z_2 < y)(z_1 \circ x \circ z_2 = y)$

x is a sequence number

Seq x: $1 \circ 1Bx \,\&\, 1 \circ 1Ex \,\&\, \neg\, 1 \circ 1 = x \,\&\, \neg\, 1 \circ 1 \circ 1Px$

y is an element of the sequence with sequence number x

$y \varepsilon x$: Seq $x \,\&\, 1 \circ 1 \circ y \circ 1 \circ 1Px$

z appears earlier than y in the sequence with number x

$z \underset{x}{\leq} y$: Seq $x \,\&\, y \varepsilon x \,\&\, (\exists t < x)(\text{Seq } t \,\&\, tBx \,\&\, z \varepsilon t \,\&\, \neg\, y \varepsilon t)$.

The expressibility of closures of sets under relations rested on Theorem 7.1, stating that a necessary and sufficient condition for x to belong to the closure of A under R is the existence of a certain sequence of elements from the field of R. This sequence should have x as its last element and each of its elements should either belong to A or stand in the relation R to some of the earlier elements of the sequence. If x is in A_R, the corresponding sequence will be called the A_R-sequence for x. We say that the relation R is bounded iff for every x in A_R, the number of elements in the A_R-sequence for x does not exceed $l(x)$. As the length of x cannot exceed x, the length of the sequence number of the A_R-sequence for x, under the assumption that R is bounded, cannot exceed $x \cdot (x+2) + 2$. Therefore the sequence number itself must be less than $17(1 + \frac{17^{x(x+2)+2} - 17}{16})$, which is less than $17^{x(x+2)+3}$.

THEOREM 5. If R is a bounded, totally representable relation and A is a totally representable subset of N, then the set A_R is totally representable.

PROOF. Let F_A, F_R totally represent A and R, respectively. It follows from the proof of Theorem 3, the Corollary to Theorem 4 and the functional representibility of $x \cdot y$, $x + y$ and 17^x that the formula

$$A_R(x): \quad (\exists y < 17^{x(x+2)+4})(\exists t < y)[\mathrm{Seq}\ y \ \& \ 1 \circ 1 \circ x \circ 1 \circ 1 E y \ \& \\ (\forall w < y)(w \varepsilon y \rightarrow F_A(w) \vee (\exists w_1 < y)(\exists w_2 < y)\ldots(\exists w_{k-1} < y) \\ (w_1 \underset{y}{\leq} w \ \& \ldots \& \ w_{k-1} \underset{y}{\leq} w \ \& \ F_R(w_1,\ldots,w_{k-1},w)))]$$

totally represents A_R.

We further construct the formulas:

x is the Gödel number of a numeral

$$\mathrm{Num}\ x: \quad x = 15 \vee (\exists y < x)[y \circ 15 = x \ \& \ (\forall z < y)(zPy \rightarrow 14Pz)]$$

x is the Gödel number of a variable

$$\mathrm{Var}\ x: \quad (\exists y < x)[12 \circ y = x \ \& \ (\forall z < y)(zPy \rightarrow 13Pz)]$$

z is the Gödel number of an expression obtained from the expressions with numbers x and y by one of the "term building" operations

$$\mathrm{tb}(x,y,z): \quad z = 14 \circ x \vee z = 10 \circ x \circ 2 \circ y \circ 11 \vee z = 10 \circ x \circ 3 \circ y \circ 11.$$

x is the Gödel number of a term iff it belongs to the closure of the set A of all Gödel numbers of numerals and variables with respect to the operation tb. This operation is bounded - in fact, the length of the A_{tb}-sequence for x is precisely $l(x)$. Also, both tb and A are totally representable. Therefore, from Theorem 5, we can conclude that the set of Godel numbers of terms is totally representable by means of some formula, which we will denote by Term x.

x is the Gödel number of an atomic formula

$$\mathrm{Atf}\ x: \quad (\exists y < x)(\exists z < x)(\mathrm{Term}\ y \ \& \ \mathrm{Term}\ z \ \& \ x = y \circ 1 \circ z)$$

x is the Gödel number of an expression obtained from the expressions numbered x and y by one of the "formula building" operations

$fb(x,y,z)$: $z = 4 \circ x \vee z = 10 \circ x \circ 5 \circ y \circ 11 \vee z = 10 \circ x \circ 6 \circ y \circ 11 \vee z = 10 \circ x \circ 7 \circ y \circ 11 \vee (\exists v < z)(\mathrm{Var}\ v \ \&\ (z = 10 \circ 8 \circ v \circ 11 \circ 10 \circ x \circ 11 \vee z = 10 \circ 9 \circ v \circ 11 \circ 10 \circ x \circ 11))$.

The Gödel number of a formula is an element of the closure of the set A of numbers of atomic formulas under the operation fb. As both A and fb are totally representable and as fb is bounded - the length of the A_{fb}-sequence for x is exactly l(x) - the set of Gödel numbers of formulas is totally representable. We call the formula which totally represents it For x.

We further represent:

the expression with Gödel number z_2 is built up from the expressions numbered x_2, y_2 by exactly the same placement of logical constants as that by which the expression with number z_1 is built up from the expressions numbered x_1, y_1

$SB(x_1,x_2,y_1,y_2,z_1,z_2,v)$: $\mathrm{Var}\ v \ \&\ \{(z_1 = 14 \circ x_1 \ \&\ z_2 = 14 \circ x_2) \vee (z_1 = 10 \circ x_1 \circ 2 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 2 \circ y_2 \circ 11) \vee (z_1 = 10 \circ x_1 \circ 3 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 3 \circ y_2 \circ 11) \vee (z_1 = x_1 \circ 1 \circ y_1 \ \&\ z_2 = x_2 \circ 1 \circ y_2) \vee (z_1 = 4 \circ x_1 \ \&\ z_2 = 4 \circ x_2) \vee (z_1 = 10 \circ x_1 \circ 5 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 5 \circ y_2 \circ 11) \vee (z_1 = 10 \circ x_1 \circ 6 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 6 \circ y_2 \circ 11)$
$(z_1 = 10 \circ x_1 \circ 7 \circ y_1 \circ 11 \ \&\ z_2 = 10 \circ x_2 \circ 7 \circ y_2 \circ 11) \vee (\exists v_1 < z_1)$
$[\mathrm{Var}\ v_1 \ \&\ \neg\, v_1 = v \ \&\ ((z_1 = 10 \circ 8 \circ v_1 \circ 11 \circ 10 \circ x_1 \circ 11 \ \&\ z_2 = 10 \circ 8 \circ v_1 \circ 11 \circ 10 \circ x_2 \circ 11) \vee (z_1 = 10 \circ 9 \circ v_1 \circ 11 \circ 10 \circ x_1 \circ 11 \ \&\ z_2 = 10 \circ 9 \circ v_1 \circ 11 \circ 10 \circ x_2 \circ 11))]\}$

w is the number of a pair whose first element is a variable, a numeral or a quantifier formula where the quantification is with respect to the variable numbered v, and whose second element results from the first by substituting the expression numbered t for the variable numbered v

$\mathrm{BegSub}(v,t,w)$: $\quad \mathrm{Var}\ v\ \&\ (\exists u_1 < w)(\exists u_2 < w)[w = u_1 \circ 2 \circ 2 \circ u_2\ \&$
$((\mathrm{Num}\ u_1\ \&\ u_2 = u_1) \vee (\mathrm{Var}\ u_1\ \&\ \neg\, u_1 = v\ \&\ u_1 = u_2) \vee (u_1 = v\ \&$
$u_2 = t) \vee (\exists u_3 < w)(\mathrm{For}\ u_3\ \&\ (u_1 = 10 \circ 8 \circ v \circ 11 \circ 10 \circ u_3 \circ 11\ \vee$
$u_1 = 10 \circ 9 \circ v \circ 11 \circ 10 \circ u_3 \circ 11)\ \&\ u_2 = u_1)]$.

y is the Gödel number of the result of substituting the expression with number w for the variable numbered v in the expression numbered x iff there exists a sequence number whose last element is $x \circ 2 \circ 2 \circ y$ and such that every element is a pair t either fulfilling BegSub(v,w,t) or else such that its first and second element are built up from the first and second elements, respectively, of some earlier pairs by parallel placements of logical constants. The length of this sequence number will not exceed $x((x \cdot 17^{x} + y) + 4)$ and therefore the sequence number itself will be less than $17^{x((x \cdot 17^{x}+y)+5)}$. It follows from Theorem 3 and the corollary to Theorem 4 that the following formula totally represents the substitution relation just described:

$\mathrm{Subst}(x,v,w,y)$: $\quad (\exists z < 17^{x((x\cdot 17^{x}+y)+5)})[\mathrm{Seq}\ z\ \&\ x \circ 2 \circ 2 \circ y \circ 1 \circ 1 Ez\ \&$
$(\forall t < z)(t \in z \rightarrow \mathrm{BegSub}(v,w,t) \vee (\exists t_1 < z)(\exists t_2 < z)(\exists x_1 < t_1)$
$(\exists x_2 < t_1)(\exists y_1 < t_2)(\exists y_2 < t_2)(\exists z_1 < t)(\exists z_2 < t)(t_1 = x_1 \circ 2 \circ 2 \circ x_2\ \&$
$t_2 = y_1 \circ 2 \circ 2 \circ y_2\ \&\ t = z_1 \circ 2 \circ 2 \circ z_2\ \&\ \mathrm{SB}(x_1,x_2,y_1,y_2,z_1,z_2,v)))]$

y is the number of the instanciation of the formula with Gödel number x, obtained by substituting the numeral numbered z for the variable following the quantifier

$\mathrm{Inst}_1(x,y,z)$: $\quad (\exists x_1 < x)(\exists v < x)(\mathrm{Var}\ v\ \&\ \mathrm{Num}\ z\ \&\ (x = 10 \circ 8 \circ v \circ 11 \circ 10 \circ$
$x_1 \circ 11 \vee x = 10 \circ 9 \circ v \circ 11 \circ 10 \circ x_1 \circ 11)\ \&\ \mathrm{Subst}(x_1,v,z,y))$

y is the Gödel number of an instanciation of the formula with number x.

$\mathrm{Inst}(x,y)$: $\quad (\exists z < y)(\mathrm{Inst}_1(x,y,z))$

the variable with Gödel number v has a free occurrence in the formula with number x

$$\text{Free}(v,x): \quad (\forall y < x)(\text{Subst}(x,v,15,y) \rightarrow y = x)$$

the term with number t is free for the variable numbered v in the formula numbered x

$$\text{FrTerm}(t,v,x): \quad \text{For } x \;\&\; \text{Var } v \;\&\; \text{Term } t \;\&\; (\forall w < t)\{\text{Var } w \;\&\; [w = t \lor$$
$$(\exists t_1 < t)(\exists t_2 < t)(\neg\, 13Bt_2 \;\&(t = t_1 \circ w \lor t = w \circ t_2 \lor$$
$$t = t_1 \circ w \circ t_2) \rightarrow \neg\, (\exists y < x)(\text{Free}(v,y) \;\&$$
$$10 \circ 8 \circ w \circ 11 \circ 10 \circ y \circ 11Px \lor 10 \circ 9 \circ w \circ 11 \circ 10 \circ y \circ 11Px)]\}$$

x is the Gödel number of an axiom of arithmetic

$$\text{ArAx}(x): \quad (\exists u < x)(\exists v < x)(\exists w < x)\{\text{Var } u \;\&\; \text{Var } v \;\&\; \text{Var } w \;\&[(x = 10 \circ 9 \circ$$
$$u \circ 11 \circ 10 \circ 10 \circ 9 \circ v \circ 11 \circ 10 \circ 10 \circ 9 \circ w \circ 11 \circ 10 \circ 10 \circ u \circ 1 \circ v \circ$$
$$7 \circ 10 \circ u \circ 1 \circ w \circ 7 \circ v \circ 1 \circ w \circ 11 \circ 11 \circ 11 \circ 11 \circ 11 \lor x = 10 \circ 9 \circ u \circ$$
$$11 \circ 10 \circ 10 \circ 9 \circ v \circ 11 \circ 10 \circ 10 \circ u \circ 1 \circ v \circ 7 \circ 14 \circ u \circ 1 \circ 14 \circ v \circ$$
$$11 \circ 11 \circ 11 \lor x = 10 \circ 9 \circ u \circ 11 \circ 10 \circ 4 \circ 15 \circ 1 \circ 14 \circ u \circ 11 \lor$$
$$x = 10 \circ 9 \circ u \circ 11 \circ 10 \circ 10 \circ 9 \circ v \circ 11 \circ 10 \circ 10 \circ 14 \circ u \circ 1 \circ 14 \circ v \circ$$
$$7 \circ u \circ 1 \circ v \circ 11 \circ 11 \circ 11 \lor x = 10 \circ 9 \circ u \circ 11 \circ 10 \circ 10 \circ u \circ 2 \circ 15 \circ$$
$$11 \circ 1 \circ 14 \circ u \circ 11 \lor x = 10 \circ 9 \circ u \circ 11 \circ 10 \circ 10 \circ 9 \circ v \circ 11 \circ 10 \circ 10 \circ u \circ$$
$$2 \circ 14 \circ v \circ 11 \circ 1 \circ 14 \circ 10 \circ u \circ 2 \circ v \circ 11 \circ 11 \circ 11 \lor x = 10 \circ 9 \circ u \circ$$
$$11 \circ 10 \circ 10 \circ u \circ 3 \circ 15 \circ 11 \circ 1 \circ u \circ 11 \lor x = 10 \circ 9 \circ u \circ 11 \circ 10 \circ 10 \circ$$
$$9 \circ v \circ 11 \circ 10 \circ 10 \circ u \circ 3 \circ 14 \circ v \circ 11 \circ 1 \circ 10 \circ 10 \circ u \circ 3 \circ v \circ 11 \circ 2 \circ$$
$$u \circ 11 \circ 11 \circ 11 \lor (\exists y < x)(\exists y_1 < x)(\exists y_2 < x)(\text{Free}(u,y) \;\&$$
$$\text{Subst}(y,u,15,y_1) \;\&\; \text{Subst}(y,u,14 \circ u,y_2) \;\&\; x = 10 \circ y_1 \circ 7 \circ 10 \circ 10 \circ$$
$$9 \circ u \circ 11 \circ 10 \circ y \circ 7 \circ y_2 \circ 11 \circ 7 \circ 10 \circ 9 \circ u \circ 11 \circ y \circ 11 \circ 11 \circ 11)]\}$$

x is the Gödel number of a logical axiom

LogAx(x): (∃y < x)(∃w < x)(∃z < x){For y & For w & For z & [x = 10 ∘ y ∘
7 ∘ 10 ∘ w ∘ 7 ∘ y ∘ 11 ∘ 11 ∨ x = 10 ∘ 10 ∘ y ∘ 7 ∘ 10 ∘ w ∘ 7 ∘ z ∘ 11 ∘
11 ∘ 7 ∘ 10 ∘ 10 ∘ y ∘ 7 ∘ w ∘ 11 ∘ 7 ∘ 10 ∘ y ∘ 7 ∘ z ∘ 11 ∘ 11 ∘ 11 ∨
x = 10 ∘ 10 ∘ 4 ∘ w ∘ 7 ∘ 4 ∘ y ∘ 11 ∘ 7 ∘ 10 ∘ 10 ∘ 4 ∘ w ∘ 7 ∘ y ∘ 11 ∘ 7 ∘
w ∘ 11 ∘ 11 ∨ (∃v < x)(∃t < x)(∃y_1 < x)(FrTerm(t,v,y) &
Subst(y,v,t,y_1) & x = 10 ∘ 10 ∘ 9 ∘ v ∘ 11 ∘ 10 ∘ y ∘ 11 ∘ 7 ∘ y_1 ∘ 11) ∨
(∃v < x)(Var v & ⌐ Free(v,y) & x = 10 ∘ 10 ∘ 9 ∘ v ∘ 11 ∘ 10 ∘ 10 ∘
y ∘ 7 ∘ w ∘ 11 ∘ 11 ∘ 7 ∘ 10 ∘ y ∘ 7 ∘ 10 ∘ 9 ∘ v ∘ 11 ∘ 10 ∘ w ∘ 11 ∘ 11 ∘ 11) ∨
x = 10 ∘ 10 ∘ y ∘ 7 ∘ w ∘ 11 ∘ 7 ∘ 10 ∘ 4 ∘ y ∘ 5 ∘ w ∘ 11 ∘ 11 ∨
x = 10 ∘ 10 ∘ 4 ∘ y ∘ 5 ∘ w ∘ 11 ∘ 7 ∘ 10 ∘ y ∘ 7 ∘ w ∘ 11 ∘ 11 ∨
x = 10 ∘ 4 ∘ 10 ∘ 4 ∘ y ∘ 5 ∘ 4 ∘ w ∘ 11 ∘ 7 ∘ 10 ∘ y ∘ 6 ∘ w ∘ 11 ∘ 11 ∨
x = 10 ∘ 10 ∘ y ∘ 6 ∘ w ∘ 11 ∘ 7 ∘ 4 ∘ 10 ∘ 4 ∘ y ∘ 5 ∘ 4 ∘ w ∘ 11 ∘ 11 ∨
(∃v < x)(Var v & x = 10 ∘ 10 ∘ 8 ∘ v ∘ 11 ∘ 10 ∘ y ∘ 11 ∘ 7 ∘ 4 ∘ 10 ∘ 9 ∘
v ∘ 11 ∘ 10 ∘ 4 ∘ y ∘ 11 ∨ x = 10 ∘ 4 ∘ 10 ∘ 9 ∘ v ∘ 11 ∘ 10 ∘ 4 ∘ y ∘ 11 ∘
7 ∘ 10 ∘ 8 ∘ v ∘ 11 ∘ 10 ∘ y ∘ 11 ∘ 11)]}

the formula with Gödel number z is obtainable from the formulas numbered x and y by one of the rules of inference

Inf(x,y,z): For x & For y & (x = 10 ∘ y ∘ 7 ∘ z ∘ 11 ∨ (∃v < z)(Var v &
z = 10 ∘ 9 ∘ v ∘ 11 ∘ 10 ∘ x ∘ 11))

x is the sequence number of a proof of the formula with Gödel number y

Proof(x,y): Seq x & 1 ∘ 1 ∘ y ∘ 1 ∘ 1Ex & (∀z < x)[z ε x → ArAx(z) ∨ LogAx(z)
(∃z_1<x)(∃z_2<x)($z_1 \underset{x}{\leq} z$ & $z_2 \underset{x}{\leq} z$ & Inf(z_1,z_2,z))].

All the formulas constructed until now had the property of totally representing the relations they expressed. Therefore by Theorem 4 the following formula represents Th_0:

Prov x: $(\exists y)\ \mathrm{Proof}(y,x)$

y is the Gödel number of the diagonalization of the formula numbered x

Diag(x,y): $(\exists v < y)(\mathrm{Var}\ v\ \&\ y = 10 \circ 9 \circ v \circ 11 \circ 10 \circ 10 \circ x \circ 7 \circ v \circ 1 \circ x \circ 11 \circ 11)$.

The length of the number of the diagonalization of x does not exceed $4x + 8$. Therefore the number of the diagonalization itself is less than 17^{4x+9}, and we obtain the following formula to represent Ref^*:

Ref^* x: $(\exists y < 17^{4x+9})(\mathrm{Diag}(x,y)\ \&\ \mathrm{Prov}\ 4 \circ y)$.

Because of the restricted quantifiers, the formula which we have just obtained and which we would use for Gödel's original proof is much longer than the one we employed in Tarski's version. The question arises whether the syntactic feature which made all our formulas longer - the restriction of quantifiers - is a necessary one, or whether it was just a convenient device we employed to be able to immediately tell that our formulas represent the relations they express. It turns out that the existence of an existential quantification of a restricted quantifier formula expressing a relation is a necessary condition for the relation's representability (by "restricted quantifier formulas" we mean ones in which all the quantifiers are restricted by functionally representable functions). To show this, we first notice that the function Q(x), which we found expressible, is also totally represented by the formula

$Qx = y$: $(x = 1\ \&\ y = 15) \vee (\exists y_1 < y)(17^x = 16 \cdot y_1 + 17\ \&\ y = 14 \cdot y_1 + 15)$.

This lets us prove the following

THEOREM 6. If arithmetic is ω-consistent, then a relation is representable if and only if it can be expressed and represented by the existential quantification of a formula containing only restricted quantifiers.

PROOF. We have already shown that under the assumption of ω-consistency such a formula will indeed represent the relation it expresses. Suppose now that the relation R is representable, i.e. there exists a formula F such that for all natural numbers $n_1,\ldots, n_k$

$$F(\bar{n}_1,\ldots,\bar{n}_k) \text{ is true iff it is provable, iff } R(n_1,\ldots,n_k) \text{ holds.}$$

Let a be the Gödel number of $F(v_1,\ldots,v_k)$ and let $b_1,\ldots,b_k$ be the Gödel numbers of the variables $v_1,\ldots, v_k$, respectively. The following formula also represents R:

$$(\exists y_1 < 17^{x_1+1})(\exists y_2 < 17^{x_2+1})\ldots(\exists y_k < 17^{x_k+1})(\exists v_1 < 17^{a\cdot y_1})$$
$$(\exists v_2 < 17^{v_1\cdot y_2})\ldots(\exists v_{k-1} < 17^{v_{k-2}\cdot y_{k-1}})(\exists v_k < 17^{v_{k-1}\cdot y_k})[Qx_1 = y_1 \;\&$$
$$Qx_2 = y_2 \;\&\ldots\&\; Qx_k = y_k \;\&\; \text{Subst}(a,b_1,y_1,v_1) \;\&\; \text{Subst}(v_1,b_2,y_2,v_2)$$
$$\&\ldots\&\; \text{Subst}(v_{k-2},b_{k-1},y_{k-1},v_{k-1}) \;\&\; \text{Subst}(v_{k-1},b_k,y_k,v_k) \;\&\; \text{Prov}\; v_k].$$

As Prov v_k is the existential quantification of a formula with only restricted quantifiers, the above formula can be transformed into the existential quantification of a formula with restricted quantifiers only.

The above theorem of course in no way implies that a formula whose quantifiers are not restricted cannot represent the relation it expresses. We leave it as an open question whether the formulas we have obtained in this Appendix can be proven to be equivalent to the formulas with unrestricted quantifiers which we have used in the main part of this paper.

BIBLIOGRAPHY

[1] Gödel, Kurt. On Formally Undecidable Propositions of Principia Mathematica and Related Systems, Basic Books, New York, 1962.

[2] Grzegorczyk, Andrzej. Zarys Logiki Matematycznej, Państwowe Wydawnictwo Naukowe, Warszawa, 1961.

[3] Hilbert, David and Bernays, Paul. Grundlagen der Mathematik, 2 vols., Springer-Verlag, Berlin, 1970.

[4] Mendelson, Elliott. Introduction to Mathematical Logic, Van Nostrand, Princeton, New Jersey, 1964.

[5] Mostowski, Andrzej. Sentences Undecidable in Formalized Arithmetic, North-Holland, Amsterdam, 1964.

[6] Quine, Willard V. Mathematical Logic, Harvard University Press, Cambridge, Massachussetts, 1965.

[7] Smullyan, Raymond M. First-Order Logic, Springer-Verlag, New York, 1968.

[8] Smullyan, Raymond M. Languages in which Self-Reference is Possible, Journal of Symbolic Logic 22, pp. 55-67, 1957.

[9] Smullyan, Raymond M. Theory of Formal Systems, Princeton University Press, Princeton, New Jersey, 1961.

[10] Tarski, Alfred. The Concept of Truth in Formalized Languages , in Logic, Semantics, Metamathematics, pp. 152-278, Clarendon Press, Oxford, 1956.

[11] Tarski, Alfred, Mostowski, Andrzej and Robinson, Raphael. Undecidable Theories, North-Holland, Amsterdam, 1968.

AUTOBIOGRAPHICAL STATEMENT

Małgorzata Askanas was born in Poland on July 29, 1948. There she graduated from high school and, for three years, studied mathematics at the University of Warsaw. In 1969 she came to New York, where she enrolled in the doctoral program at the Graduate Center of City University of New York. From 1970 to 1975, while a student there, she taught mathematics at Lehman, John Jay and Sarah Lawrence College.