STANFORD ARTIFICIAL INTELLIGENCE PROJECT
MEMO AIM-129

COMPUTER SCIENCE DEPARTMENT REPORT
NO. CS167

SEMANTICS OF ALGOL-LIKE STATEMENTS

BY

SHIGERU IGARASHI

COMPUTER SCIENCE DEPARTMENT

STANFORD UNIVERSITY

STANFORD ARTIFICIAL INTELLIGENCE PROJECT JUNE 1970
MEMO AIM-129

COMPUTER SCIENCE DEPARTMENT REPORT
NO. CS167

Semantics of Algol-like Statements

by: Shigeru Igarashi */

Abstract: The semantics of elementary Algol-like statements is discussed, mainly based on an axiomatic method.

Firstly, a class of Algol-like statements is introduced by generalized inductive definition, and the interpretation of the statements belonging to it is defined in the form of a function over this class, using the induction principle induced by the above definition. Then a category of program is introduced in order to clarify the concept of equivalence of statements, which becomes a special case of isomorphism in that category.

A revised formal system representing the concept of equivalence of Algol-like statements is presented, followed by elementary metatheorems.

Finally, a process of decomposition of Algol-like statements, which can be regarded as a conceptual compiler, or a constructive description of semantics based on primitive actions, is defined and its correctness is proved formally, by the help of the induced induction principle.

(To appear in Symposium on the Semantics of Algorithmic Languages, Engeler, E. (ed.), Lecture Notes in Mathematics. Springer-Verlag, Berlin, Heidelberg, New York, 1970.)

The research reported here was supported in part by the Advanced Research Project Agency of the Office of the Department of Defense (SD-183).

*/ Computer Science Department, Stanford University, Stanford, California.

Page Intentionally Left Blank

1. Introduction

This paper is intended to describe an axiomatic approach to the semantics of Algol-like statements, which is mainly based on the axiomatic treatments of the equivalence of Algol-like statements by Igarashi (1964).

In Section 2, the class of Algol-like statements of our concern is defined syntactically, in order to clarify the scope of the present paper, which class is essentially generated by simple variables of a type, go to statements, labels, assignment statements with a set of functions, if-then-else with a set of predicates, semicolons for concatenation, and parentheses to compose compound statements.

Besides McCarthy's operator, namely $(\rightarrow,)$ for if-then-else, some notations different from usual ones will be introduced for the sake of conciseness, which will possibly help us to apply our mathematical intuition, though the writer has no intention of proposing such a notation for a general use. It must be noted that we use only different symbols and do not change the syntax. (Otherwise, it might become uncertain that we are working on algorithmic languages.)

We use a generalized inductive definition in order to define the class of our concern, which, although a little unnatural, constitutes a basis for defining and proving some things related to that class, by the help of the apparent induction principle induced by it.

In Section 3, the interpretation (that might be seen to be already a kind of semantics) of the statements belonging to the above mentioned class is given, which is done using induction on the class and the result

has a somewhat analytical appearance. Actually we shall define the interpretation as a function on the class into a certain set of partial functions, and, presumably, one can prove everything about these Algol-like statements using this function.

Some results included in the work by Manna and McCarthy (1969) will be taken into consideration, when we define the interpretation of conditional statements.

In Section 4, categories of a kind whose objects are Algol-like statements, the interpretation being fixed, will be introduced in order to clarify the meaning of the relations which have been used in equivalence theories of Algol-like statements by Yanov (1958), Igarashi (1964), de Bakker (1968), etc. (McCarthy (1963a) discussed the equivalence of conditional forms, which was also related to Algol-like statements, because the latter contain conditional statements.) together with the correspondence between these relations and the notion of correctness introduced by Floyd (1967) and refined by Manna (1968, 1969), which is also related to the discussions by Hoare (1969).

The relations $\overset{\sim}{\underset{X}{}}$ and $\tilde{=}$ defined by Igarashi (1964) become special cases of isomorphisms in one of these categories. (On the one hand, these categories, whose objects are defined in Sections 2 and 3, are intended to serve as a model of the formal system described in the later sections, though we shall not enter into this point. On the other hand, they can possibly be regarded as a basis for further algebraic theories concerning programs, as a branch of mathematical theory of computation.)

In Section 5, a formal system representing the relations $\tilde{\tilde{X}}$ and $\tilde{=}$ will be presented, which is a revision of the main formal system (L.4) in the paper by Igarashi (1964), of which the latter will sometimes be called 'the previous system'. Besides minor refinements, it is so extended that partial functions and partial predicates may be allowed in statements and that the ability of the formalism may be considerably improved, although it is incomplete (which is inevitable). Especially, Inference Rule 9 is new, for which McCarthy's notion of homomorphisms of programs (unpublished) and Floyd's above mentioned work are taken into consideration as well as the obvious relationship between program schemata, firstly treated by Yanov (1958), and finite automata discussed by Igarashi (1963) and Rutledge (1964). This rule is, however, still a result of compromise between capability and simplicity.

Axioms related to go to statements have been entirely reformed.

In Section 6, a number of elementary metatheorems concerning the formal system of Section 5 are proved. These metatheorems show that any theorem in the previous system becomes a theorem also in the present system. Therefore each of the completeness theorems for the previous system remains valid, though we shall not enter into this point.

It must be noted that the incompleteness of the formal system does not imply that this formalism gives only an inadequate description of semantics, for describing or defining the meaning of a program can be regarded as a rather special case of equivalence. In fact, for any Algol-like statement A (in the sense of Section 2) in which variable

symbols $x_1,\ldots,x_n$ occur and for any variable-free arithmetic expressions (constants in effect) $c_1,\ldots,c_n,d_1,\ldots,d_n$, the following holds:

> Let $\tilde{c}_1,\ldots,\tilde{c}_n,\tilde{d}_1,\ldots,\tilde{d}_n$ be the values corresponding to $c_1,\ldots,c_n,d_1,\ldots,d_n$, respectively. Then, A stops and gives the final values $\tilde{d}_1,\ldots,\tilde{d}_n$ to $x_1,\ldots,x_n$, respectively, provided that the initial values of $x_1,\ldots,x_n$ are $\tilde{c}_1,\ldots,\tilde{c}_n$, respectively, <u>if and only if</u> the formula
>
> $$x_1 := c_1;\ldots;x_n := c_n;A \supset x_1 := d_1;\ldots;x_n := d_n$$
>
> is provable in the formal system of our concern. (See Theorem 55 by Igarashi (1964).)

Thus the formalism has an ability no less than the explicit definition of the interpretation given in Section 3. (Namely, $J[A](\tilde{c}_1,\ldots,\tilde{c}_n,\iota) = (\tilde{d}_1,\ldots,\tilde{d}_n,\iota)$ if and only if the above formula is provable.)

In Section 7, we shall define a special transformation of the class of Algol-like statements of our concern. On the one hand, this transformation can be regarded as a representation of a conceptual compiler. On the other hand, it demonstrates how the meaning of each statement can be defined in terms of certain primitive actions on a conceptual machine. (Therefore, this transformation itself might be regarded as a 'constructive' definition of semantics.)

In Section 8, we shall formally prove the validity of the above transformation, (which mathematically means that each program is transformed into a program equivalent to it), in the system presented in Section 5. On the one hand, this can be regarded as a kind of proof of

compiler correctness (at least most of the essential features of the proof of compiler correctness being included), which has been done firstly by McCarthy and Painter (1967) for arithmetic expressions, using induction on expressions. On the other hand, this can be regarded as a sufficient proof of the validity of the particular description of semantics in Section 7 which is based on primitive actions. (Also cf., Painter (1967) and Kaplan (1968).)

Notation and Terminology

We shall use the following notations and terminology.

1. Sets.

Symbol ϕ denotes the null set. $S+S'$ denotes set $S \cup S'$ whenever $S \cap S' = \phi$. $\eta = \{0,1,2,\ldots,\}$. $\eta^{+} = \{1,2,\ldots\}$. $[0] = \phi$. If $n \geq 1$, then $[n] = \{1,2,\ldots,n\}$.

2. Functions.

We shall use the word function to mean a possibly partial function.

(f1) Expression

$$f : S \rightarrow S'$$

reads as follows.

(i) $f(a)$ may or may not be defined, for each $a \in S$.

(ii) If $f(a)$ is defined, then $f(a) \in S'$.

(iii) If $a \notin S$, then $f(a)$ is undefined.

(f2) Dom $f = \{a \mid f(a)$ is defined$\}$.

(f3) Let $S_0 \subseteq S$, then $f|S_0$ means the function g defined as follows. $(f : S \to S')$

$g : S_0 \to S'$.

$\mathrm{Dom}\ g = \mathrm{Dom}\ f \cap S_0$.

$g(a) = f(a)$ for each $a \in \mathrm{Dom}\ g$.

(f4) We note that $f|\mathrm{Dom}\ f$ is a total function for any f .

(f5) $f = g$ means that f and g are defined on the same set and that $f|\mathrm{Dom}\ f = g|\mathrm{Dom}\ g$, while the latter equality means the equivalence of the total functions in the usual sense.

(f6) If $f : S \to S'$ and $g : S' \to S''$, then $g \circ f$, or gf , means the function h defined as follows.

$h : S \to S''$.

$\mathrm{Dom}\ h = \mathrm{Dom}\ f \cap \{a | f(a) \in \mathrm{Dom}\ g\}$.

$h(a) = g(f(a))$ for each $a \in \mathrm{Dom}\ g$.

(f7) If $f : S \to S$, then f^n denotes the function $f \circ \ldots \circ f$ (n times). $\lim_{n \to \infty} f^n$ means the function g defined as follows.

$g : S \to S$.

$a \in \mathrm{Dom}\ g$ if and only if there exists $M_a \in \eta$ such that $f^{M_a}(a) = f^{M_a+1}(a)$, so that $f^m(a) = f^n(a)$ for any $m \geq M_a$ and $n \geq M_a$.

$g(a) = f^{M_a}(a)$ for each $a \in \mathrm{Dom}\ g$.

(f8) If $f : S \to S'$ and $g : S \to S'$, then $f+g$ means the function h defined as follows.

$$h : S \to S' .$$

$$\mathrm{Dom}\ h = (\mathrm{Dom}\ f - \mathrm{Dom}\ g) \cup (\mathrm{Dom}\ g - \mathrm{Dom}\ f) \cup \{a \mid a \in \mathrm{Dom}\ f \cap \mathrm{Dom}\ g \text{ and } f(a) = g(a)\} .$$

$$h(a) = \begin{cases} f(a) & a \in \mathrm{Dom}\ f \\ g(a) & a \in \mathrm{Dom}\ g - \mathrm{Dom}\ f . \end{cases}$$

3. Predicates

We shall use the word predicate to mean a possibly partial predicate. We shall write $p(a) = T$, $p(a) = F$, and $p(a) = U$, to mean $p(a)$ is true, false, and undefined, respectively. For each predicate p, ∇p denotes the total predicate defined by

$$(\nabla p)(a) = \begin{cases} T & p(a) = U \\ F & \text{otherwise.} \end{cases}$$

Similarly, for each function f, ∇f denotes the total predicate defined by

$$(\nabla f)(a) = \begin{cases} T & f(a) \text{ is undefined} \\ F & \text{otherwise.} \end{cases}$$

(Here p and f are assumed to be unary and defined on a certain fixed set, for simplicity's sake.) Thus $(\nabla f)(a)$ means $\neg * f(a)$ used by Manna and McCarthy (1969), while we shall use $*$ for various purposes in the present paper.

4. Truth Tables.

Since we are going to treat partial predicates, we have to define the meaning of logical connectives $\neg$, $\wedge$, $\vee$, $\supset$, and $\equiv$, for three-valued logic, for which we shall use the truth tables by Łukasiewicz (1941) denoted by Γ_{ℓ} , and that by McCarthy (1963b) denoted by Γ_{m} . Γ_{ℓ} for the value U is as follows.

$(\neg U) = U$. $(U \wedge T) = (T \wedge U) = U$. $(U \wedge F)^{*} = (F \wedge U) = F$.

$(U \wedge U) = U$. $(U \vee T)^{*} = (T \vee U) = T$. $(U \vee F) = (F \vee U) = U$.

$(U \vee U) = U$. $(U \supset T)^{*} = T$. $(U \supset F) = U$. $(U \supset U) = U$.

$(T \supset U) = U$. $(F \supset U) = T$. $(U \equiv T) = (T \equiv U) = F$.

$(U \equiv F) = (F \equiv U) = F$. $(U \equiv U) = T$.

In Γ_{m} the asterisked members, the remaining members being the same, become as follows. ($F \wedge U = F$ and $T \vee U = T$.) $(U \wedge F) = U$. $(U \vee T) = U$. $(U \supset T) = U$. In order to indicate the truth tables considered, logical connectives will be suffixed by Γ_{ℓ} or Γ_{m} . Thus, for instance, $\wedge_{\Gamma_{m}}(U,F) = U$.

5. Structures.

By a structure $\mathfrak{A}$ we shall mean a collection of functions and predicates defined on a set, which is called the underlying set of $\mathfrak{A}$ and denoted by $|\mathfrak{A}|$, together with that set. In the present paper these functions and predicates are possibly partial. We shall consider two structures (or two similarity classes strictly) $\mathfrak{A}$ and $\mathfrak{B}$ in the text.

2. Formation of Algol-like Statements

Alphabet

Let $\mathfrak{L}$, $\mathfrak{V}$, $\mathfrak{F}$, and $\mathfrak{R}$ be four disjoint sets whose elements are called label symbols, variable symbols, function symbols, and predicate symbols, respectively. The set $\mathfrak{F}$ is the union of disjoint sets $\mathfrak{F}^{(0)}, \mathfrak{F}^{(1)}, \ldots,$ and the elements of $\mathfrak{F}^{(n)}$ are called n-ary function symbols. Similarly, $\mathfrak{P}$ is the union of disjoint sets $\mathfrak{P}^{(0)}, \mathfrak{P}^{(1)}, \ldots,$ and the elements of $\mathfrak{P}^{(n)}$ are called n-ary predicate symbols. The alphabet of Algol-like statements consists of all the elements of $\mathfrak{L}$, $\mathfrak{V}$, $\mathfrak{F}$, and $\mathfrak{P}$, together with the following special symbols.

$$\Lambda \quad ^{-1} \quad := \quad ; \quad (\quad \rightarrow \quad , \quad)$$

In some cases described below the logical symbols:

$$\neg \quad \wedge \quad \vee \quad \forall \quad \exists$$

will be also contained.

Algol-like Statements

Algol-like statements, or statements, are defined together with a function denoted by $(\ )^{\sim}$ which sends each statement onto a finite subset of $\mathfrak{L}$, by generalized inductive definition as follows.

Atomic Statements

(a1) Λ is an atomic statement. $(\Lambda)^- = \emptyset$.

(a2) For each $\sigma \epsilon \mathfrak{f}$, σ and σ^{-1} are both atomic statements.
$(\sigma)^- = \emptyset$. $(\sigma^{-1})^- = [\sigma]$.

(a3) For each $x \epsilon \mathfrak{V}$ and each $y \epsilon \mathfrak{V}$, $x := y$ is an atomic statement.
$(x := y)^- = \emptyset$.

Statements

An atomic statement is a statement. Any other word on the above alphabet is a statement if and only if it is defined to be a statement by a repeated use of the following rules.

(b1) If A and B are two statements such that $(A)^- \cap (B)^- = \emptyset$, then A;B is a statement. $(A;B)^- = (A)^- + (B)^-$.

(b2) If $x := f_1, \ldots, x := f_n$ are n statements and $\pi^{(n)} \epsilon \mathfrak{P}^{(n)}$, then $x := \pi^{(n)} f_1 \ldots f_n$ is a statement. $(x := \pi^{(n)} f_1 \ldots f_n)^- = \emptyset$.

(b3) If $x := f_1, \ldots, x := f_n$, A , and B are n+2 statements such that $(A)^- \cap (B)^- = \emptyset$ and $\rho^{(n)} \epsilon \mathfrak{P}^{(n)}$, then $(\rho^{(n)} f_1 \ldots f_n \rightarrow A,B)$ is a statement. $((\rho^{(n)} f_1 \ldots f_n \rightarrow A,B))^- = (A)^- + (B)^-$.

A statement which is defined to be so only by the above rules will be called a basic statement.

(c1) If $(p \rightarrow A,B)$ is a statement, then $(\neg p \rightarrow A,B)$ is a statement.
$((\neg p \rightarrow A,B))^- = ((p \rightarrow A,B))^-$.

(c2) If $(p \to A,B)$ and $(q \to A,B)$ are two statements, then $(p \wedge q \to A,B)$ and $(p \vee q \to A,B)$ are both statements. The values of $(\ )^-$ are both identical with $((p \to A,B))^-$.

(c3) If $(p \to A,B)$ is a statement such that $x \varepsilon V$ occurs in p and neither $\forall x$ nor $\exists x$ occurs in p, then $(\forall x p \to A,B)$ and $(\exists x p \to A,B)$ are both statements. The values of $(\ )^-$ are both identical with $((p \to A,B))^-$.

Parentheses and commas will be used also auxiliarly to avoid syntactic ambiguity and to improve readability. Especially $\pi^{(n)} f_1 \ldots f_n$ and $\rho^{(n)} f_1 \ldots f_n$ are written as $\pi^{(n)}(f_1,\ldots,f_n)$ and $\rho^{(n)}(f_1,\ldots,f_n)$, respectively. Semicolons will be abbreviated if there is no possibility of ambiguity.

Representation by ALGOL 60

The statements in the above sense are intended to mean the statements in the sense of ALGOL 60 (Naur et al., 1960) as follows.

Λ corresponds to a dummy statement (empty).

σ corresponds to go to σ.

σ^{-1} corresponds to σ : (dummy statement labelled by σ).

$(p \to A,B)$ corresponds to if p then A else B.

$:=$, ;, $\neg$, $\wedge$, and $\vee$ mean the same as in ALGOL 60.

The parentheses used to avoid ambiugity either correspond to begin and end delimiting compound statements or mean the same as in ALGOL 60.

$(A)^-$ denotes the set of labels standing in A.

Thus each statement can be regarded as a statement in the sense of ALGOL 60 in so far as neither $\forall$ nor $\exists$ occurs in that. Thus we shall call σ, σ^{-1}, f such that $x := f$ is a statement, and p such that $(p \rightarrow A,B)$ is a statement, respectively, a go-to, a labelling, an arithmetic expression, and a Boolean expression.

Notations

Statements are denoted by $A,B,C,\ldots$. Arithmetic expressions and Boolean expressions are denoted by $f,g,h,\ldots$, and, $p,q,r,\ldots$, respectively. Label symbols and variable symbols are denoted by $\sigma,\tau,\upsilon,\ldots$, and, $x,y,z,\ldots$, respectively. We shall use a number of functions and predicates defined on the statements which describe elementary syntactic properties. The function $(\ )^-$, being a typical example, was already defined in the above. All other functions and predicates listed below can be effectively defined in a similar manner.

1. Sets of Labels. By an occurrence of $\sigma \in f$ in a statement A we mean only such an occurrence as is different from the occurrences in the statements of the form σ^{-1} occurring in A.

$A^+ = \{\sigma | \sigma$ occurs in $A\}$.

$A^- = \{\sigma | \sigma^{-1}$ occurs in $A\}$.

$A^{\pm} = A^+ \cup A^-$.

$A^{++} = A^+ - A^-$.

$A^{-+} = \{\sigma | \sigma \in A^+ \cap A^-$ and σ^{-1} occurs textually earlier than an occurrence of σ in $A\}$.

Thus A^+ means the set of labels which are used for the purpose of designating the destinations of the go to statements occurring in A. If $A^{++} \neq \phi$, then the control may leave A by executing a go to statement whose destination is not within A. Such a go to statement will be called an exit of A. If $A^{-+} = \phi$, there are no loops in A.

2. Sets of Variables.

$V[A] = \{x|x \text{ occurs in } A\}$,

$V[f] = \{x|x \text{ occurs in } f\}$,

and

$V[p] = \{x|x \text{ occurs in } p\}$.

$L[A] = \{x|$ a statement of the form $x := f$ occurs in $A\}$.

$R[A]$ is defined by induction as follows:

For each atomic statement such that $V[A] = \phi$, $R[A] = \phi$.

$R[x := f] = V[f]$.

$R[A;B] = R[A] \cup R[B]$.

$R[(p \rightarrow A,B)] = V[p] \cup R[A] \cup R[B]$.

Thus $L[A]$ means the set of variables whose values may be changed by the execution of A, while $R[A]$ means the set of variables whose values may affect the course of action and the results of executing A.

3. Substitution. Let $B_1,\ldots,B_n$ and A be $n+1$ statements such that B_i occurs in A m_i times $(m_i \geq 0)$, where the occurrences may be overlapped by each other unless they are not the same. Let B_i^j, $j \in [m_i]$, denotes the j-th occurrence of B_i, where the order is

defined by the position of the occurrence of the first symbol. Let $C_1,\ldots,C_n$ be n statements. Then, by

$$A_{B_1,\ldots,B_n}[C_1,\ldots,C_n]$$

or (omitted commas)

$$A_{B_1\ldots B_n}[C_1,\ldots,C_n]$$

is meant an arbitrary statement that is obtained from A by substituting C_i for $\hat{B}_i^{h(i,1)},\ldots,\hat{B}_i^{h(i,\ell_i)}$, for each $i\in[n]$, with the following restrictions:

(i) $0 \leq \ell_i \leq m_i$.

(ii) $1 \leq h(i,1) < \ldots < h(i,\ell_i) \leq m_i$.

(iii) The occurrence $\hat{B}_i^{h(i,j)}$ and $\hat{B}_{i'}^{h(i',j')}$ do not overlap each other, for any distinct pairs (i,j) and (i',j').

(iv) The result of the substitution is a statement.

By

$$A_{B_1\ldots B_n}[C_1,\ldots,C_n]^{\circ}$$

is meant the unique statement that is obtained in the case that $\ell_i = m_i$, for every $i\in[n]$, in the above, which does not always exist because of the restriction concerning overlapping and the requirement that the result should be a statement.

We shall use the same notation also for arithmetic expressions and Boolean expressions.

4. Copies. Let $\sigma_1,\ldots,\sigma_n$ be arbitrary distinct elements of $A^{\pm} - A^{++}$, and let $\tau_1,\ldots,\tau_n$ be distinct and $\tau_i \notin A^{\pm}$, for any $i\epsilon[n]$. Then

$$A_{\sigma_1\ldots\sigma_n\,\sigma_1^{-1}\ldots\sigma_n^{-1}}[\tau_1,\ldots,\tau_n,\ \tau_1^{-1},\ldots,\tau_n^{-1}]^o$$

is called a copy of A. If A_1 is a copy of A, and, A_2 is a copy of A_1, then A_2 is also called a copy of A. Copies of A are denoted by A',A",A"',... .

5. Go-to and Labelling.

A begins with a labelling, if A is of the form $\sigma^{-1}B$.

A ends with a go-to, if either A is of the form $B\sigma$ or A is of the form $(p \to B,C)$ and B and C both end with go-tos.

An occurrence of statement B in A is preceded by a go-to, (equivalently, B is preceded by a go-to in A), if A is of the form $C_\Lambda[\sigma B]$.

Page Intentionally Left Blank

3. Interpretation of Algol-like Statements

By an interpretation of statements we shall mean $(U,\kappa,\mathfrak{R},\Gamma^{o},J)$ defined as follows.

Let U be a subset of V, $\mathcal{A}_U$ the set of statements $\{A|V[A] \subseteq U\}$, and κ a bijection (i.e., 1-1 and onto function) such that

$$\kappa : U \to I ,$$

where I is either $[s]$, for an s, or η^{+} in accordance with the cardinality of U. Let $\mathfrak{L}'$ denote $\mathfrak{L}+\{\iota\}$, where ι is a new fixed symbol.

Let $\mathfrak{A}$ be a structure that satisfies the following conditions.

1. $|\mathfrak{R}| \neq \emptyset$.
2. For each $\pi^{(n)} \in \mathfrak{F}^{(n)}$, an n-ary partial function denoted by $\pi_{\mathfrak{R}}^{(n)}$ is defined. I.e.,
$$\pi_{\mathfrak{R}}^{(n)} : |\mathfrak{R}|^{n} \to |\mathfrak{R}| .$$
3. For each $\rho^{(n)} \in \mathfrak{R}^{(n)}$, an n-ary partial relation denoted by $\rho_{\mathfrak{R}}^{(n)}$ is defined. I.e.,
$$\rho_{\mathfrak{R}}^{(n)} : |\mathfrak{R}|^{n} \to \{T,F\} .$$

The elements of $|\mathfrak{R}|$ will be denoted by $a_1,b_1,c_1, a_2,b_2,c_2, \cdots$. Thus by $\mathfrak{R}$ will be meant the total functions by which $\pi^{(n)} \vdash \pi_{\mathfrak{R}}^{(n)}$ and $\rho^{(n)} \vdash \rho_{\mathfrak{R}}^{(n)}$ as well as the structure itself, strictly.

Let Γ^0 be a set of truth tables for logical connectives. Let $|\mathcal{B}|$ denote $|R|^s \times \mathfrak{L}^{\mathfrak{L}}$, i.e.,

$$\underbrace{|R| \times \ldots \times |R|}_{s \text{ times}} \times (\mathfrak{L}^{\mathfrak{L}}\{\mathfrak{L}\}) ,$$

if U is finite. The elements of $|\mathcal{B}|$ will be denoted by $a,b,c,\ldots$. For each $a \in |\mathcal{B}|$ such that

$$a = (a_1, \ldots, a_s, \sigma)$$

and each $u \in U$, a_u denotes $a_{\kappa(u)}$, and a_χ denotes σ. We write $(a)_u$ instead of a_u frequently for the readability's sake. If U is infinite, the infinite dimensicnal direct product $|R|^I$ will be used instead of $|R|^s$, namely s is considered to be infinite.

The total function J defined below sends each statement $A \in \mathcal{A}_U$ onto a partial function, $J[A]$, from $|\mathcal{B}|$ into $|\mathcal{B}|$. $J[A]$ will be written as $A_{\mathcal{B}}$, thus

$$A_{\mathcal{B}} : |\mathcal{B}| \to |\mathcal{B}| .$$

Two partial functions, one sending each arithmetic expression f such that $V[f] \subseteq U$ onto a partial function

$$f_{\mathcal{B}} : |\mathcal{B}| \to |R| ,$$

and the other sending each Boolean expression p such that $V[p] \subseteq U$ onto a partial predicate

$$p_{\mathcal{B}} : |\mathcal{B}| \to \{T,F\} ,$$

will be defined simultaneously for the readability's sake.

For a partial function

$$\varphi : |\mathfrak{B}| \to |\mathfrak{B}| \ ,$$

$\bar{\varphi}$ denotes the function defined by

$$\bar{\varphi} : |\mathfrak{B}| \to |\mathfrak{B}|$$

and

$$\bar{\varphi}(a) = \begin{cases} a & a_\chi = \iota \\ \varphi(a) & \text{otherwise.} \end{cases}$$

Definition of $\tilde{\iota}$

The definition of $J[A]$, i.e., $A_{\mathfrak{B}}$, given in accordance with the last rule which should be used in order to define A to be a statement (Section 2), which defines $J[A]$ for every $A \in \mathcal{A}_U$ effectively by the induction principle induced by the definition of statements, is as follows.

Atomic Statements

(a1) $A = \Lambda$.

$$A_{\mathfrak{B}}(a) = a \quad \text{for any } a \in |\mathfrak{B}| \ .$$

Hereafter the phrase like 'for any $a \in |\mathfrak{B}|$' will be omitted.

(a2) (i) $A = \sigma$.

$$(A_{\beta}(a)) = \begin{cases} \sigma & \chi \\ a & U \end{cases} \quad , \text{ if } a_{\chi} = \iota ;$$

and

$$A_{\beta}(a) = a \ , \quad \text{otherwise.}$$

(ii) $A = \sigma^{-1}$.

$$(A_{\beta}(a)) = \begin{cases} \iota & \chi \\ a & \end{cases} \quad , \text{ if } a_{\chi} = \sigma ;$$

and

$$A_{\beta}(a) = a \ , \quad \text{otherwise.}$$

(a3) $A = x := y$.

$$y_{\beta}(a) = a_y \ .$$

$$(A_{\beta}(a)) = \begin{cases} y_{\beta}(a) & x \\ a_u & U\text{-}x \text{ or } \chi \end{cases} \quad , \text{ if } a_{\chi} = \iota \ ;$$

and

$$A_{\beta}(a) = a \ , \quad \text{otherwise.}$$

Statements (non-atomic)

(b1) $A = B;C$.

$$A_{\beta}(a) = \lim_{n \to \infty} (\overline{C_{\beta} \circ B_{\beta}})^{n}((C_{\beta} \circ B_{\beta})(a)) \ .$$

(b2) $A = x := \pi^{(n)} f_1 \ldots f_n$.

$$(\pi^{(n)} f_1 \ldots f_n)_{\mathcal{B}}(a) = \pi_R^{(n)}(f_{1,\mathcal{B}}(a), \ldots, f_{n,\mathcal{B}}(a)) \quad .$$

$$(A_{\mathcal{B}}(a))_u = \begin{cases} (\pi^{(n)} f_1 \ldots f_n)_{\mathcal{B}}(a) & u = x \\ a & u \in U - \{x\} \text{ or } u = X \end{cases} \text{, if } a_X = \iota \text{ ;}$$

and

$A_{\mathcal{B}}(a) = a$, otherwise.

(b3) $A = (\rho^{(n)} f_1 \ldots f_n \to B, C)$.

$$(\rho^{(n)} f_1 \ldots f_n)_{\mathcal{B}}(a) = \rho_R^{(n)}(f_{1,\mathcal{B}}(a), \ldots, f_{n,\mathcal{B}}(a)) \quad .$$

$$A_{\mathcal{B}}(a) = \begin{cases} \lim_{n \to \infty} (\bar{B}_{\mathcal{B}} + \bar{C}_{\mathcal{B}})^n B_{\mathcal{B}}(a) \text{ ,} \\ \qquad a_X = \iota \text{ and } (\rho^{(n)} f_1 \ldots f_n)_{\mathcal{B}}(a) = T \text{ ,} \\ \qquad \text{or } a_X \in \bar{B} \text{ ;} \\ \lim_{n \to \infty} (\bar{B}_{\mathcal{B}} + \bar{C}_{\mathcal{B}})^n C_{\mathcal{B}}(a) \\ \qquad a_X = \iota \text{ and } (\rho^{(n)} f_1 \ldots f_n)_{\mathcal{B}}(a) = F \text{ ,} \\ \qquad \text{or } a_X \in \bar{C} \text{ ;} \\ a \text{ , } \quad a_X \notin \bar{B} \cup \bar{C} \cup \{\iota\} \text{ ;} \\ \text{undefined, otherwise.} \end{cases} \tag{1}$$

(c1) $A = (\neg\, p \rightarrow B,C)$.

$$(\neg\, p)_{\beta}(a) = \neg_{\Gamma^o}(p_{\beta}(a)) \quad . \qquad \text{(See Section 1.)}$$

A_{β} is defined by the same rule as (1) of (b3) above except that $(\rho^{(n)} f_1 \ldots f_n)_{\beta}(a)$, occurring twice in it, should be replaced by $(\neg\, p)_{\beta}(a)$.

(c2) (i) $A = (p \wedge q \rightarrow B,C)$.

$$(p \wedge q)_{\beta}(a) = \wedge_{\Gamma^o}(p_{\beta}(a), q_{\beta}(a)) \quad . \quad \text{(See Section 1.)}$$

A_{β} is defined by the same rule as (1) of (b3) above except that $(\rho^{(n)} f_1 \ldots f_n)_{\beta}(a)$ should be replaced by $(p \wedge q)_{\beta}(a)$.

The case $A = (p \vee q \rightarrow B,C)$ as well as the case (C3) will be omitted, for it suffices to define $(p \vee q)_{\beta}$, $(\forall x p)_{\beta}$, and $(\exists x p)_{\beta}$ similarly and use (1) as the above.

Intuitive Meaning of J

Practically, $J[A]$, namely A_{β} , has the following meaning.

We consider a computational process denoted by (A,a) as follows:

1. Suppose

$$a = (a_1, \ldots, a_s, \sigma) \quad . \quad (s \text{ may be infinite})$$

Assign the value $a_x = a_{\kappa(x)}$ to the variable x (identified with

the variable symbol x) as the initial value for each $x \in U$.

2. Execute A from the point labelled by σ , while the leftmost point of A is chosen as the entry if $\sigma = \iota$, and, if $\sigma \notin A^-$ then we consider A has no effect (i.e., identity transformation).

Then the following hold.

If the process (A,a) terminates at the exit whose destination is τ , giving the final value b_x to the variable x for each $x \in U$, then

$$(J[A](a))_x = b_x \quad \text{for each } x \in U$$

and

$$(J[A](a))_\chi = \tau \ ,$$

and vice versa.

If (A,a) terminates at the normal exit, i.e. the rightmost point of A , then

$$(J[A](a))_\chi = \iota \ ,$$

while the relationship concerning the values remains unchanged, and, if (A,a) does not terminate, then J[A] is undefined. The converse are also valid.

Choice of Γ^o

As studied by Manna and McCarthy (1969), the choice of Γ^o is an important problem. We shall assume Γ_ℓ as the foundation hereafter, unless we specify Γ^o . However, it must be noted that all the axiom

schemata of the formal system presented in Section 5 are valid, whichever set of truth tables we may use. From the practical point of view, the process of most implementations are related to Γ_m rather than to Γ_t.

On the other hand, they make no difference in so far as all $f_{\mathfrak{A}}^{(n)}$ and $p_{\mathfrak{A}}^{(n)}$ are total and neither $\forall$ nor $\exists$ is involved, which is also the usual case when we consider actual ALGOL 60 programs which contain no recursive calls of procedures.

Remark

Function J is an extension of J_1 for T_1-statements and J for T_2-statements (Igarashi 1964). For instance, J[A](a) defined above is identical with

$$(J_1[A](a_1,\ldots,a_s),t) \quad .$$

The reader may notice that $|\mathfrak{A}|$ in the present paper corresponds to $\mathfrak{B}$ in that paper, while $\mathfrak{B}$ in this paper is used in a different meaning.

4. Category of Programs

Programs in the General Sense

It seems to be convenient for us to consider more general programs as the background for the treatments of the properties of Algol-like statements. By a program, let us mean a partial function from an arbitrary set to another set together with its denotation. This definition does not exclude those partial functions which cannot be defined effectively. Instead, we shall describe it explicitly whenever the definability or constructiveness matters.

Programs will be denoted by $A,B,C,\ldots$. For each A , $J[A]$ denotes the partial function corresponding to A , and $G[A]$ the graph of $J[A]$. Let D be an Algol-like statement such that $D \in \mathcal{A}_U$, and $(U,\kappa,\mathfrak{R},\Gamma^o,J)$ be an interpretation. Then the pair $(D, (U,\kappa,\mathfrak{R},\Gamma^o,J))$ is a program, for a unique partial function $J[D]$, namely $D_{\mathfrak{B}}$, is determined by it. Therefore we shall assume the interpretation is fixed hereafter, so that each $D \in \mathcal{A}_U$ represents a unique program. Thus we identify an Algol-like statement with the program represented by it, and the set of such programs will be denoted by $\mathcal{A}$.

What we shall do firstly is almost the same as considering a subcategory of $\mathcal{E}ns$ (the category of sets) whose objects are graphs of partial functions. The only difference lies in that the denotations are distinguished in our treatments. For instance, we do not say A and B are identical nor $A = B$, even if $J[A] = J[B]$, while we may say A and B are isomorphic.

Category $\mathcal{Pr}$

Each program will be called an object of category $\mathcal{Pr}$. The class of all the objects, namely programs, is denoted by $Ob\ \mathcal{Pr}$ For each pair A and B belonging to $Ob\ \mathcal{Pr}$, $Hom_{\mathcal{Pr}}(A,B)$ denotes the set of triples of the form (A,ζ,B) such that

$$\zeta : G[A] \to G[B]$$

and that ζ is a total function. The elements of $Hom_{\mathcal{Pr}}(A,B)$ are called morphisms of $\mathcal{Pr}$. If there is no possibility of confusion the morphism (A,ζ,B) will be abbreviated by ζ . We frequently write $\zeta : A \to B$ or $A \xrightarrow{\zeta} B$ instead of $\zeta \in Hom_{\mathcal{Pr}}(A,B)$. If $A \xrightarrow{\xi} B \xrightarrow{\eta} C$, then $(A,\eta\xi,C) \in Hom_{\mathcal{Pr}}(A,C)$ is defined as the composition of morphisms (A,ξ,B) and (B,η,C) , where $\eta\xi$ in $(A,\eta\xi,C)$ denotes the composition of functions ξ and η in the usual sense. Let $id_{G[A]}$ denote the identity function of G[A] onto itself. The morphism $(A,id_{G[A]},A)$ is called the identity morphism of A and is denoted by 1_A .

We shall see that $\mathcal{Pr}$ satisfies the axioms of category as follows:

1. Associativity of Composition. If

$$A \xrightarrow{\xi} B \xrightarrow{\eta} C \xrightarrow{\zeta} D \ ,$$

then $\zeta(\eta\xi) = (\zeta\eta)\xi$ as morphisms.

2. Identity. If $A \xrightarrow{\xi} B$, then $\xi = \xi 1_A$. If $C \xrightarrow{\eta} A$, then $\eta = 1_A\eta$.

3. If the pairs (A_1,B_1) and (A_2,B_2) are distinct, then

$$\mathrm{Hom}_{\mathcal{P}r}(A_1,B_1) \cap \mathrm{Hom}_{\mathcal{P}r}(A_2,B_2) = \phi \ .$$

Category $\mathcal{P}r^{\mathcal{L}}$

Let $\mathcal{P}r^{\mathcal{L}}$ denote the full subcategory of $\mathcal{P}r$ such that $\mathrm{Ob}\,\mathcal{P}r^{\mathcal{L}}$ consists of only those programs A such that

$$\mathrm{Dom}(J[A]) \subseteq |\mathcal{B}^{\mathcal{L}}| \ ,$$

where

$$|\mathcal{B}^{\mathcal{L}}| = \{a \,|\, a \in |\mathcal{B}| \text{ and } a_\chi = \mathcal{L}\} \ . \quad \text{(See the below modification of J.)}$$

For each $A \in \mathrm{Ob}\,\mathcal{P}r^{\mathcal{L}}$ and $B \in \mathrm{OB}\,\mathcal{P}r^{\mathcal{L}}$,

$$\mathrm{Hom}_{\mathcal{P}r^{\mathcal{L}}}(A,B) = \mathrm{Hom}_{\mathcal{P}r}(A,B) \ ,$$

by definition (of full subcategory).

We consider a map:

$$\mathrm{Ob}\,\mathcal{P}r \to \mathrm{Ob}\,\mathcal{P}r^{\mathcal{L}}$$

which sends each $A \in \mathrm{Ob}\,\mathcal{P}r$ onto ${}_{\mathcal{L}}A \in \mathrm{Ob}\,\mathcal{P}r^{\mathcal{L}}$ such that

$$J[{}_{\mathcal{L}}A] = J[A] \Big| |\mathcal{B}^{\mathcal{L}}| \ .$$

That is to say we shall forget computational processes starting from any entry different from the normal one, namely the leftmost point, if A is an Algol-like program, modifying $J[A]$ into $J[A]\Big||\mathcal{B}^{\mathcal{L}}|$.

Hereafter we shall be concerned with $\mathcal{P}r^{\mathcal{L}}$, so that A,B,C,... will be understood as ${}_{\mathcal{L}}A, {}_{\mathcal{L}}B, {}_{\mathcal{L}}C, \ldots$ if the former do not belong to Ob $\mathcal{P}r^{\mathcal{L}}$. Apparently the morphism (A,ζ,B) is a <u>monomorphism</u>, <u>epimorphism</u>, or <u>isomorphism</u>, according as the function ζ is univalent (1-1), onto, or univalent and onto. We shall write $\zeta : A \tilde{\to} B$ or $A \overset{\zeta}{\tilde{=}} B$ to express that $\zeta : A \to B$ is an isomorphism, and $A \tilde{=} B$ to express that there is an isomorphism from A to B, namely A and B are isomorphic.

<u>Value-Preserving Monomorphisms</u>

We pay special attention to such a monomorphism ζ that has the following property:

Suppose $\zeta : A \to B$, and the function $\zeta : G[A] \to G[B]$ sends $(a,b) \in G[A]$ onto $(c,d) \in G[B]$ such that

$$a = c$$

and

$$b_u = d_u \quad \text{for each } u \in X + \{X\},$$

for a subset X of $\mathbb{U}$, for any $a \in |\mathcal{B}^{\mathcal{A}}|$.

In such a case, ζ (as a morphism and as a function) will be said to preserve the values of X, or to <u>preserve</u> X, and we shall frequently write ζ_X instead of ζ in order to indicate that ζ preserves X. Moreover, if the choice of ζ itself does not matter, we write $A \overset{\cdot}{\tilde{\to}}_X B$ instead of $\zeta_X : A \to B$. Similarly we shall frequently write $A \overset{\cdot}{\tilde{\to}}_X B$ or $A \overset{\cdot}{\tilde{=}}_X B$ instead of $\zeta_X : A \tilde{=} B$, and $A \tilde{=} B$ instead of $\zeta_U : A \tilde{=} B$, that is $A \overset{\cdot}{\tilde{=}}_U B$.

Remarks

(i) $A \vec{X} B \vec{Y} C$ implies $A \underset{X\cap Y}{\rightarrow} C$.

(ii) $\xi_X \zeta = \eta_Y$ implies that ζ preserves $X \cap Y$.

(iii) $\zeta \xi_X = \eta_Y$ implies that the function $\zeta | \mathrm{Im}\ \xi_X$ preserves $X \cap Y$.

(iv) $\eta_Y \xi_X = 1_A$ implies that ξ and η both preserve $X \cup Y$.

(v) In an arbitrary category $\mathcal{C}$, a morphism γ is an isomorphism if and only if there exists a morphism δ and $c, d \in \mathrm{Ob}\ \mathcal{C}$ such that

$$\delta\gamma = 1_c \quad \text{and} \quad \gamma\delta = 1_d .$$

Such a δ is unique and usually denoted by γ^{-1} .

Proposition 1. If $A \vec{X} B$ and $B \vec{Y} A$, then $A \overset{\sim}{X \cup Y} B$.

Proof. By definition of $\vec{X}$, there exists $\xi_X : A \rightarrow B$. Then,

$$\xi_X(a, J[A](a)) = (a, J[B](a)) \quad \text{for any } a \in \mathrm{Dom}\, J[A] ,$$

because the right side is the unique element of the form (a,b) belonging to $G[B]$. Similarly there exists $\eta_Y : B \rightarrow A$ such that

$$\eta_Y(a, J[B](a)) = (a, J[A](a)) \quad \text{for any } a \in \mathrm{Dom}\, J[B] .$$

Thus ξ_X is an isomorphism, for $\eta_Y \xi_X = 1_A$ and $\xi_X \eta_Y = 1_B$ (cf. Remark (v)). Besides, ξ preserves $X \cup Y$, by Remark (iv).

Q.E.D.

Proposition 2. $A \overset{\cong}{X} B$ if and only if $A \vec{X} B$ and $B \vec{X} A$.

Proof. Sufficiency: Apparent from Proposition 1.

Necessity: If $A \overset{\cong}{X} B$, there exists $\zeta_X : A \to B$ and $\zeta^{-1} : B \to A$ such that $\zeta^{-1}\zeta_X = 1_A$ (cf. Remark (v)). ζ^{-1} preserves X, by Remark (iv).

Q.E.D.

For each $A \in \mathcal{A}$ and $B \in \mathcal{A}$, these value-preserving monomorphisms or isomorphisms have the practical meanings listed below. The reader may recall that ${}_{\mathcal{L}}A$ is understood whenever A denotes such a program that $\mathrm{Dom}\, J[A] \subseteq |\mathcal{D}^{\mathcal{L}}|$ is not satisfied.

1. Relation $\vec{X}$.

The following relationships are equivalent with each other.

(a) $A \vec{X} B$.

(b) $\mathrm{Dom}\, J[A] \subseteq \mathrm{Dom}\, J[B]$, and for any $a \in \mathrm{Dom}\, J[A]$,

$$(J[A](a))_u = (J[B](a))_u \quad \text{for each } u \in X + \{X\}.$$

(c) For each $a \in |\mathcal{D}^{\mathcal{L}}|$, if the process (A,a) (see Section 3) terminates with the result b, $b \in |\mathcal{D}|$, then the process (B,a) terminates with the result c satisfying

$$b_x = c_x \quad \text{for each } x \in X,$$

namely the values of variables coincide variable-wise, and

$$b_X = c_X,$$

namely the destinations of the exits are identical.

2. Relation $\vec{\phi}$.

The relationship $A \vec{\phi} B$ holds if and only if the following conditions are satisfied.

If (A,a) terminates, then (B,a) terminates for any $a \in |\mathcal{D}^{\nu}|$.

Besides, the destinations of the exits are identical.

3. Relation $\tilde{\vec{X}}$.

The following relationships are equivalent with each other.

(a) $A \tilde{\vec{X}} B$.

(b) $A \vec{X} B$ and $B \vec{X} A$, or, by Proposition 1, $A \vec{X} B$ and $B \vec{\phi} A$.

(c) $\mathrm{Dom}\, J[A] = \mathrm{Dom}\, J[B]$,

and, for any $a \in \mathrm{Dom}\, J[A]$,

$$(J[A](a))_u = (J[B](a))_u \quad \text{for each } u \in X + \{x\} .$$

(d) The process (A,a) terminates if and only if (B,a) terminates, and the same conditions as 1(c) above are satisfied by the results of these processes.

4. Strong Equivalence and Ordering.

The relationship $A \cong B$ holds if and only if A and B are strongly equivalent in the usual sense. The relationship $A \vec{U} B$ holds if and only if $J[A] \leq J[B]$ in the natural ordering of partial functions, namely $\varphi \leq \psi$ if and only if φ is a restriction of ψ . $A \tilde{\cong} B$ if and only if $A \vec{U} B$ and $B \vec{U} A$, which are still weaker than $J[A] = J[B]$

in the original sense of J[A] and J[B], being equivalent to $J[_{\iota}A] = J[_{\iota}B]$, i.e.,

$$A_{\beta}\Big|\,|\mathcal{D}^{\iota}| = B_{\beta}\Big|\,|\mathcal{D}^{\iota}| \ .$$

5. Correctness.

Firstly, the concept of correctness of programs introduced by Floyd (1967) and extended by Manna (1969) will be explained in our notation so that the comparison becomes easier. Manna's definitions are as follows:

Program A is said to be <u>partially correct w.r.t.</u> predicates p_{β} and q_{β} if and only if

$$p_{\beta}(a) = T \ \text{ implies } \ q_{\beta}(J[A](a)) = T \ , \ \text{for any } \ a \in \mathrm{Dom}\, J[A] \ . \qquad (1)$$

Program A is said to be <u>correct w.r.t.</u> p_{β} and q_{β} if and only if

$$p_{\beta}(a) = T \ \text{ implies } \ a \in \mathrm{Dom}\, J[A] \ , \qquad (2)$$

besides (1) above.

Let δ denote either σ or $\sigma^{-1}\sigma$ for an arbitrary σ such that $\sigma \notin A^{+}$. Then, apparently, (1) and (2) are equivalent to the following relationships in this order.

$$(p \to A,\delta) \underset{\beta}{\simeq} (p \to A;(q \to \Lambda,\delta),\delta) \ . \qquad (1')$$

$$(p \to A,\delta) \underset{\phi}{\simeq} (p \to \Lambda,\delta) \ . \qquad (2')$$

6. Representations of $\vec{\underset{X}{}}$ and $\tilde{\underset{X}{}}$ by $\tilde{=}$.

Since we shall consider a formal system which represents (although incompletely) the concept of <u>equivalence</u>, namely relations $\tilde{\underset{X}{}}$ and $\tilde{=}$, we shall see that $\vec{\underset{X}{}}$ and $\tilde{\underset{X}{}}$ can be defined by $\tilde{=}$, here. We shall use, however, $\tilde{\underset{X}{}}$ as well as $\tilde{=}$ in the formal system because of its practical applicability.

Let $\Sigma^{x_1 \ldots x_n}(f_1,\ldots,f_n)$ denote the statement

$$x_1 := f_1 \;;\ldots;\; x_n := f_n \;.$$

Relationship $A \tilde{\underset{X}{}} B$ holds if and only if

$$A;\Sigma^{t_1 \ldots t_m}(c,\ldots,c) \;\tilde{=}\; B;\Sigma^{t_1 \ldots t_m}(c,\ldots,c) \quad ,$$

for an arithmetic expression c such that $V[c] = \phi$ and $t_1,\ldots,t_m$ such that $\{t_1,\ldots,t_m\} = V[A] \cup V[B] - X$.

Relationship $A \vec{\underset{X}{}} B$ holds if and only if

$$A \tilde{\underset{X}{}} \Sigma^{v_1 \ldots v_n}(u_1,\ldots,u_n) \;;\; (A\sigma_1^{-1} \ldots \sigma_k^{-1})' \;;\; \Sigma^{u_1 \ldots u_n}(v_1,\ldots,v_n) \;;\; B \;,$$

where the following conditions are satisfied:

$$\{u_1,\ldots,u_n\} = V[A] \cap V[B] \;.$$

$$\{v_1,\ldots,v_n\} \cap (V[A] \cup V[B] \cup X) = \phi \;.$$

$$\{\sigma_1,\ldots,\sigma_k\} = A^{++} \quad .$$

$(A\sigma_1^{-1}\ldots\sigma_k^{-1})'$ is a copy of $A\sigma_1^{-1}\ldots\sigma_k^{-1}$ (see Section 2) such that $(A\sigma_1^{-1}\ldots\sigma_k^{-1})'^{\pm} \cap B^{\pm} = \phi$.

Inductive Limits

The concept of inductive limits is useful in $\mathfrak{Pr}$ and $\mathfrak{Pr}^{\mathcal{L}}$. For instance, we can frequently use the following method in order to prove $A \overline{\overline{\mathcal{Z}}} B$.

We find two sequences of programs $(A_i)_{i\in\eta}$ and $(B_i)_{i\in\eta}$ with morphisms such as

$$\xi_X^{ij} : A_i \to A_j \ ,$$

$$\eta_Y^{ij} : B_i \to B_j \ ,$$

$$(A, \xi_X^i) = \varinjlim (B_i, \eta_X^{ij}) \ ,$$

and

$$\xi_Z^i : A_i \to B_i \ ,$$

for each $i\in\eta$ and $j\in\eta$. This is a sufficient condition for a ζ such that $\zeta : A \to B$ and that ζ preserves X to exist. If p and q contradict each other, then $(p \to A, (q \to B, \Delta))$ is a sum of $(p \to A, \Delta)$ and $(q \to B, \Delta)$, in the sense of the terminology of category, being a special case of inductive limit, where Δ is a statement of the form $\sigma^{-1}\sigma$ such that $\sigma \notin A^{\pm} \cup B^{\pm}$ and $A^{++} \cap B^{-} = A^{-} \cap B^{++} = \phi$. This fact may be considered as a justification of writing $p\cdot A + \bar{p}\cdot B$ instead of $(p \to A, B)$ conveniently used in the proof of the completeness of L.3 by Igarashi (1964).

5. Formal System Representing the Equivalence of Statements

Well-formed Formulas

For two arbitrary Algol-like statements A and B belonging to $\mathcal{A}_U$ and an arbitrary subset X of U,

$$A \cong B$$

and

$$A \overset{\sim}{\underset{X}{}} B$$

are well-formed formulas, or wffs. (cf. Intended Interpretation below.)

Substitution Rules

In the following schemata of axioms and inference rules, arbitrary statements; variable symbols; label symbols; arithmetic expressions; Boolean expressions; and sets of variable symbols can be substituted in place of $A,B,C,\ldots$; x,y,z ; $\sigma,\sigma_1,\ldots,\ \tau,\tau_1,\ldots$; $f,g,\ldots$; $p,q,r,\ldots$; and $X,Y,Z,\ldots$; respectively, provided that the results of such substitutions constitute wffs, and that all the restrictions imposed on the schemata, immediately following each schema, are fulfilled.

An arbitrary copy of the statement that is substituted in place of C can be substituted in place of C' in Axiom 12; any other occurrence of substitution operator indicated by brackets should be treated similarly; and an arbitrary statement of the form $\sigma^{-1}\sigma$ can be substituted in place of Δ ; with the same proviso as the above.

A schema of wffs $\mathcal{S}(i)$ in which i occurs as index of statements should be replaced by the line of the form

$$\mathcal{B}(1) \ \ldots \ \mathcal{B}(\nu)$$

before any other substitution, where $\nu \in \eta$ and ν should be substituted in place of n occurring in the restrictions.

The symbol 1 stands for a nullary predicate symbol such that $1_{\mathcal{R}} = T$. Similarly $0_{\mathcal{R}} = F$.

The formulas in the sense of predicate calculus that are obtained after the substitutions of the symbols $f,g,\ldots$, $p,q,\ldots$ and that constitute a part of restriction, except those expressions containing set-theoretic symbols, should be interpreted in one of the following ways:

(I) Let $\mathcal{A}$ be a formula (in the sense of predicate calculus) that contains exactly n variables such as $x_1,\ldots,x_n$. Then, we consider that the restriction expressed by $\mathcal{A}$ is satisfied if and only if

$$(\forall x_1 \ldots \forall x_n \mathcal{A})_{\mathcal{B}} = T \ .$$

(II) We presuppose an axiom system Γ (or theory) that is consistent (and semantically complete, preferably) and that contains all the symbols belonging to $\mathfrak{F}$ or $\mathfrak{P}$ and the two symbols $=$ and $\blacktriangledown$. Then, we consider the restriction expressed by $\mathcal{A}$, as above, is satisfied if and only if

$$\vdash_{\Gamma} \mathcal{A} \ .$$

In the both methods, logical connectives occurring in the restrictions before substitutions should be read as the connectives of $\Gamma_{\mathcal{L}}$, and

$\varphi = \psi$ interpreted as either both sides are defined and equal, or both sides are undefined.

Remark

Since semantically complete axiom systems do not always exist, we have to note (I).

Axioms and Theorems

Any wff that is a result of substitution into an axiom schema is an axiom. An axiom is a theorem. If

$$\frac{\mathfrak{F}_1 \cdots \mathfrak{F}_n}{\mathfrak{F}}$$

is a result of substitution into an inference rule schema, and $\mathfrak{F}_1, \ldots, \mathfrak{F}_n$ are theorems, then $\mathfrak{F}$ is also a theorem. All the theorems are defined to be so only by these rules. We shall frequently write

$$\vdash \mathfrak{F}$$

to mean that $\mathfrak{F}$ is a theorem.

Asterisks are used to emphasize a certain restriction, for the readability's sake, so that they are not parts of the formal system. Index like (Ia^*), (IIIm^*), etc. indicates that the same axiom or inference rule was used and indexed by Ia, IIm, etc. by Igarashi (1964), for the convenience of comparison.

Special Substitution

In the following schemata of axioms and inference rules, any occurrence of $\simeq$ can be replaced by $\tilde{=}$, and vice versa.

Axioms and Inference Rules

Axiom 1.(a) $(AB)C \cong A(BC)$.

(b) $\sigma((AB)C) \cong \sigma(A(BC))$.

Axiom 2.(a) $A\Lambda \cong A$.

(b) $\Lambda A \cong A$. (Ie^{+})

Axiom 3.(a) $\sigma^{-1} \cong \Lambda$.

(b) $\sigma\sigma^{-1} \cong \Lambda$.

Axiom 4. $\sigma A \cong \sigma$.

$o \notin A^{-}$.

Axiom 5. $A\Delta \cong \Delta$.

$A^{++} = \emptyset$.

Axiom 6. $x := x \cong \Lambda$. (Ia^{+})

Axiom 7.(a) $x := f;A;x := g \cong A_x[f]^{o};x := g_x[f]^{o}$. (Ib^{+})

$A^{++} = \emptyset$.

$L[A] \cap (V[f] \cup \{x\}) = \emptyset$.

(b) $x := f;A;y := g \cong x := f;A_x[f];y := g_x[f]$. (Ic^{+})

x and y are distinct.

$L[A] \cap (V[f] \cup \{x\}) = \emptyset$.

$x \notin V[f]$.

Axiom 8. $A \overset{\sim}{\underset{X}{=}} \Lambda$. (Id$^+$)

$L[A] \cap X = \emptyset$.

$A^{++} = \emptyset$.

$A^{-+} = \emptyset$.

Every function or predicate symbol occurring in A represents a total function or predicate, by the interpretation.

Axiom 9. $(1 \rightarrow A,B) \cong A$. (IIIm$^+$)

Axiom 10. $(p \rightarrow A,B) \cong (\neg p \rightarrow B,A)$. (IIIo$^+$)

Axiom 11.(a) $(p \rightarrow (q \rightarrow A,B),C) \cong (p \wedge q \rightarrow A,(p \wedge \neg q \rightarrow B,C))$. (IIIp$^+$)

(b) $(p \rightarrow (q \rightarrow A,B),C) \cong (p \rightarrow \Delta,C)$.

$p \supset \nabla q$.

Axiom 12.(a) $(p \rightarrow A,B)C \cong (p \rightarrow AC,BC')$. (IIIu$^+$)

(b) $\sigma(p \rightarrow A,B)C \cong \sigma(p \rightarrow AC,BC')$.

$\sigma \not\in C'^-$.

Axiom 13. $x := f;(p \rightarrow A,B) \cong (p_x[f]^* \rightarrow x := f;A,x := f;B)$. (IIIt$^+$)

* If $x \in V[f]$, then $p_x[f]$ is restricted to be $p_x[f]^\circ$.

Axiom 14. $(p \rightarrow A,B) \cong (p \rightarrow A_C[(p \rightarrow C,D)],B)$.

$L[A] \cap V[p] = \emptyset$.

Axiom 15.(a) $(p \to x := f, A) \cong (p \to x := g, A)$.

$p \supset f = g$.

(b) $(p \to x := f, A) \cong (p \to \Delta, A)$.

$p \supset \blacktriangledown f$.

Axiom 16.(a) $A \cong A_f[g]$.

$f = g$.

(b) $A \cong A_p[q]$.

$p \equiv q$.

Inference Rule 1.

$$\frac{A \overset{\cong}{X} B}{B \overset{\cong}{X} A} \quad . \qquad (Ij^+)$$

Inference Rule 2.

$$\frac{A \overset{\cong}{X} B \quad B \overset{\cong}{X} C}{A \overset{\cong}{X} C} \quad . \qquad (Ik^+)$$

Inference Rule 3.

$$\frac{A \overset{\cong}{X} B \quad A \overset{\cong}{Y} B}{A \overset{\cong}{Z} B} \quad .$$

$Z \subseteq X \cup Y$.

Inference Rule 4.

$$\frac{(p \to A,C) \mathrel{\tilde{\tilde{X}}} (p \to B,C) \quad (q \to A,D) \mathrel{\tilde{\tilde{X}}} (q \to B,D)}{(r \to A,E) \mathrel{\tilde{\tilde{X}}} (r \to B,E)} \ .$$

$$r \supset p \vee q \ .$$

Inference Rule 5. (a)

$$\frac{\sigma A \cong \tau B}{C \cong C_{\sigma}[\tau]} \ .$$

A and B end with go-tos.

A and B occur in C .

(b)

$$\frac{\sigma A \cong B}{C \cong C_{\sigma}[B]} \ .$$

B ends with a go-to.

A occurs in C , or, A is $C_{A_1 \ldots A_n}[\Lambda,\ldots,\Lambda]$, where $A_1,\ldots,A_n$ are preceded by go-tos in C .

Inference Rule 6.

$$\frac{A \mathrel{\tilde{\tilde{X}}} B}{AC \mathrel{\tilde{\tilde{X} \cup L[C]}} BC} \ .$$

$R[C] \subseteq X$.

$C^{++} \cap A^{-} = C^{++} \cap B^{-} = \emptyset$.

Inference Rule 7.

$$\frac{A \underset{X}{\cong} B^{*} \quad \sigma_i A \underset{X}{\cong} \sigma_i B}{CA \underset{X}{\cong} CB} \ .$$

$$C^{++} \cap A^{-} = C^{++} \cap B^{-} = \{\sigma_1, \ldots, \sigma_n\} \ .$$

$$A^{++} \cap C^{-} = B^{++} \cap C^{-} = \emptyset \ .$$

* If C ends with a go-to, or A and B both begin with labellings, then the upper left formula may be omitted, provided that $n \geq 1$.

Inference Rule 8.

$$\frac{A \cong B^{*} \quad \sigma_i A \cong \sigma_i B}{C \cong C_A[B]} \ . \qquad (\mathrm{IVg}^{+})$$

$$C_A[\Lambda]^{++} \cap A^{-} = C_A[\Lambda]^{++} \cap B^{-} = \{\sigma_1, \ldots, \sigma_n\} \ .$$

* Same as above.

Inference Rule 9.

$$\frac{D^i A \cong A^i A \quad \tilde{D}^i B \cong B^i B \quad A^i_{\sigma_1 \ldots \sigma_n}[\tilde{\sigma}_1, \ldots, \tilde{\sigma}_n]^{0} \underset{X}{\cong} B^i \quad B^i \underset{X}{\cong} C^i}{D^k A \underset{X}{\cong} \tilde{D}^k B} \ .$$

$$k \in [n] \ .$$

1. The set $S = \{\sigma_1,\ldots,\sigma_n\}$ is a non-empty subset of A^-, and a total function

$$\zeta : S \to \mathfrak{L}$$

sends each σ_i onto $\tilde{\sigma}_i$. ζ, together with S, satisfies the following conditions:

$$S \supseteq S'$$

and

$$\zeta(\sigma) = \sigma \qquad \text{for each } \sigma \in S \cap S'',$$

where

$$S' = \bigcup_i (A^i)^{++} \cap A^-$$

and

$$S'' = \bigcup_i (A^i)^{++} \cap A^{++} .$$

2. The following conditions are satisfied for each $i \in [n]$.

   (i) D^i is of the form $(p_i \to \sigma_i, \delta^i)$ and $\tilde{D}^i$ is of the form $(p_i \to \tilde{\sigma}_i, \delta^i)$, where δ^i is either τ_i or $\tau_i^{-1}\tau_i$ such that $\tau_i \notin A^{\pm} \cup B^{\pm}$.

   (ii) All the occurrences of σ_i in $A^1,\ldots,A^n$ are within the statements of the form $(p_i \to \sigma_i, \varepsilon^i)$, or all the occurrences of $\tilde{\sigma}_i$ in $B^1,\ldots,B^n$ are within the statements of the form $(p_i \to \tilde{\sigma}_i, \varepsilon^i)$ where ε^i subjects to the same restriction as δ^i above.

   (iii) $R[C^i] \subseteq X$.

3. If A does not begin with a labelling σ^{-1} such that $\sigma \in S$, then all of $A^1,\ldots,A^n$ must end with go-tos. If B does not begin with a labelling σ^{-1} such that $\sigma \in \zeta(S)$, then all of $B^1,\ldots,B^n$ must end with go-tos.

Intended Interpretation

A wff of the form

$$A \tilde{\equiv}_X B$$

will be interpreted as the relationship $A \tilde{\equiv}_X B$ in the sense of category ρr^{ι} (see Section 4). Similarly, wff

$$A \cong B$$

will be interpreted as the relationship $A \cong B$ in ρr^{ι}.

Intuitively, it seems to be obvious that $\vdash A \tilde{\equiv}_X B$ always implies that relationship $A \tilde{\equiv}_X B$ in ρr^{ι} holds so that the above system is consistent. We shall not verify the consistency, however, in the present paper, for which presumably the constructive definition of J will suffice. (See Section 3.)

6. Elementary Metatheorems

Index such as (Th. 3^{+}) shows the number of the same theorem for the formal systems treated by Igarashi (1964). The results of this section imply that every axiom of L.4 in that paper becomes a theorem in the present system and that for every rule of inference of L.4 such as

$$\frac{\mathfrak{F}_1 \cdots \mathfrak{F}_n}{\mathfrak{F}}$$

the following holds:

$$\text{If } \vdash \mathfrak{F}_1, \ldots, \vdash \mathfrak{F}_n, \text{ then } \vdash \mathfrak{F} .$$

Therefore every theorem concerning completeness in that paper holds also for the present formal system.

Theorem 1. (Reflexivity)

$$\vdash A \underset{X}{\cong} A . \qquad \text{(Th. } 3^{+}\text{)}$$

Proof.

$A\Lambda \cong A$. (Ax. 2a) (1)

$A \cong A\Lambda$. (Inf. 1, (1)) (2)

$A \cong A$. (Inf. 2, (1), (2)) (3)

$A \underset{X}{\cong} A$. (Inf. 3, (3))

Q.E.D.

Thus $\overset{\simeq}{\underset{X}{}}$ satisfies the equivalence law formally, the symmetricity and the transitivity being Inf. 1 and Inf. 2.

Theorem 2.

If $\vdash A_1 \overset{\simeq}{\underset{X_1}{}} A_2$, ..., $\vdash A_{n-1} \overset{\simeq}{\underset{X_{n-1}}{}} A_n$, then $\vdash A_1 \overset{\simeq}{\underset{X}{}} A_n$, for any X such that $X \subseteq \bigcap_{i\in[n]} X_i$.

Proof. A repeated use of Inf. 3 and Inf. 2.

Q.E.D.

Theorem 3.

$\vdash (0 \rightarrow A,B) \cong B$. (Th. 25^+, cf. McCarthy (1963a))

Proof. $(0 \rightarrow A,B) \cong (\neg 1 \rightarrow A,B)$ (Axiom 16b)

$\cong (1 \rightarrow B,A)$ (Axiom 10)

$\cong B$. (Axiom 9)

Q.E.D.

Theorem 4.

If $\underset{\Gamma}{\vdash} p \vee \neg p$, then

$\vdash (p \rightarrow A,A) \cong A$. (IIIn$^+$, cf. McCarthy (1963a))

Proof. $(p \rightarrow (p \rightarrow A,A),\Lambda) \cong (p \wedge p \rightarrow A,(p \wedge \neg p \rightarrow A,\Lambda))$ (Axiom 11a)

$\cong (p \rightarrow A,(0 \rightarrow A,\Lambda))$ (Axiom 16b)

$\cong (p \rightarrow A,\Lambda)$. (Theorem 3, Inf. 8) (1)

Similarly,

$$\vdash (\neg p \to (p \to A,A),\Lambda) \cong (\neg p \to A,\Lambda) \quad . \qquad (2)$$

Thus,

$$(p \vee \neg p \to (p \to A,A),\Lambda) \cong (p \vee \neg p \to A,\Lambda) \quad .$$

((1), (2), Inf. 4)

The premise of the theorem, Axiom 16b, and Axiom 9 give the conclusion.

Q.E.D.

The premise of Theorem 4, being the law of the excluded middle, holds if $p_{\mathcal{B}}$ is total and Γ is semantically complete. (See Section 5 method (II).)

Theorem 5.

$$\vdash (p \to A,(q \to B,C)) \cong (p \to A,(\neg p \wedge q \to B,C)) \quad , \qquad (IIIq^{+})$$

with the same premise as Theorem 4.

Proof.

$$(p \to A,(q \to B,C)) \cong (\neg p \to (q \to B,C),A) \qquad \text{(Axiom 10)}$$

$$\cong (\neg p \wedge q \to B,(\neg p \wedge \neg q \to C,A)) \quad . \qquad \text{(Axiom 11a)} \qquad (1)$$

$$(p \to A,(\neg p \wedge q \to B,C)) \cong (\neg p \to (\neg p \wedge q \to B,C),A) \qquad \text{(Axiom 10)}$$

$$\cong (\neg p \wedge \neg p \wedge q \to B,(\neg p \wedge \neg(\neg p \wedge q) \to C,A)) \qquad \text{(Axiom 11a)}$$

$$\cong (\neg p \wedge q \to B,(\neg p \wedge \neg q \to C,A)) \quad . \qquad \text{(Axiom 16b)} \qquad (2)$$

Statements (1) and (2) are identical.

Q.E.D.

The above also implies that Axiom IIq of L.2 in the previous paper was dependent on others.

Theorem 6.

If $\vdash_\Gamma f = g$, then

$$\vdash x := f \cong x := g \quad . \qquad (If^+)$$

Proof. A special case of Axiom 16a.

Q.E.D.

Theorem 7.

If $\vdash_\Gamma p \supset f = g$, then

$$\vdash (p \to x := f;A,B) \cong (p \to x := g;A,B) \quad . \qquad (IIIv^+)$$

Proof. $(p \to x := f,\Lambda) \cong (p \to x := g,\Lambda)$. (Axiom 15a)

Right multiplying both sides by A ,

$$(p \to x := f;A,A') \cong (p \to x := g;A,A') \quad . \qquad \text{(Axiom 12a)}$$

By Inf. 4,

$$(p \to x := f;A,B) \cong (p \to x := g;A,B) \quad .$$

Q.E.D.

Theorem 8.

If $\vdash_\Gamma p \equiv q$, $\vdash A \overset{=}{X} B$, and $\vdash C \overset{=}{X} D$, then

$$\vdash (p \to A,C) \overset{=}{X} (q \to B,D) \quad . \qquad (IIIs^+)$$

Proof. $(p \to A,C) \overset{\simeq}{\underset{X}{}} (p \to B,C)$ (Inf. 4, premise)

$\simeq (\neg p \to C,B)$ (Axiom 10)

$\overset{\simeq}{\underset{X}{}} (\neg p \to D,B)$ (Inf. 4, premise)

$\simeq (p \to B,D)$ (Axiom 10)

$\simeq (q \to B,D)$. (Axiom 16b)

By Theorem 2,

$$(p \to A,C) \overset{\simeq}{\underset{X}{}} (q \to B,D) \quad .$$

Q.E.D.

Theorem 9.

If $\vdash A \overset{\simeq}{\underset{X}{}} B$ and $\vdash A \overset{\simeq}{\underset{Y}{}} B$, then

$$\vdash A \underset{X \cup Y}{\simeq} B \quad . \qquad (\mathrm{Ih}^{+})$$

Proof. A special case of Inf. 3.

Q.E.D.

Theorem 10.

If $\vdash A \underset{X \cup Y}{\simeq} B$, then

$$\vdash A \overset{\simeq}{\underset{X}{}} B \quad . \qquad (\mathrm{Ii}^{+})$$

Proof. A special case of Inf. 3.

Q.E.D.

Theorem 11. (Superfluous Labels)

If $\sigma \notin A^+ \cup B^-$, then $\vdash AB \cong A\sigma^{-1}B$. (IVa$^+$)

Proof. $\Lambda \cong \sigma^{-1}$. (Axiom 3a) (1)

$A \Lambda B \cong A\sigma^{-1}B$. (Inf. 8, (1)) (2)

$A \cong A\Lambda$. (Axiom 2a) (3)

$\sigma A \cong (\sigma A)\Lambda$ (Axiom 2a)

$\cong \sigma(A\Lambda)$. (Axiom 1a) (4)

By Inf. 8 with (3) and (4),

$AB \cong A \Lambda B$. (5)

By (2) and (5),

$AB \cong A\sigma^{-1}B$.

Q.E.D.

Theorem 12. (Disconnected Statements)

If $\sigma \notin B^-$ and $A^+ \cap B^- = \emptyset$, then

$\vdash A\sigma B \cong A\sigma$. (IVb$^+$)

Proof. $\sigma B \cong \sigma$. (Axiom 4, premise) (1)

Also the premise implies that $A^+ \cap (\sigma B)^- = A^+ \cap (\sigma)^- = \emptyset$, so that

$A(\sigma B) \cong A\sigma$. (Inf. 8, (1))

Q.E.D.

Theorem 13. (Superfluous Go-Tos)

$$\vdash A \cong A_{\sigma^{-1}}[\sigma\sigma^{-1}] \quad .$$

Proof. For any τ ,

$$\tau\sigma^{-1} \cong \tau\sigma\sigma^{-1}$$

$$\cong \begin{cases} \Lambda & \tau = \sigma \\ \tau & \text{otherwise,} \end{cases} \qquad (1)$$

because the formula

$$\sigma\sigma \cong \sigma \qquad \text{(Theorem 12)}$$

and Inf. 8 give

$$(\sigma\sigma)\sigma^{-1} \cong \sigma\sigma^{-1} \quad .$$

Inf. 8 with (1) gives the conclusion.

Q.E.D.

Theorem 14. (Additional Exits)

If $\vdash A\sigma \cong B\sigma$ for a σ such that $\sigma \notin A^{\pm} \cup B^{\pm}$, then

$$\vdash A \cong B \quad . \qquad (IVf^{+})$$

Proof. Right multiplying both sides of the first formula by σ^{-1} , we obtain

$$A\sigma\sigma^{-1} \cong B\sigma\sigma^{-1} \quad . \qquad \text{(Inf. 6)}$$

By the premise concerning σ and Inf. 8,

$$A \cong B \quad .$$

Q.E.D.

Theorem 15. (Copies)

$$\vdash A \cong A' \quad . \qquad (\text{Th. } 41^{+})$$

Proof. (1) The case that $A^{\pm} \cap (A')^{-} = \emptyset$ will be proved firstly. Suppose $A^{\pm} - A^{++} = \{\alpha_1,\ldots,\alpha_n\}$ and A' is $A_{\alpha_1\ldots\alpha_n\alpha_1^{-1}\ldots\alpha_n^{-1}}[\beta_1,\ldots,\beta_n,\beta_1^{-1},\ldots,\beta_n^{-1}]^{\circ}$. Let B be $A_{\alpha_1\ldots\alpha_n\alpha_1^{-1}\ldots\alpha_n^{-1}}[\alpha_1^{-1}\beta_1^{-1}\gamma_1\gamma_1^{-1},\ldots,\alpha_n^{-1}\beta_n^{-1}\gamma_n\gamma_n^{-1}]$, where $\gamma_i \notin A^{\pm} \cup B^{\pm}$ for any $i\in[n]$. Then

$$\vdash A \cong B \quad . \qquad (\text{Theorems 11 and 13}) \qquad (1)$$

But

$$\vdash B \cong B_{\alpha_i}[\beta_i] \qquad \text{for each occurrence of } \alpha_i \ , \qquad (2)$$

because $\alpha_i^{-1}\beta_i^{-1}\gamma_i$ occurs in B, for which

$$\alpha_i(\alpha_i^{-1}\beta_i^{-1}\gamma_i) \cong \beta_i(\alpha_i^{-1}\beta_i^{-1}\gamma_i) \cong \gamma_i \quad , \qquad (\text{Axiom 3b, Theorems 11, 13})$$

so that Inf. 5a gives (2). Since the number of occurrences of α_i in B is finite,

$$\vdash B \cong B_{\alpha_1\ldots\alpha_n}[\beta_1,\ldots,\beta_n]^{\circ} \qquad (3)$$

by the repeated use of (2). But the right side of (3) is

$$A'_{\beta_1^{-1}\ldots\beta_n^{-1}}[\alpha_1^{-1}\beta_1^{-1}\gamma_1\gamma_1^{-1},\ldots,\alpha_n^{-1}\beta_n^{-1}\gamma_n\gamma_n^{-1}]$$

by definition of A' , so that

$$\vdash (3) \cong A' \quad , \tag{4}$$

similarly to (1). Formulas (1), (3) and (4) give

$$A \cong A' \quad .$$

(ii) The case that $A^{+} \cap (A')^{-} \neq \emptyset$ is reduced to (i) as follows:

Consider another copy A'' of A for which $A^{\pm} \cap (A'')^{-} = \emptyset$ and $(A')^{\pm} \cap (A'')^{-} = \emptyset$. Then $\vdash A \cong A''$ and $\vdash A' \cong A''$ according to (i), so that $\vdash A \cong A'$.

Q.E.D.

Theorem 16. (Operating σ (1))

If B occurs in A and ends with a go-to, and $\sigma \epsilon B^{-}$, then

$$\vdash \sigma A \cong (\sigma B)'A \quad .$$

Proof. $\vdash \sigma B \cong (\sigma B)'$ by Theorem 15. $(\sigma B)'$ ends with a go-to, so that

$$\sigma A \cong (\sigma A)_{\sigma}[(\sigma B)'] \qquad \text{(Inf. 5a)}$$

$$\cong (\sigma B)'A \quad .$$

Q.E.D.

Theorem 17. (Operating σ (2))

If $\sigma A_{B_1 \ldots B_n}[A, \ldots, A]$ ends with a go-to, and, $B_1, \ldots, B_n$ are preceded by go-tos in A , then

$$\vdash \sigma A \cong (\sigma A_{B_1 \ldots B_n}[\Lambda,\ldots,\Lambda])'A \ ,$$

for any σ such that $\sigma \notin \bigcup_{i\in[n]} B_i$.

Proof. Similar to the above, while we notice the latter alternative in the restrictions of Inf. 5b.

Q.E.D.

Theorem 18.

If

$$\vdash \sigma_i A \cong A^i A \qquad \text{for each } i\in[n]$$

and

$$\vdash \sigma_i B \cong A^i B \qquad \text{for each } i\in[n] \ ,$$

for a subset $S = \{\sigma_1,\ldots,\sigma_n\}$ of A^- such that $S \supseteq S'$, where

$$S' = \bigcup_{i\in[n]} (A^i)^{++} \cap A^- \ ,$$

and each A^i ends with a go-to, then

$$\vdash \sigma_i A \cong \sigma_i B \qquad \text{for any } i\in[n] \ .$$

Proof. Let D^i be $(1 \to \sigma_i,\tau)$, where $\tau \notin A^{\pm} \cup B^{\pm}$, and $\hat{A}^i$ be $A^i_{\sigma_1\ldots\sigma_n}[D^1,\ldots,D^n]^\circ$, for each $i\in[n]$. Then,

$$\begin{aligned} D^i A &\cong \sigma_i A && \text{(Axiom 9, Inf. 6)} \\ &\cong A^i A && \text{(premise)} \\ &\cong \hat{A}^i B \ . && \text{(repeat Inf. 8, Axiom 9)} \qquad (1) \end{aligned}$$

Similarly,

$$D^i B \simeq \hat{A}^i B \quad . \tag{2}$$

In order to use Inf. 9, σ_i is defined as $\tilde{\sigma}_i$, and $\hat{A}^i$ is substituted in place of A^i, B^i, and C^i of that schema. The left two schemata of wffs become (1) and (2), and the right two

$$\hat{A}^i_{\sigma_1 \ldots \sigma_n}[\tilde{\sigma}_1, \ldots, \tilde{\sigma}_n] \underset{X}{\simeq} \hat{A}^i \tag{3}$$

and

$$\hat{A}^i \underset{X}{\simeq} \hat{A}^i \quad . \tag{4}$$

But the left side of (3) is $\hat{A}^i$ itself, so that (3) as well as (4) holds because of the reflexivity (Theorem 1). We examine the restrictions.

Condition 1. $\zeta(\sigma_i) = \sigma_i$ for each $i \in [n]$, so that the second condition, namely

$$\zeta(\sigma) = \sigma \qquad \text{for each} \quad \sigma \in S \cap S'' \ ,$$

where

$$S'' = \bigcup_{i \in [n]} (A^i)^{++} \cap A^{++} \ ,$$

is satisfied, while the first condition is included in the premise of the theorem explicitly.

Condition 2. (i), (ii) Apparent. (iii) We define U as X .

Condition 3. Apparent.

Thus, by Inf. 9,

$$\vdash D^i A \cong D^i B \qquad \text{for any } i \in [n] \ .$$

By the derivations for (1) and (2),

$$\sigma_i A \cong D^i A \cong D^i B \cong \sigma_i B \ .$$

Q.E.D.

Theorem 19. (Interchange of Copies)

If B ends with a go-to, and B and B' occur in A , then

$$\vdash A \cong A_{BB'}[B',B] \ . \qquad (\mathrm{IVc}^+)$$

Proof. (i) The case that A begins with a labelling and that B and B' are preceded by go-tos in A is proved firstly. Let C be $A_{BB'}[\Lambda,\Lambda]$ and D be the right side of the conclusion of the theorem. Let τ be a label such that $\tau \notin A^{\pm}$.

$$\sigma A\tau \cong \begin{cases} (\sigma B)'A\tau & \sigma \in B^- \quad \text{(Theorem 16)} \\ (\sigma B')'A\tau & \sigma \in (B')^- \quad \text{(Theorem 16)} \\ (\sigma C)'\tau A\tau & \sigma \in C^- \ . \quad \text{(Theorem 17)} \end{cases} \qquad (1)$$

Similarly,

$$\sigma D\tau \cong \begin{cases} (\sigma B)'D\tau & \sigma \in B^- \\ (\sigma B')'D\tau & \sigma \in (B')^- \\ (\sigma C)'\tau A\tau & \sigma \in C^- \end{cases} \qquad (2)$$

because $D_{B'B}[\Lambda,\Lambda]$ is also C . By Theorem 18, (1) and (2),

$$\sigma A\tau \cong \sigma D\tau \qquad \text{for any } \sigma\in A^{-} .$$

Therefore,

$$\sigma A \cong \sigma D \qquad \text{for any } \sigma\in A^{-} . \qquad \text{(Theorem 14)}$$

Choosing σ_o such that σ_o^{-1} occurs at the leftmost of A ,

$$A \cong D . \qquad \text{(Theorem 13)}$$

(ii) If A does not begin with a labelling, then we prove

$$\tau\tau^{-1}A \cong \tau\tau^{-1}A_{BB'}[B',B] \qquad (3)$$

for a τ such that $\tau\notin A^{\pm}$, which is a special case of (i). Formula (3) and Theorem 13 give the conclusion. If B or B' is not preceded by go-tos in A , then we insert $\alpha\alpha^{-1}$ and $\beta\beta^{-1}$ before B and B' , where $\alpha\notin A^{\pm}$ and $\beta\notin A^{\pm}$. $\beta^{-1}B'$ being a copy of $\alpha^{-1}B$, (i) implies

$$A_{BB'}[\alpha\alpha^{-1}B,\beta\beta^{-1}B'] \cong A_{BB'}[\alpha\beta^{-1}B',\beta\alpha^{-1}B] . \qquad (4)$$

Because of $\alpha(\alpha^{-1}B) \cong \beta(\beta^{-1}B')$ and Inf. 5a, used twice,

$$(4) \cong A_{BB'}[\beta\beta^{-1}B',\beta\alpha^{-1}B]$$

$$\cong A_{BB'}[\beta\beta^{-1}B',\alpha\alpha^{-1}B] . \qquad (5)$$

Deleting $\alpha\alpha^{-1}$ and $\beta\beta^{-1}$ from the left sides of (4) and (5) by Theorem 11 and Theorem 13, we get

$$A \cong A_{BB'}[B',B] .$$

Q.E.D.

Theorem 21. (Go To leading to usual Statements)

If $\sigma^{-1}B\tau^{-1}$ occurs in A, then

$$\vdash A \cong A_{\sigma}[B'\tau] \quad . \qquad (IVd^{+})$$

Proof. (i) The case that $\sigma \notin B^{++}$ is proved firstly. Let C be $A_{\tau^{-1}}[\tau\tau^{-1}]$. Then

$$A \cong C \quad . \qquad \text{(Theorem 13)} \qquad (1)$$

$\sigma^{-1}B\tau$ occurs in C and

$$\sigma(\sigma^{-1}B\tau) \cong B\tau \qquad \text{(Theorem 11, Theorem 13)}$$

$$\cong B'\tau \quad . \qquad \text{(Theorem 15)} \qquad (2)$$

By (2) and Inf. 5b,

$$C \cong C_{\sigma}[B'\tau]$$

$$\cong A_{\sigma}[B'\tau] \quad . \qquad \text{(Theorem 13)} \qquad (3)$$

Formulas (1) and (3) give the conclusion.

(ii) The case that $\sigma \in B^{++}$ will be proved. Suppose B' is $B_{\sigma_1 \ldots \sigma_n \sigma_1^{-1} \ldots \sigma_n^{-1}}[\sigma_1', \ldots, \sigma_n', \sigma_1'^{-1}, \ldots, \sigma_n'^{-1}]$. Let B" be $B'_{\sigma}[\sigma"]$, where $\sigma" \notin A^{\pm} \cup (B')^{\pm}$. Then $\sigma"^{-1}B"$ is a copy of $\sigma^{-1}B$, and

$$B"_{\sigma"}[\sigma]^{0} = B' \quad . \qquad (4)$$

Instead of (2) in the case (i), we have

$$\sigma(\sigma^{-1}B\tau) \cong (\sigma^{-1}B)\tau \qquad \text{(Theorem 13)}$$
$$\cong \sigma''^{-1}B''\tau \ . \qquad \text{(Theorem 15)} \qquad (5)$$

Therefore,

$$A \cong A_\sigma[\sigma''^{-1}B''\tau] \ . \qquad \text{(Inf. 5b)} \qquad (6)$$

But every occurrence of σ'' in the right side of (5) can be replaced by σ, because of

$$\sigma''(\sigma''^{-1}B''\tau) \cong \sigma(\sigma^{-1}B\tau) \qquad \text{(Theorem 15)}$$

and Inf. 5a. Thus

$$(6) \cong (A_\sigma[\sigma''^{-1}B''\tau])_{\sigma''}[\sigma]^\circ$$
$$\cong (A_\sigma[B''\tau])_{\sigma''}[\sigma]^\circ \ . \qquad \text{(Theorem 11)} \qquad (7)$$

The right side of (7) is $A_\sigma[B'\tau]$ because of (4), namely $A \cong A_\sigma[B'\tau]$.

Q.E.D.

Theorem 22. (Go To leading to Exits)

If $\tau \notin A^-$ and $\sigma^{-1}\tau$ occurs in A, then

$$\vdash A \cong A_\sigma[\tau] \ . \qquad (\text{IVe}^+)$$

Proof. $\sigma(\sigma^{-1}\tau) \cong \tau$ (Theorem 13, Theorem 11)

and Inf. 5b give the conclusion.

Q.E.D.

Theorem 23.

If $A^+ \cap C^- = A^- \cap C^+ = \phi$, $B^+ \cap D^- = B^- \cap D^+ = \phi$, $\vdash A \underset{R[C]\cup R[D]\cup X}{\simeq} B$, and $\vdash C \overset{\simeq}{X} D$, then

$$\vdash AC \overset{\simeq}{X} BD \quad . \qquad (Ig^+)$$

Proof. (i) The case that

$$B^+ \cap C^- = B^- \cap C^+ = \phi \qquad (1)$$

is proved firstly. The first wff of the premise of the theorem implies

$$\vdash AC \underset{R[C]\cup R[D]\cup X}{\simeq} BC \quad . \qquad \text{(Inf. 6)} \qquad (2)$$

The second wff, $C \overset{\simeq}{X} D$, implies

$$\vdash BC \overset{\simeq}{X} BD \quad . \qquad \text{(Inf. 7)} \qquad (3)$$

Thus,

$$\vdash AC \overset{\simeq}{X} BD \quad . \qquad \text{(Theorem 2, (2), (3))}$$

(ii) If (1) does not hold, we consider the copies B' and C' such that $A^+ \cap C'^{-1}$, $A^- \cap C'^+$, $B'^+ \cap D^-$, $B'^- \cap D^+$, $B'^+ \cap C'$, and $B'^- \cap C'^+$ are all ϕ. By Theorem 15,

$$B \cong B'$$

and

$$C \cong C' \quad .$$

We carry out the following derivation.

$$AC \cong AC' \qquad \text{(Inf. 6)}$$

$$\overset{\cong}{X} B'D \qquad \text{(by (i) above)}$$

$$\cong BD \ . \qquad \text{(Inf. 7)}$$

Namely,

$$AC \overset{\cong}{X} BD \ .$$

Q.E.D.

The above metatheorems show that wff $\mathfrak{F}$ is provable in the present formal system if it is provable in the previous system as noted at the beginning of this section. For the convenience of later use, Theorems 11 and 12 will be modified as follows. (Proofs are essentially the same as before.)

Theorem 11. (Superfluous Labels)

If $\sigma \notin A^-$, then $\vdash A \cong A_B[\sigma^{-1}B]$.

Theorem 12. (Disconnected Statements)

If $A_B[\Lambda]^+ \cap B^- = \emptyset$ and B is preceded by a go-to in A, then

$$\vdash A \cong A_B[\Lambda] \ .$$

The first of the following theorems will be used in Section 8, while the second is related to the notion of correctness. Theorem 24 says that two statements which are concatenations of a number of statements (loops may be contained semantically) are equivalent if the constituent statements

are equivalent statement-wise, which fact is related to compilation. Moreover, this theorem gives an example of proving the equivalence of two statements which do not necessarily terminate.

Theorem 24.

If

$$\vdash A_i \overset{\sim}{\underset{X}{=}} B_i \ ,$$

$$\vdash \sigma A_i \overset{\sim}{\underset{X}{=}} \sigma B_i \quad \text{for each } \sigma \in A_i^- \ ,$$

and

$$V[A_i] \subseteq X \ , \quad \text{for each } i \in [n] \ ,$$

then

$$\vdash A_1 \ldots A_n \overset{\sim}{\underset{X}{=}} B_1 \ldots B_n$$

and

$$\vdash \sigma(A_1 \ldots A_n) \overset{\sim}{\underset{X}{=}} \sigma(B_1 \ldots B_n) \quad \text{for each } \sigma \in \bigcup_{i \in [n]} A_i^- \ .$$

Proof. Let C and D be

$$\tau_1^{-1} A_1 \tau_2 \tau_2^{-1} A_2 \ldots \tau_n \tau_n^{-1} A_n \tau_{n+1}$$

and

$$\tau_1^{-1} B_1 \tau_2 \tau_2^{-1} B_2 \ldots \tau_n \tau_n^{-1} B_n \tau_{n+1} \ ,$$

respectively, where $\tau_1, \ldots, \tau_{n+1}$ do not belong to $(A_1 \ldots A_n)^{\pm} \cup (B_1 \ldots B_n)^{\pm}$.

Suppose $C^- = \{\sigma_1,\ldots,\sigma_n\}$, while $C^- = \bigcup_{i\in[n]} A_i^- + \{\tau_1,\ldots,\tau_n\}$ by definition. Then we notice the following.

$$\vdash \sigma\tau_i^{-1}A_i \mathrel{\overset{\approx}{X}} \sigma\tau_i^{-1}B_i \quad \text{for each } \sigma\in A_i^- + \{\tau_i\} \ , \tag{1}$$

because,

$$\tau_i\tau_i^{-1}A_i \cong A_i \qquad \text{(Theorems 11 (extended), 13)}$$

$$\mathrel{\overset{\approx}{X}} B_i \qquad \text{(premise of the theorem)}$$

$$\cong \tau_i\tau_i^{-1}B_i \ , \qquad \text{(Theorem 11, Theorem 13)}$$

and, for $\sigma\in A_i^-$,

$$\sigma\tau_i^{-1}A_i \cong \sigma A_i \qquad \text{(Theorem 11)}$$

$$\mathrel{\overset{\approx}{X}} \sigma B_i \qquad \text{(premise of the theorem)}$$

$$\cong \sigma\tau_i^{-1}B_i \ . \qquad \text{(Theorem 11)}$$

Therefore,

$$\vdash \sigma\tau_i^{-1}A_i\tau_{i+1} \mathrel{\overset{\approx}{X}} \sigma\tau_i^{-1}B_i\tau_{i+1} \quad \text{for each } \sigma\in A_i^- + \{\tau_i\} \ . \tag{2}$$

(Inf. 6, (1))

By Theorem 16,

$$\vdash \sigma C \cong (\sigma\tau_i^{-1}A_i\tau_{i+1})'C \quad \text{for each } \sigma\in A_i^- + \{\tau_i\} \ , \tag{3}$$

and

$$\vdash \sigma D \cong (\sigma\tau_i^{-1}B_i\tau_{i+1})'D \quad \text{for each } \sigma\in B_i^- + \{\tau_i\} \ . \tag{4}$$

But

$$(\sigma\tau_i^{-1}A_i\tau_{i+1})' \cong \sigma\tau_i^{-1}A_i\tau_{i+1} \quad \text{(Theorem 15)}$$

$$\overset{=}{X} \sigma\tau_i^{-1}B_i\tau_{i+1} \quad \text{(by (2))}$$

$$\cong (\sigma\tau_i^{-1}B_i\tau_{i+1})' , \quad \text{(Theorem 15)}$$

so that

$$\vdash (\sigma\tau_i^{-1}A_i\tau_{i+1})' \overset{=}{X} (\sigma\tau_i^{-1}B_i\tau_{i+1})' . \tag{5}$$

We change the index i of Inf. 9 into j, define σ_j as $\tilde{\sigma}_j$, and substitute σ_j (we can simply use σ_j instead of $(1 \to \sigma_j, \delta^i)$ as shown in the proof of Theorem 18), C, D, $(\sigma_j\tau_i^{-1}A_i\tau_{i+1})'$, $(\sigma_j\tau_i^{-1}B_i\tau_{i+1})'$, and C in place of D^i, A, B, A^i, B^i, and C, respectively. We note that

$$\vdash (\sigma\tau_i^{-1}A_i\tau_{i+1})' \overset{=}{X} (\sigma\tau_i^{-1}A_i\tau_{i+1})' . \quad \text{(reflexivity)} \tag{6}$$

Then wffs (3) - (6) constitute the premises of Inf. 9, and all the restrictions are apparently satisfied, so that

$$\vdash \sigma_k C \overset{=}{X} \sigma_k D \quad \text{for each } \sigma_k \epsilon C^- . \tag{7}$$

Therefore, for each $\sigma_k \epsilon A^-$,

$$\sigma_k(A_1 \ldots A_n) \cong \sigma_k C \quad \text{(Theorems 11, 13)}$$

$$\overset{=}{X} \sigma_k D \quad \text{(by (7))}$$

$$\cong \sigma_k(B_1 \ldots B_n) . \quad \text{(Theorems 11, 13)}$$

Similarly,

$$A_1 \ldots A_n \cong \tau_1 C$$

$$\overset{=}{X} \tau_1 D$$

$$\cong B_1 \ldots B_n \ .$$

Q.E.D.

Theorem 25. (Verification Condition for Assignment Operator)

Statement $x := f$ is partially correct w.r.t. p and q if and only if

$$\vdash_{\Gamma} p \supset q_x[f]^{\circ} \ . \quad \text{(Cf., Floyd (1967) and Hoare(1969).)}$$

Proof. We shall examine the conditions for p and q to satisfy

$$(p \to x := f,\Delta) \cong (p \to x := f;(q \to \Lambda,\Delta),\Delta) \ . \tag{1}$$

(See Section 4, 5. Correctness, (1'))

$$(p \to x := f;(q \to \Lambda,\Delta),\Delta)$$

$$\cong (p \to (q_x[f]^{\circ} \to x := f, x := f;\Delta),\Delta) \qquad \text{(Axiom 13)}$$

$$\cong (p \wedge q_x[f]^{\circ} \to x := f,(p \wedge \neg\, q_x[f]^{\circ} \to \Delta,\Delta))$$

(Axioms 5, 11a)

$$\cong (p \wedge q_x[f]^{\circ} \to x := f,\Delta) \ . \qquad \text{(Theorem 4)} \tag{2}$$

Therefore, (1) is equivalent to

$$(p \to x := f,\Delta) \cong (p \wedge q_x[f]^{\circ} \to x := f,\Delta) \ , \tag{3}$$

for which, obviously,

$$\vdash_{\Gamma} p \equiv p \wedge q_x[f]^{\circ}$$

namely

$$\vdash_{\Gamma} p \supset q_x[f]^{\circ} \qquad (4)$$

is necessary (see 3 below) and sufficient.

Q.E.D.

Remarks

1. Formula of (4) is logically equivalent to Floyd's original formula (written in our notation):

$$\exists x_o(x = f_x[x_o]^{\circ} \wedge p_x[x_o]^{\circ}) \supset q \quad ,$$

provided that the equality axioms are satisfied.

2. We assumed the completeness of Γ (including the law of the excluded middle) in order to use Theorem 4.

3. The necessity is based on the meaning of formulas, which can be, however, improved as follows.

We shall consider

$$\vdash (p \rightarrow \Lambda, \Delta) \cong \Lambda$$

as an assertion of the validity of formula p in the sense of predicate

calculus, and denote it by

$$\vdash^{*} p \ .$$

Then we can prove $\vdash^{*} p \supset q_x[f]^{\circ}$ formally from wff (3) by the following derivation:

Let r denote $p \wedge q_x[f]^{\circ}$, and A the statement $(r \to \Lambda,\Delta)$.

$$(p \to x := f,\Delta) \underset{\emptyset}{\simeq} (p \to \Lambda,\Delta) \ . \quad \text{(Axiom 8, Theorem 8)} \tag{5}$$

$$(r \to x := f,\Delta) \underset{\emptyset}{\simeq} (r \to \Lambda,\Delta) \quad \text{(similarly)}$$

$$\underset{\emptyset}{\simeq} (p \to \Lambda,\Delta) \ , \quad \text{(by (5))}$$

so that

$$(p \to \Lambda,\Delta) \cong (r \to \Lambda,\Delta) \ . \quad \text{(Inf. 3)} \tag{6}$$

$$(p \to \Lambda,\Delta) \cong (p \wedge r \to \Lambda,(p \wedge \neg r \to \Delta,\Delta)) \quad \text{(Theorem 4)}$$

$$\cong (p \to (r \to \Lambda,\Delta),\Delta) \quad \text{(Axiom 11a)}$$

$$\cong (p \to (p \to \Lambda,\Delta),\Delta) \quad \text{(by (6))}$$

$$\cong (p \wedge p \to \Lambda,(p \wedge \neg p \to \Delta,\Delta)) \quad \text{(Axiom 11a)}$$

$$\cong (p \to \Lambda,\Delta) \ . \quad \text{(Axiom 16b, Theorem 4)} \tag{7}$$

Similarly,

$$(\neg p \wedge \neg r \to \Lambda,\Delta) \cong (\neg p \to \Lambda,\Delta) \ . \tag{8}$$

Therefore

$$(p \wedge r \vee \neg p \wedge \neg r \to \Lambda,\Delta) \cong (1 \to \Lambda,\Delta) \quad \text{(Inf. 4, (7), (8))}$$

$$\cong \Lambda \ . \tag{9}$$

But

$$(p \supset q_x[f]^0 \rightarrow \Lambda,\Delta) \cong (p \equiv r \rightarrow \Lambda,\Delta) \qquad \text{(Axiom 16b)}$$

$$\cong (p \wedge r \vee \neg p \wedge \neg r \rightarrow \Lambda,\Delta)\ , \quad \text{(similarly)} \qquad (10)$$

so that

$$\vdash (p \supset q_x[f]^0 \rightarrow \Lambda,\Delta) \cong \Lambda\ . \qquad \text{(by (9), (10))}$$

(The sufficiency comes from Axiom 16b.)

4. Although the main reason that we introduced quantifiers into Algol-like statements (see Section 2) is to include formulas of usual predicate calculus in conditional statements in connection with the notion of correctness, this syntactic generalization of Algol-like statements may not be essential. For, the study of Engeler (1967) seems to suggest that infinitary logic is frequently more appropriate than ordinary logic. It must be noted that the example given by Floyd (1967) may be considered to be based upon infinitary logic. Also, the verification conditions for branch and join commands (the rest not being essential) can be stated and proved without using quantifiers, similarly to the above.

7. Decomposition of Statements

Let V be a subset of $\mathfrak{V}$ such that $\mathfrak{V}-V$ contains infinite elements $w_0, w_1, \ldots$, and L be a subset of $\mathfrak{L}$ such that $\mathfrak{L}-L$ contains infinite elements $\sigma_0, \sigma_1, \ldots$. By $\mathcal{A}_0$ is denoted the set of statements defined by induction as follows.

(d1) Λ belongs to $\mathcal{A}_0$.

(d2) For each $\sigma \in \mathfrak{L}$, σ and σ^{-1} belong to $\mathcal{A}_0$.

(d3) For each $x \in \mathfrak{V}$ and a fixed element w_0 of $\mathfrak{V}-V$, $x := w_0$ and $w_0 := x$ belong to $\mathcal{A}_0$.

(d4) For each $\pi^{(n)} \in \mathfrak{P}^{(n)}$ and $e_1, \ldots, e_{n-1}$ such that either $e_i \in \mathfrak{P}^{(0)}$ or $e_i \in \mathfrak{V}$ for each $i \in [n-1]$, $w_0 := \pi^{(n)} w_0 e_1 \cdots e_{n-1}$ belongs to $\mathcal{A}_0$.

(d5) For each $\rho^{(n)} \in \mathfrak{P}^{(n)}$, $\sigma \in \mathfrak{L}$, and $e_1, \ldots, e_{n-1}$ as above, $(\rho^{(n)} w_0 e_1 \cdots e_{n-1} \rightarrow \sigma, \Lambda)$ belongs to $\mathcal{A}_0$.

(e1) If A and B belong to $\mathcal{A}_0$, then AB belongs to $\mathcal{A}_0$. ($\bar{A} \cap \bar{B} = \emptyset$ should be satisfied. Otherwise, AB is not a statement.)

Let $\mathcal{A}_1$ be the set of statements consisting of all A such that $V[A] \subseteq V$, $A^{\dagger} \subseteq L$, and that the logical symbols other than $\neg$ and $\vee$ do not occur in A.

We shall establish a function

$$\Phi : \mathcal{A}_1 \rightarrow \mathcal{A}_0 ,$$

which has the following characteristics.

1. **Constructiveness:**

   Φ is total and effectively defined.

2. **Correctness:**

   $\vdash A \overset{\cong}{V} \Phi(A)$ for any $A \in \mathcal{A}_1$.

In other words, Φ is an algorithm that carries out a translation of $\mathcal{A}_1$ into $\mathcal{A}_0$, of which the latter consists of sequences of relatively simple statements. Moreover, we can formally prove that Φ always gives a statement equivalent to the original one in so far as the values of variables belonging to V and the destinations of exits are concerned. (Actually we prove the above also for each entry. cf. proof of Theorem 26).

For the convenience of description, we introduce two sets of statements, as follows:

$$\mathcal{A}_2 = \{x := f \mid x \in V \text{ and } V[f] \subseteq V\} .$$

$$\mathcal{A}_3 = \{(p \to \tau, \Lambda) \mid \tau \in f \text{ and } V[p] \subseteq V\} .$$

Besides, $\mathcal{A}_1^*$, $\mathcal{A}_2^*$, and $\mathcal{A}_3^*$ will be used, whose elements differ from $\mathcal{A}_1$, $\mathcal{A}_2$, and $\mathcal{A}_3$, respectively, only in that some suffixes are added. (See Definition of Θ below.)

Definition of Φ

Let Θ and Ψ be two functions as defined below. Then

$$\Phi(A) = \Psi(\Theta_0(A)) \quad \text{for each } A \in \mathcal{A}_1 .$$

1. Definition of θ

We define the function

$$\theta : \mathcal{A}_1 \times \eta \to \mathcal{A}_1^* \ ,$$

where the elements of $\mathcal{A}_1^*$ are statements whose symbols are possibly suffixed. For each A and each $\nu \in \eta$, $\theta_\nu(A)$ denotes the image of (A,ν). Actually, however, θ is extended so that, for each arithmetic expression f such that $V[f] \subseteq V$ and for each Boolean expression p such that $V[p] \subseteq V$, $\theta_\nu(f)$ and $\theta_\nu(p)$ are defined. Besides, two auxiliary functions

$$\lambda : \mathcal{A}_1 \cup \{p | V[p] \subseteq V\} \to \eta$$

and

$$\mu : \{f | V[f] \subseteq V\} \to \eta$$

are defined.

Practical meaning of these functions are as follows.

$\mu(f)$: The number of required working storages to compute f .

$\theta_\nu(f)$: The result of suffixing function symbols occurring in f so as to specify the allocation of working storages. (ν is irrelevant.)

$\lambda(p)$: The number of auxiliary labels to compute p , which is the number of occurrences of symbol $\neg$ in p .

$\mu(p)$: The number of required working storages to compute p .

$\theta_\nu(p)$: The result of suffixing p to specify all the auxiliary labels using index greater than ν .

$\lambda(A)$ and $\theta_\nu(A)$: Similar to $\lambda(p)$ and $\theta_\nu(p)$.

Functions θ , λ , and μ are defined simultaneously by induction on statements as follows.

Atomic Statements

(a1) and (a2) $C = \Lambda$, σ, or σ^{-1} :

$\theta_\nu(C) = C$ for each ν .

$\lambda(C) = 0$.

(a3) $C = x := f$, where $f = y$:

$\mu(f) = 0$.

$\theta_\nu(f) = f$ for each ν .

$\theta_\nu(C) = x := \theta_\nu(f)$. (1)

$\lambda(C) = 0$. (2)

Statements (non-atomic)

(b1) $C = AB$:

$\theta_\nu(C) = \theta_\nu(A)\theta_{\nu+\lambda(A)}(B)$.

$\lambda(C) = \lambda(A) + \lambda(B)$.

(b2) $C = x := f$, where $f = \pi^{(n)} f_0 \ldots f_{n-1}$:

$\mu(f) = M+m$,

where

$$M = \max_{0 \leq i \leq n-1} \mu(f_i) \quad , \tag{3}$$

and m is the number of f_i such that $f_i \notin V$.

$$\theta_\nu(f) = \pi^{(n)}_{M+1,\ldots,M+m}\, \theta_\nu(f_0) \ldots \theta_\nu(f_{n-1}) \quad . \tag{4}$$

$\theta_\nu(C)$ and $\lambda(C)$ are defined by (1) and (2) above.

(b3) $C = (p \rightarrow A,B)$, where $p = \rho^{(n)} f_0 \ldots f_{n-1}$:

$\mu(p) = M+m$,

where M and m are defined by (3) and (4) above.

$\theta_\nu(p) = \rho^{(n)}_{M+1,\ldots,M+m}\, \theta_\nu(f_0) \ldots \theta_\nu(f_{n-1})$.

$\lambda(p) = 0$.

(i) If A is τ and B is Λ , then

$$\theta_\nu(C) = (\theta_\nu(p) \rightarrow \tau,\Lambda) \quad , \tag{5}$$

and

$$\lambda(C) = \lambda(p) \quad . \tag{6}$$

(ii) If A is not of the form τ or B is not Λ , then

$$\theta_\nu(C) = (\theta_{\nu+\lambda(A)+\lambda(B)}(p)\ \overline{\ }_{M+1,M+2}\ \theta_\nu(A), \theta_{\nu+\lambda(A)}(B)) \quad , \tag{7}$$

where

$$N = \nu + \lambda(A) + \lambda(B) + \lambda(p) \quad ,$$

and

$$\lambda(C) = N+2 \quad . \tag{6}$$

(c1) $C = (\neg p \rightarrow A,B)$:

$$\theta_\nu(\neg p) = \neg_{\nu+1} \theta_\nu(p) \quad .$$

$$\lambda(\neg p) = \lambda(p)+1 \quad .$$

$\theta_\nu(C)$ and $\lambda(C)$ are defined by (5)-(8) above. (Substitute $\neg p$ in place of p .)

(c2) $C = (p \vee q \rightarrow A,B)$:

$$\theta_\nu(p \vee q) = \theta_\nu(p) \vee \theta_{\nu+\lambda(p)}(q) \quad .$$

$$\lambda(p \vee q) = \lambda(p) + \lambda(q) \quad .$$

$\theta_\nu(C)$ and $\lambda(C)$ are defined by (5)-(8) above. (Subsitute $p \vee q$ in place of p .)

2. Definition of Ψ

We define the function

$$\Psi : a_1^* \cup a_2^* \cup a_3^* \rightarrow a_0 \quad .$$

By A^* , f^* , and p^* will be denoted $\theta_\nu(A)$, $\theta_\nu(f)$, and $\theta_\nu(p)$, respectively, for certain values of ν . Thus, for instance,

(b1) below, i.e.,

$$\Psi(A^*B^*) = \Psi(A^*)\Psi(B^*)$$

reads as follows:

Since $C = AB$, $\theta_\nu(C)$ is of the form A^*B^*. Define $\Psi(A^*)\Psi(B^*)$ as $\Psi(\theta_\nu(C))$.

w_0 plays the role of an accumulator.

Ψ is defined by induction as follows.

Atomic Statements

(a1) $\Psi(\Lambda) = \Lambda$.

(a2) $\Psi(\sigma) = \sigma$.

$\Psi(\sigma^{-1}) = \sigma^{-1}$.

(a3) (i) $\Psi(w_0 := y) = w_0 := y$.

(ii) If $x \neq w_0$, then $\Psi(x := y)$ is defined by (1) below. (Substitute y in place of f.)

Statements (non-atomic)

(b1) $\Psi(A^*B^*) = \Psi(A^*)\Psi(B^*)$.

(b2) (i) $\Psi(w_0 := \pi^{(0)}) = w_0 := \pi^{(0)}$.

(ii) $\Psi(w_0 := \pi^{(n)}_{\alpha(1)\ldots\alpha(m)} f_0^* \cdots f_{n-1}^*)$

$= C_{n-1}\cdots C_0;\ w_0 := \pi^{(n)} w_0 u_1 \cdots u_{n-1}$, $(n \geq 1)$

where

$$u_i = \begin{cases} f_i & f_i \in V \\ w_{\alpha(\beta(i))} & f_i \notin V \end{cases} \qquad \text{for } i \in [n-1] \ ,$$

C_0 is $w_0 := f_0$,

and

$$C_i = \begin{cases} \Lambda & f_i \in V \\ u_i := f_i & f_i \notin V \end{cases} \qquad \text{for each } i \in [n-1] \ ,$$

$\beta(i)$ being defined by the following induction:

$$\beta(0) = 0 \ .$$

$$\beta(i+1) = \begin{matrix} \beta(i) & f_i \in V \\ \beta(i)+1 & f_i \notin V \end{matrix} \ .$$

(iii) $$\forall(x := f^*) = \forall(w_0 := f^*)x := w_0 \ . \quad (x \neq w_0) \qquad (1)$$

(b3) (i) $$\forall((\rho^{(0)} \to \tau, \Lambda)) = (\rho^{(0)} \to \tau, \Lambda) \ .$$

(ii) $$\forall((\rho^{(n)}_{\alpha(1)\ldots\alpha(m)} f^*_0 \ldots f^*_{n-1} \to_{\gamma(1)\gamma(2)} \tau, \Lambda) \ , \quad (n \geq 1)$$

where $C_0, \ldots, C_{n-1}$, $u_1, \ldots, u_{n-1}$ are the same as above. (cf. (b2)(ii).)

(iii) $$\forall((p^* \to_{\gamma(1)\gamma(2)} A^*, B^*)$$

$$= \forall((p^* \to_{\gamma(1)\gamma(2)} \sigma_{\gamma(1)}, \Lambda))\forall(B^*)\sigma_{\gamma(2)}\sigma^{-1}_{\gamma(1)}\forall(A^*)\sigma^{-1}_{\gamma(2)} \ . \qquad (2)$$

(A is not of the form τ , or B is not Λ .)

(c1) (i) $\forall((\neg_\delta p^* \to \tau, \Lambda))$

$$= \forall((p^* \to \sigma_\delta, \Lambda))\tau\sigma_\delta^{-1} \quad .$$

(ii) If A is not of the form τ , or B is not Λ , then

$\forall((\neg_\delta p^* \to_{\gamma(1)\gamma(2)} A,B))$ is defined by (2) above.

(Substitute $\neg_\delta p^*$ in place of p^* .)

(c2) (i) $\forall((p^* \vee q^* \to \tau, \Lambda))$

$$= \forall((p^* \to \tau, \Lambda))\forall((q^* \to \tau, \Lambda)) \quad .$$

(ii) If A is not of the form τ , or B is not Λ , then

$\forall((p^* \vee q^* \to_{\gamma(1)\gamma(2)} A,B))$ is defined by (2) above.

(Substitute $p^* \vee q^*$ in place of p^* .)

Example

We consider the statement

$$\underline{\text{if}}\ x < 0\ \underline{\text{then}}\ x := -x \ , \tag{1}$$

which was used as an example of compilation in (Igarashi, 1968).

Here, let us allow only binary - , and see how the statement

$$\underline{\text{if}}\ x < 0\ \underline{\text{then}}\ x := 0-x \ , \tag{2}$$

namely

$$(x < 0 \to x := 0-x, \Lambda) \tag{3}$$

in our notation, is treated.

Let A be $(\rho^{(1)}x \to x := \pi^{(2)}\pi^{(0)}x, \Lambda)$. Then,

$$\theta_0(A) = A^* = (\rho^{(1)}x \to_{1,2} x := \pi_1^{(2)}\ \pi^{(0)}x,A)$$

and

$$\Psi(A^*) = w_0 := x;(\rho^{(1)}w_0 \to \sigma_1,A)\sigma_2\sigma_1^{-1}\ ;$$

$$w_0 := \pi^{(0)};\ w_0 := \pi^{(2)}w_0x;\ x := w_0;\ \sigma_2^{-1}\ .$$

Especially, we define $x < 0$ as $\rho^{(1)}x$, 0 as $\pi^{(0)}$, and $x-y$ as $\pi^{(0)}xy$, so that A becomes (3).

For readability's sake, $\Phi(A)$ i.e., $\Psi(A^*)$ will be written in ALGOL 60 and listed with corresponding actions, symbols w_0, σ_1, and σ_2 being replaced by acc, L1, and L2, respectively.

```
    acc := x;                          load x
    if acc < 0 then go to L1;          jump on minus L1
    go to L2;                          jump L2
L1:                                    insert label L1

    acc := 0;                          load 0
    acc := acc - x;                    subtract x
    x := acc;                          store x
L2:                                    insert label L2
```

(4)

Statement (4) is different only in trivial points from program *B* (in the above paper) for which

$$\vdash (1) \underset{\{x\}}{=} \mathcal{B}$$

is proved as an example of derivation. That proof, for this particular pair of statements, needed two pages of derivation (20 steps) preceded by one page (10 steps) for an auxiliary formula, being derived directly from the previous formal system. In the present paper, however, we shall prove, also formally, that

$$A \underset{V}{\cong} \Phi(A)$$

is valid for every $A \in \mathcal{A}_1$, which implies that $(2) \underset{V\text{-}\{acc\}}{=} (4)$.

Page Intentionally Left Blank

8. Formal Proof of the Correctness of Decomposition

In this section we shall prove formally the following theorem which implies the validity of the transformation defined in the previous section.

Theorem 26. Let (V,K,R,Γ°,J) be an interpretation such that π_R is a total function for each $\pi\in\mathfrak{F}$ and that ρ_R is a total predicate for each $\rho\in\mathfrak{P}$. Then

$$\vdash A \underset{V}{\simeq} \Phi(A) \quad \text{for any } A\in\mathcal{A}_1 .$$

We shall prove the following lemmas firstly.

Lemma 1. If $x\notin V[f]$, then

$$\vdash x := f;\ y := g \underset{V-\{x\}}{\simeq} y := g_x[f]^{\circ} ,$$

and

$$\vdash x := f;\ (p \to \sigma,\Lambda) \underset{V-\{x\}}{\simeq} (p_x[f]^{\circ} \to \sigma,\Lambda) .$$

Proof. Choose z such that $z \neq x$.

$$\begin{aligned} x := f;\ y := g &\simeq x := f;\ y := g;\ z := z && \text{(Axioms 2a, 6, etc.)} \\ &\simeq x := f;\ y := g_x[f];\ z := z && \text{(Axiom 7b)} \\ &\simeq x := f;\ y := g_x[f] . && \text{(Conversely)} \quad (1) \end{aligned}$$

$$x := f \underset{V-\{x\}}{\simeq} \Lambda , \qquad \text{(Axiom 8)} \quad (2)$$

so that, right multiplying both sides of (2) by $y := g_x[f]^\circ$, we obtain

$$x := f;\ y := g_x[f]^\circ \underset{\forall-\{x\}}{\simeq} y := g_x[f]^\circ \ .\ \text{(Inf. 6)} \qquad (3)$$

It must be noted that only $g_x[f]^\circ$ instead of an arbitrary $g_x[f]$ should be used because it must not contain x to use Inf. 6. By (1) and (3), the first wff is provable, while the latter can be proved in the same manner.

Q.E.D.

Lemma 2. Let C and D denote $(p \to A,B)$ and $(p \to \tau_1,\Lambda)B\tau_2\tau_1^{-1}A\tau_2^{-1}$, respectively. Then

$$\vdash C \cong D \ ,$$

and

$$\vdash \sigma C \cong \sigma D \quad \text{for each } \sigma \in A^- \cup B^- \ .$$

Proof. Let $\hat{C}$ and $\hat{D}$ denote

$$\gamma^{-1}(p \to \alpha\alpha^{-1}A,\beta\beta^{-1}B)\delta$$

and

$$\gamma^{-1}(p \to \tau_1,\Lambda)\beta\beta^{-1}B\tau_2\tau_1^{-1}\alpha\alpha^{-1}A\tau_2^{-1}\delta \ ,$$

respectively, where α, β, γ, and δ do not belong to $C^{\pm} \cup D^{\pm}$. Then, by Theorems 11-13, $\vdash C \cong \hat{C}$, $\vdash \sigma C \cong \sigma\hat{C}$, $\vdash D \cong \hat{D}$, and, $\vdash \sigma D \cong \sigma\hat{D}$, for any $\sigma \in A^- \cup B^-$. Let $\{\sigma_1,\ldots,\sigma_n\}$ be $A^- \cup B^- \cup \{\alpha,\beta,\gamma\}$.

$$\sigma_i\hat{D} \cong \begin{cases} (\sigma_i\alpha^{-1}A\tau_2^{-1}\delta)'\hat{D} & \sigma_i \epsilon A^- \cup \{\alpha\} \\ (\sigma_i\beta^{-1}B\tau_2)'\hat{D} & \sigma_i \epsilon B^- \cup \{\beta\} \\ (\gamma\gamma^{-1}(p \to \tau_1, \Lambda)\beta)'\hat{D} & \sigma_i = \gamma \ . \end{cases}$$

(Theorem 16, Theorem 17)

But

$$(\sigma_i\beta^{-1}B\tau_2)'\hat{D} \cong (\sigma_i\beta^{-1}B)'\tau_2\hat{D}$$

$$\cong (\sigma_i\beta^{-1}B)'\delta\hat{D} \ , \qquad \text{(Theorem 22)}$$

and

$$(\gamma\gamma^{-1}(p \to \tau_1, \Lambda)\beta)'\hat{D} \cong (p \to \tau_1, \Lambda)\beta\hat{D}$$

$$\cong (p \to \alpha, \Lambda)\beta\hat{D} \qquad \text{(Theorem 21)}$$

$$\cong (p \to \alpha\beta, \beta)\hat{D} \qquad \text{(Axiom 12a)}$$

$$\cong (p \to \alpha, \beta)\hat{D} \ . \qquad \text{(Theorem 12)}$$

Therefore

$$\sigma_i\hat{D} \cong \begin{cases} (\sigma_i A)'\delta\hat{D} & \sigma_i \epsilon A^- \\ (\sigma_i B)'\delta\hat{D} & \sigma_i \epsilon B^- \\ A'\delta\hat{D} & \sigma_i = \alpha \\ B'\delta\hat{D} & \sigma_i = \beta \\ (p \to \alpha, \beta)\hat{D} & \sigma_i = \gamma \ . \end{cases} \qquad (1)$$

Apparently (1) is provable if $\hat{C}$ is substituted in place of $\hat{D}$, so that

$$\sigma_i\hat{C} \cong \sigma_i\hat{D} \quad \text{for each} \quad \sigma_i \epsilon A^- \cup B^- \cup \{\alpha,\beta,\gamma\} \ .$$

Therefore,

$$\sigma C \cong \sigma\hat{C} \cong \sigma\hat{D} \cong \sigma D \quad \text{for each} \quad \sigma\epsilon A^- \cup B^- \ ,$$

and

$$C \cong \hat{C} \cong \gamma\hat{C} \cong \gamma\hat{D} \cong \hat{D} \cong D \ . \qquad \text{(Theorem 18)}$$

Q.E.D.

Lemma 3.

$$\vdash \sigma(p \to A,B) \cong \sigma(q \to B,A) \quad \text{for each} \quad \sigma\epsilon A^- \cup B^- \ .$$

Proof. Let τ be a label symbol such that $\tau \notin A^- \cup B^-$. Then

$$\sigma(p \to A,B)\tau \cong \sigma(p \to A\tau,B\tau) \ , \qquad \text{(Axiom 12b)} \qquad (1)$$

$$\sigma(q \to B,A)\tau \cong \sigma(q \to B\tau,A\tau) \ , \qquad \text{(Axiom 12b)} \qquad (2)$$

and, by Theorem 16,

$$\sigma(p \to A\tau,B\tau) \cong \begin{cases} (\sigma A)'\tau(p \to A\tau,B\tau) & \sigma\epsilon A^- \ , \\ (\sigma B)'\tau(p \to A\tau,B\tau) & \sigma\epsilon B^- \ . \end{cases} \qquad (3)$$

Similarly,

$$\sigma(q \to B\tau, A\tau) \cong \begin{cases} (\sigma A)'\tau(q \to B\tau, A\tau) & \sigma \in \bar{A} \ , \\ (\sigma B)'\tau(q \to B\tau, A\tau) & \sigma \in \bar{B} \ . \end{cases} \tag{4}$$

Therefore, by Theorem 18,

$$\sigma(p \to A\tau, B\tau) \cong \sigma(q \to B\tau, A\tau) \ , \tag{5}$$

so that, using (1) and (2),

$$\sigma(p \to A,B)\tau \cong \sigma(q \to B,A)\tau \ .$$

Thus,

$$\sigma(p \to A,B) \cong \sigma(q \to B,A) \qquad \text{(Theorem 14)}$$

Q.E.D.

Lemma 4. If the interpretation satisfies the premise of Theorem 26, then

$$\vdash (p \to \tau, \Lambda)(q \to \tau, \Lambda) \cong (p \vee q \to \tau, \Lambda) \ .$$

Proof.

$$(p \to \tau, \Lambda)(q \to \tau, \Lambda) \cong (p \to \tau(q \to \tau, \Lambda), (q \to \tau, \Lambda)) \quad \text{(Axiom 12a)}$$

$$\cong (p \to \tau, (q \to \tau, \Lambda)) \ . \quad \text{(Theorem 12)} \quad (1)$$

$$(p \vee q \to \tau , \Lambda) \cong (\neg(\neg p \wedge \neg q) \to \tau , \Lambda) \qquad \text{(Axiom 16b)}$$

$$\cong (\neg p \wedge \neg q \to \Lambda, \tau) \qquad \text{(Axiom 10)}$$

$$\cong (\neg p \wedge \neg q \to \Lambda, (\neg p \wedge q \to \tau, \tau)) \qquad \text{(Theorem 4)}$$

$$\cong (\neg p \to (\neg q \to \Lambda, \tau), \tau) \qquad \text{(Axiom 11a)}$$

$$\cong (p \to \tau , (\neg q \to \Lambda, \tau)) \qquad \text{(Axiom 10)}$$

$$\cong (p \to \tau , (q \to \tau , \Lambda)) \quad . \qquad \text{(Axiom 10)} \qquad (2)$$

Statements (1) and (2) are identical.

Q.E.D.

Proof of Theorem 26.

We shall prove the following statements, which include the conclusion of the theorem, by induction.

1. For each $A \in \mathcal{A}_1$ such that A is neither of the form $x := f$ nor of the form $(p \to \tau, \Lambda)$,

$$\vdash A \underset{V}{\cong} \Psi(A^*)$$

and

$$\vdash \sigma A \underset{V}{\cong} \sigma\Psi(A^*) \qquad \text{for each } \sigma \in \bar{A} \ .$$

2. For each statement of the form $x := f$ belonging to $\mathcal{A}_1$ or $\mathcal{A}_2$,

$$\vdash x := f \underset{S[x:=f^*]}{\cong} \Psi(x := f^*) \ ,$$

where

$$S[x := f^*] = \{x\} \cup (V - W[f^*] - \{w_0\}) \quad ,$$

$W[f^*]$ being $\{w_i \mid i$ occurs in f^* as suffix$\}$.

3. For each statement of the form $(p \to \tau, \Lambda)$ belonging to $\mathcal{A}_1$ or $\mathcal{A}_3$,

$$\vdash (p \to \tau, \Lambda) \overset{\sim}{\underset{V}{=}} V((p^* \to \tau, \Lambda)) \quad .$$

Since $V \subseteq S[x := f^*]$, these statements imply

$$\vdash A \overset{\sim}{\underset{V}{=}} V(A^*) \quad \text{for any } A \in \mathcal{A}_1 \ .$$

Atomic Statements

(a1), (a2(i), (a2(ii), and (a3)(i).

$V(A^*)$ is identical with A , so that the above statements are apparent.

(a3)(ii).

$V(w_0 := y)x := w_0$ is $w_0 := y;\ x := w_0$,

for which

$$w_0 := y;\ x := w_0 \underset{V-\{w_0\}}{\simeq} x := y \quad , \qquad \text{(Lemma 1)}$$

and

$$S[x := y] = V - \{w_0\} \ .$$

Statements (non-atomic)

Hereafter the statements 1 - 3 will be used as the induction hypotheses.

(b1) By Hypothesis 1,

$$A \underset{V}{\simeq} \mathbf{V}(A^*) \ ,$$

$$\sigma A \underset{V}{\simeq} \sigma\mathbf{V}(A^*) \qquad \text{for each } \sigma \epsilon A^- \ ,$$

$$B \underset{V}{\simeq} \mathbf{V}(B^*) \ ,$$

and

$$\sigma B \underset{V}{\simeq} \sigma\mathbf{V}(B^*) \qquad \text{for each } \sigma \epsilon B^- \ .$$

Therefore,

$$AB \underset{V}{\simeq} \mathbf{V}(A^*)\mathbf{V}(B^*)$$

and

$$\sigma AB \underset{V}{\simeq} \sigma\mathbf{V}(A^*)\mathbf{V}(B^*) \ . \qquad \text{(Theorem 24)}$$

(b2)(i) Apparent because $\mathbf{V}(A^*)$ is identical with A.

(b2)(ii) Let $D^{(n)}$ be $\pi^{(n)}w_0u_1\ldots u_{n-1}$, $D_k^{(n)}$ be $\pi^{(n)}f_0\ldots f_k u_{k+1}\ldots u_{n-1}$, and

$$T_k = V - \bigcup_{i=0}^{k} W[f_i^*] - \{u_i \mid i \epsilon [k] \text{ and } u_i \notin V\} \ , \quad \text{for } k = 0,\ldots,n-1 \ .$$

We prove, firstly,

$$C_k\ldots C_0 D^{(n)} \underset{T_k}{\simeq} D_k^{(n)} \qquad \text{for each } k \qquad (1)$$

by induction on k .

Step k = 0 :

$$w_0 := f_0 \underset{S[w_0:=f_0^*]}{\simeq} C_0 \quad . \qquad \text{(Hypothesis 2)} \qquad (2)$$

We note that

$$R[D^{(n)}] = \{w_0, u_1, \ldots, u_{n-1}\} \subseteq S[w_0 := f_0^*] \quad , \qquad (3)$$

which is shown as follows.

$$S[w_0 := f_0^*] = V - W[f_0^*] \quad . \qquad \text{(by definition)}$$

But by definition of $W[f_0^*]$,

$$w_0 \notin W[f_0^*] \quad ,$$

$$W[f_0^*] \cap V = \phi \quad ,$$

and, if $u_i \notin V$, then $u_i \notin W[f_0^*]$, $(i = 0, \ldots, n-1)$. Thus $R[D^{(n)}] \cap W[f_0^*] = \phi$, so that (3) holds. By (2) and (3),

$$w_0 := f_0 \; ; \; D^{(n)} \underset{S[w_0:=f_0^*] \cup \{w_0\}}{\simeq} C_0 D^{(n)} \qquad \text{(Inf. 6)}$$

$$\simeq D_0^{(n)} \quad . \qquad \text{(Axiom 7a)} \qquad (4)$$

Step k+1 : We use (1) as the supposition of induction. Firstly, we prove the case that $u_{k+1} \notin V$.

$$C_{k+1}(C_k \ldots C_0 D^{(n)}) \underset{T_k}{\simeq} C_{k+1} D_k^{(n)} \quad . \qquad \text{(Inf. 7, (1))} \qquad (5)$$

$$C_{k+1} \underset{S[u_{k+1}:=f^*_{k+1}]}{\simeq} u_{k+1} := f_{k+1} \quad . \qquad \text{(Hypothesis 2)} \qquad (6)$$

We note that

$$R[D_k^{(n)}] = (\bigcup_{i=0}^{k} V[f_i]) \cup \{u_{k+1},\ldots,u_{n-1}\} \subseteq S[u_{k+1} := f^*_{k+1}] \ , \qquad (7)$$

which is shown similarly to the above, by

$$W[f^*_{k+1}] \cap V = \phi \ ,$$

$$V[f_i] \subseteq V \ ,$$

and, if $u_i \notin V$, then $u_i \notin W[f^*_{k+1}]$, $(i = 0,\ldots,n-1)$. Therefore

$$C_{k+1}D_k^{(n)} \underset{S[u_{k+1}:=f^*_{k+1}] \cup \{w_0\}}{\simeq} u_{k+1} := f_{k+1} \ ; \ D_k^{(n)} \qquad \text{(Inf. 6)} \qquad (8)$$

$$\underset{V-\{u_{k+1}\}}{\simeq} D_{k+1}^{(n)} \quad . \qquad \text{(Lemma 1)} \qquad (9)$$

But

$$T_k \cap (S[u_{k+1} := f^*_{k+1}] \cup \{w_0\}) \cap (V - \{u_{k+1}\})$$

$$= T_k \cap (\{u_{k+1}\} \cup (V - W[f_{k+1}])) \cap (V - \{u_{k+1}\})$$

$$= T_k - W[f_{k+1}] - \{u_{k+1}\}$$

$$= T_{k+1} \ ,$$

so that

$$C_{k+1}\ldots C_0 D^{(n)} \underset{T_{k+1}}{\simeq} D_{k+1}^{(n)} \quad . \qquad ((5),\ (8),\ (9),\ \text{Theorem 2}) \qquad (10)$$

Secondly, the case that $u_{k+1} \in V$ has to be proved. In this case, however, C_{k+1} is Λ, $D^{(n)}_{k+1}$ is identical with $D^{(n)}_{k}$, and $T_{k+1} = T_k$, so that (1) implies (10). Thus (1) has been proved.

Let $k = n-1$.

$$C_{n-1}\cdots D_0 D^{(n)} \underset{T_{n-1}}{\simeq} D^{(n)}_{n-1} \quad . \qquad \text{(by (1))} \qquad (11)$$

Apparently,

$$T_{n-1} = V - W[f^*] = S[w_0 := f^*] \quad ,$$

and $D^{(n)}_{n-1}$ is $w_0 := \pi^{(n)} f_0 \cdots f_{n-1}$, that is $w_0 := f$, so that

$$C_{n-1}\cdots C_0 D^{(n)} \underset{S[w_0 := f^*]}{\simeq} w_0 := f \; . \qquad \text{(by (11))} \qquad (12)$$

<u>(b2)(iii)</u>. By (b2)(ii) above,

$$Y(w_0 := f^*) \underset{V-W[f^*]}{\simeq} w_0 := f \quad ,$$

so that

$$Y(w_0 := f^*)x := w_0 \underset{\{x\} \cup (V-W[f^*])}{\simeq} w_0 := f;\ x := w_0 \qquad \text{(Inf. 6)}$$

$$\underset{V-\{w_0\}}{\simeq} x := f \quad . \qquad \text{(Lemma 1)}$$

Therefore

$$x := f \underset{\{x\} \cup (V-W[f^*]-\{w_0\})}{\simeq} Y(x := f^*) \quad . \qquad \text{(Theorem 2)}$$

(b3)(i). Apparent because $\Psi(A^*)$ is identical with A.

(b3)(ii). We have only to modify the proof of (b2)(ii) as follows.

Let $D^{(n)}$ be $(\rho^{(n)}w_0u_1\ldots u_{n-1} \rightarrow \tau,\Lambda)$,

$D_k^{(n)}$ be $(\rho^{(n)}f_0\ldots f_k u_{k+1}\ldots u_{n-1} \rightarrow \tau,\Lambda)$, and

$$T_k = V - \bigcup_{i=0}^{k} W[f_i^*] - \{u_i \mid i\in[k] \text{ and } u_i \notin V\} - \{w_0\} ,$$

for $k = 0,\ldots,n-1$.

Then we can prove wff (1) above also for this case, using the axioms, theorems, etc. in the same manner. Letting $k = n-1$, we have

$$C_{n-1}\ldots D_0 D^{(n)} \underset{V-W[f^*]-\{w_0\}}{\simeq} (p \rightarrow \tau,\Lambda) . \tag{13}$$

Therefore,

$$\Psi((p^* \rightarrow \tau,\Lambda)) \underset{V}{\simeq} (p \rightarrow \tau,\Lambda) .$$

(b3)(iii). By (b3)(ii) above,

$$(p \rightarrow \sigma_{\gamma(1)},\Lambda) \underset{V}{\simeq} \Psi((p^* \rightarrow \sigma_{\gamma(1)},\Lambda)) . \tag{14}$$

By Hypothesis 1,

$$A \underset{V}{\simeq} \Psi(A^*) ,$$

$$\sigma A \underset{V}{\simeq} \sigma\Psi(A^*) \qquad \text{for each } \sigma\in A^- ,$$

$$B \underset{V}{\simeq} \Psi(B^*) ,$$

$$\sigma B \overset{\cong}{V} \sigma\forall(B^*) \qquad \text{for each } \sigma\epsilon B^- ,$$

and

$$\sigma_{\gamma(1)} \overset{\cong}{V} \sigma_{\gamma(1)} . \qquad \text{(reflexivity)}$$

Therefore,

$$\forall((p^* \to \sigma_{\gamma(1)},\Lambda))\forall(B^*)\sigma_{\gamma(2)}\sigma^{-1}_{\gamma(1)}\ \forall(A^*)\sigma^{-1}_{\gamma(2)}$$

$$\overset{\cong}{V} (p \to \sigma_{\gamma(1)},\Lambda)B\sigma_{\gamma(2)}\sigma^{-1}_{\gamma(1)}A\sigma^{-1}_{\gamma(2)} \qquad \text{(Theorem 24)} \qquad (15)$$

$$\cong (p \to A,B) . \qquad \text{(Lemma 2)}$$

Thus

$$(p \to A,B) \overset{\cong}{V} \forall((p^* \to_{\gamma(1)\gamma(2)} A^*,B^*)) . \qquad (16)$$

By the same theorem and lemma,

$$\sigma(p \to A,B) \overset{\cong}{V} \sigma\forall((p^* \to_{\gamma(1)\gamma(2)} A^*,B^*)) .$$

(c1)(i).

$$\forall((p^* \to \sigma_\delta,\Lambda)) \overset{\cong}{V} (p \to \sigma_\delta,\Lambda) . \qquad \text{(Hypothesis 3)} \qquad (17)$$

Right multiplying both sides of (17) by $\tau\sigma^{-1}_\delta$, we have

$$\forall((p^* \to \sigma_\delta,\Lambda))\tau\sigma^{-1}_\delta \overset{\cong}{V} (p \to \sigma_\delta,\Lambda)\tau\sigma^{-1}_\delta \qquad \text{(Inf. 6)}$$

$$\cong (p \to \sigma_\delta\tau\sigma^{-1}_\delta,\tau\sigma'^{-1}_\delta) \qquad \text{(Axiom 12a)}$$

$$\cong (p \to \Lambda,\tau) \qquad \text{(Theorems 11 - 13)}$$

$$\cong (\neg p \to \tau,\Lambda) . \qquad \text{(Axiom 10)}$$

Thus

$$\forall((\neg_\delta p^* \to \tau,\Lambda)) \tilde{\simeq}_{\forall} (\neg p \to \tau,\Lambda) \quad . \qquad \text{(Theorem 2)}$$

(c1)(ii). By (c1)(i) above, (14) holds also in this case, so that the same proof as that of (b3)(iii) suffices. (Substitute $\neg p$ and $\neg_\delta p^*$ in place of p and p^* in (14), respectively.)

(c2)(i).

$$\forall((p^* \to \tau,\Lambda)) \tilde{\simeq}_{\forall} (p \to \tau,\Lambda) \quad . \qquad \text{(Hypothesis 3)} \qquad (18)$$

$$\forall((q^* \to \tau,\Lambda)) \tilde{\simeq}_{\forall} (q \to \tau,\Lambda) \quad . \qquad \text{(Similarly)} \qquad (19)$$

Therefore, by Theorem 24,

$$\forall((p^* \to \tau,\Lambda))\forall((q^* \to \tau,\Lambda)) \tilde{\simeq}_{\forall} (p \to \tau,\Lambda)(q \to \tau,\Lambda)$$

$$\simeq (p \vee q \to \tau,\Lambda) \quad . \quad \text{(Lemma 4)}$$

Thus

$$\forall((p^* \vee q^* \to \tau,\Lambda) \tilde{\simeq}_{\forall} (p \vee q \to \tau,\Lambda) \quad .$$

(c2)(ii). By (c2(i) above, (14) holds also in this case, so that the same proof as that of (b3)(iii) suffices. (Substitute $p \vee q$ and $p^* \vee q^*$ in place of p and p^* in (14), respectively.)

Q.E.D.

Acknowledgment

The writer acknowledges Professor J. McCarthy, of Stanford University, for his valuable suggestions regarding the reinforcement of the formalism. The writer also acknowledges Dr. J. W. de Bakker, of Mathematisch Centrum, for stimulating the refinement of the formalism and for giving interesting examples of derivation in his exposition (de Bakker, 1969). The writer thanks E. Ashcroft for his useful suggestions and critical reading of the manuscript.

Page Intentionally Left Blank

References

Bakker, J. W. de (1968), Axiomatics of Simple Assignment Statements, Report MR94, Mathematisch Centrum, Amsterdam.

_____ (1969), Semantics of Programming Languages, Advances in Information Systems Science 2, Plenum Press.

Engeler, E. (1967), Algorithmic Properties of Structures, Math. Systems Theory 1, pp. 183-195.

Floyd, R. W. (1967), Assigning Meanings to Programs, Proc. of Symposia in Applied Mathematics 19, pp. 19-32.

Hoare, C. A. R. (1969), An Axiomatic Basis for Computer Programming, Communication of the Assoc. for Computing Machinery 12, No. 10, pp. 576-583.

Igarashi, S. (1963), On the Logical Schemes of Algorithms, Information Processing in Japan 3, pp. 12-18.

_____ (1964), An Axiomatic Approach to the Equivalence Problems of Algorithms with Applications, Ph.D. Thesis, University of Tokyo; also
Report of the Computer Centre, University of Tokyo 1 (1968), pp. 1-101; and
Publications of the Research Institute for Mathematical Sciences, Kyoto University B, No. 34 (1969).

_____ (1968), On the Equivalence of Programs Represented by Algol-like Statements, Report of the Computer Centre, University of Tokyo 1, pp. 103-118; also
Publications of the Research Institute for Mathematical Sciences, Kyoto University B, No. 33 (1969).

Kaplan, D. M. (1968), The Formal Theoretic Analysis of Strong Equivalence for Elemental Programs, Ph.D. Thesis, Stanford University.

Łukasiewicz, J. (1941), Die Logik und das Grundlagenproblem, Les Entretiens de Zurich sur les Fondements et la Methode des Sciences Mathematiques, pp. 82-108. (Or, see the below article.)

_____ (1929, English translation of the second edition: 1963), Elements of Mathematical Logic, Pergamon Press, Oxford.

Manna, Z. (1968), Termination of Algorithms, Ph.D. Thesis, Carnegie-Mellon University.

_____ (1969), The Correctness of Programs, Journal of Computer and System Sciences 3, No. 2, pp. 119-127.

_____ and McCarthy, J. (1969), Properties of Programs and Partial Function Logic, Stanford Artificial Intelligence Project Memo AIM-100, Stanford Univ. Also in Machine Intelligence 5 (1970), Edinburgh U.Press.

McCarthy, J. (1963a), A Basis for a Mathematical Theory of Computation, Computer Programming and Formal Systems, North-Holland Publishing Co., Amsterdam, pp. 33-69.

_____ (1963b), Predicate Calculus with "Undefined" as a Truth-Value, Stanford Artificial Intelligence Project, Memo 1.

_____ and Painter, J. (1967), Correctness of a Compiler for Arithmetic Expressions, Proc. of Symposia in Applied Mathematics 19, pp. 34-41.

Naur, P. et al. (1960), Report on the Algorithmic Language ALGOL 60, Communication of Assoc. for Computing Machinery 3, pp. 299-314. Also, Revised Report on the Algorithmic Language ALGOL 60, Communication of the Assoc. for Computing Machinery 6 (1963), pp. 1-17.

Painter, J. A. (1967), Semantic Correctness of a Compiler for an ALGOL-like Language, Ph.D. Thesis, Stanford University.

Rutledge, J. D. (1964), On Ianov's Program Schemata, Journal of Assoc. Computing Machinery 11, pp. 1-9.

Yanov, Y. I. (1958, English edition: 1960), The Logical Schemes of Algorithms, Problems of Cybernetics 1, Pergamon Press, New York, pp. 82-140.