ISE

ISE-TR-90-80

AN ANALYTICAL EQUIVALENCE THEORY OF COMPUTER PROGRAMS

by

Tetsuya Mizutani
Shigeru Igarashi
and
Takashi Tsuji

February 20, 1990

INSTITUTE
OF
INFORMATION SCIENCES AND ELECTRONICS
UNIVERSITY OF TSUKUBA

An analytical equivalence theory of computer programs

by Tetsuya MIZUTANI*, Shigeru IGARASHI** and Takashi TSUJI**
* Department of Information Processing, Saitama College
** Institute of Information Sciences and Electronics, University of Tsukuba

Abstract. A ν-definable act is a program, both logical and procedural, and is almost a specification. Its semantics, called analytic semantics, are given in a completely logical manner. Two concepts of homomorphism between acts, called locomorphism and contralocomorphism, which are generalizations of the concept of equivalence, are introduced. Applications of locomorphism to program verification are discussed.

§ 1. Introduction

In recent decades, verification of programs has become more and more important. Various verification systems for sequential programs have been proposed, for example, Hoare [3], [4], de Bakker [1], Igarashi [5] [6], Igarashi, London and Luckhum [7], so that, in principle, any property of sequential programs can be formally verified now. On the other hand, the various verification systems for parallel programs, for example, Lamport [13], [14], Elrad and Francez [2], Soundararajan [18], depend on the languages of parallel programs being verified, or tend to lose rigorous formalism. Perhaps Kröger's book [12] is one of the few satisfactorily formal presentations of temporal logic applicable to concrete problems. However, his system goes naturally beyond formal number theory as soon as integers are included in the data, so that his system is not so simple as it appears, while it will be obvious that his temporal formulas are just certain abbreviations of our formulas. Moreover, his system deals with only 'interleaving' concurrent processes rather than multi-CPU cases. These are the reasons why we do not use them for the uniform verification method of parallel programs and why we use the *analytic semantics* of the *ν-definable acts* (simply called ν-acts, acts, etc.) [8], [9], [10], [17]. An act is obtained from a logical formula. It is a program which is both logical and procedural,

and is simultaneously a specification. Its semantics are given both simply and precisely on the basis of logic.

We consider that the verification of programs is reduced to the equivalence of programs. A program is 'equivalent' to another if the respective output values of their corresponding variables are the same whenever their input values are. Equivalence ascertains that a program has the same properties as those another that has already been verified. It will be, however, more convenient if we will find some generalizations of the concept of equivalence, especially for parallel programs. This makes us consider *loci* of programs. A locus is a function, in a theoretical sense, from rational numbers as time values to program states, where a state is a function from the set of variables to values. In this paper, we will consider two concepts of morphism called *locomorphism* and *contralocomorphism* from a set of the loci of a program to one of another program. By these concepts we obtain properties of the former from those of the latter whenever verified.

In section 2, the definition of acts and their interpretation will be given. In section 3, we will introduce sets of loci, and define locomorphism, contralocomorphism and equivalence between them. These definitions are independent from acts, and they are useful themselves in the theoretical treatment. In section 4, we will introduce the relationships between acts. In section 5, we will discuss applications of locomorphism and contralocomorphism to programs and programming. In particular, we will discuss the preservations of specifications, the input-output relationship and the termination of programs. In section 6, we will derive locomorphism between acts in examples. Further discussion will be found in section 7.

§2. The ν-conversion

We use a higher type language both to define various data types and to analyze parallel

programs. Because of transparency and capability of developing contemporary real analysis, the formal real analysis FA [19] is chosen as the fundamental mathematical theory. It is a conservative extension of arithmetic developed on the logical system that can be regarded as a 'typed LK'. Specifically, objects of FA are typed abstracts (sets intuitively) starting from rational numbers. (We will use non-arithmetical abstracts, as well as the arithmetical ones permitted in the original FA.) We think that we must deal with rational numbers, at least, both as time values and as data. They are necessary for the former in analysis of parallel programs and for the latter in numerical programs. We prefer totally ordered time to partially ordered time, especially in the theoretical foundation, since the latter always has to be mapped onto the former both practically and theoretically, that is peculiar to computer programs. The formal semantics will be called *analytic semantics*.

2. 1. Definition. Let x, y, z, ... be metavariables denoting free variables. A word of the form νx is called a *qualitative*. For a formula A, an expression obtained from A by substituting at least one qualitative in place of free variables is called a *ν-definable act*. □

There are many interpretations of acts. Here, we adopt an interpretation called a *cosmos* using the *predicate of action*. Hereafter, we suppose that t is the 'time' variable and for a free variable x, $\hat{x}$ is the corresponding higher type variable and $\hat{x}(t)$ represents the value of x at time t. A sequence of variables $\langle x_1, \ldots, x_n \rangle$ is denoted by $\mathbf{x}$ and $\hat{\mathbf{x}}(t)$ will be written as $\mathbf{x}(t)$ when there is no confusion.

2. 2. Definition. For an act $A[\mathbf{x}, \nu\mathbf{x}, t]$, the predicate of action $Pa(A, \hat{\mathbf{x}})$ is the following formula:

$$\forall t \forall \varepsilon > 0((\exists \mathbf{y} A[\hat{\mathbf{x}}(t), \mathbf{y}, t] \supset \exists \delta > 0(\delta < \varepsilon \wedge A[\hat{\mathbf{x}}(t), \hat{\mathbf{x}}(t+\delta), t]))$$

$$\wedge (\forall \delta \geq 0(\delta < \varepsilon \supset \neg \exists \mathbf{y} A[\hat{\mathbf{x}}(t+\delta), \mathbf{y}, t+\delta]) \supset \hat{\mathbf{x}}(t) = \hat{\mathbf{x}}(t+\varepsilon))),$$

which determines $\mathbf{x}$, called a *locus* of A. □

§ 3. Relationship between sets of loci

3. 1. Definition. Let Q^+ be the set of all nonnegative rational numbers, D_1, ..., D_n be the sets of all data of types τ_1, ..., τ_n, respectively, and $D=D_1\times \ldots \times D_n$. Then, a function $\mathbf{x}:Q^+\rightarrow D$ is called *a locus* on D. If there is no confusion, $\hat{\mathbf{x}}$ is simply called a *locus* . □

3. 2. Definition. A locus $\hat{\mathbf{x}}$ is said to *terminate* if and only if it holds that $\exists t\forall u>t(\hat{\mathbf{x}}(t)=\hat{\mathbf{x}}(u))$. □

3. 3. Definition. Let L and L' be sets of loci on D and D', respectively. Then, a function $\varphi:L\rightarrow L'$ is called a *locomorphism* from L to L' if and only if there exist functions $\psi:D\rightarrow D'$ and $\pi: Q^+\rightarrow Q^+$ and it holds that

$$\forall t(\psi(\hat{\mathbf{x}}(t))=\varphi(\hat{\mathbf{x}})(\pi(t)))\wedge\forall t\forall u(t<u\supset\pi(t)\leq\pi(u))\wedge\pi(0)=0\wedge\forall t\exists u(\pi(u)>t)$$

for any locus $\hat{\mathbf{x}}$ belonging to L. A locus L is said to be *locomorphic to L' with respect to* (w. r. t. for simplicity) $<\psi, \pi>$ (See figure 1). □

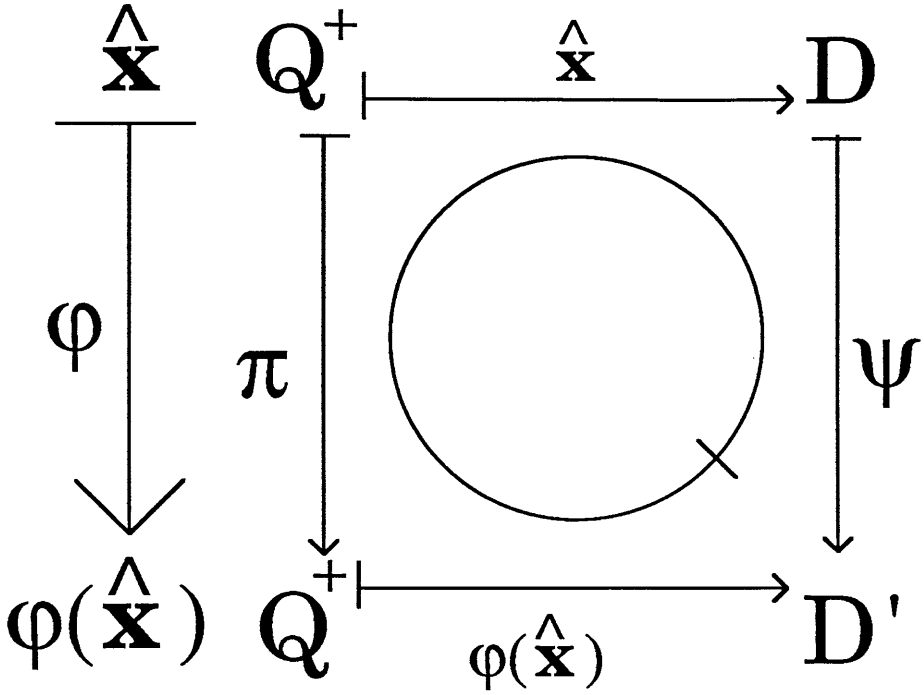

Fig. 1. A commutative diagram of locomorphism.

3. 4. Definition. Let L and L' be sets of loci on D and D', respectively. Then, a function φ:L→L' is called a *contralocomorphism* from L to L' if and only if there exist functions ψ:D'→D and π: $Q^+ \rightarrow Q^+$ and it holds that

$$\forall t(\hat{x}(\pi(t))=\psi(\varphi(\hat{x})(t)))\wedge\forall t\forall u(t<u\supset\pi(t)\leq\pi(u))\wedge\pi(0)=0\wedge\forall t\exists u(\pi(u)>t)$$

for any locus $\hat{x}$ belonging to L. L is said to be *contralocomorphic* to L' w. r. t. $\langle\psi, \pi\rangle$ (See figure 2). □

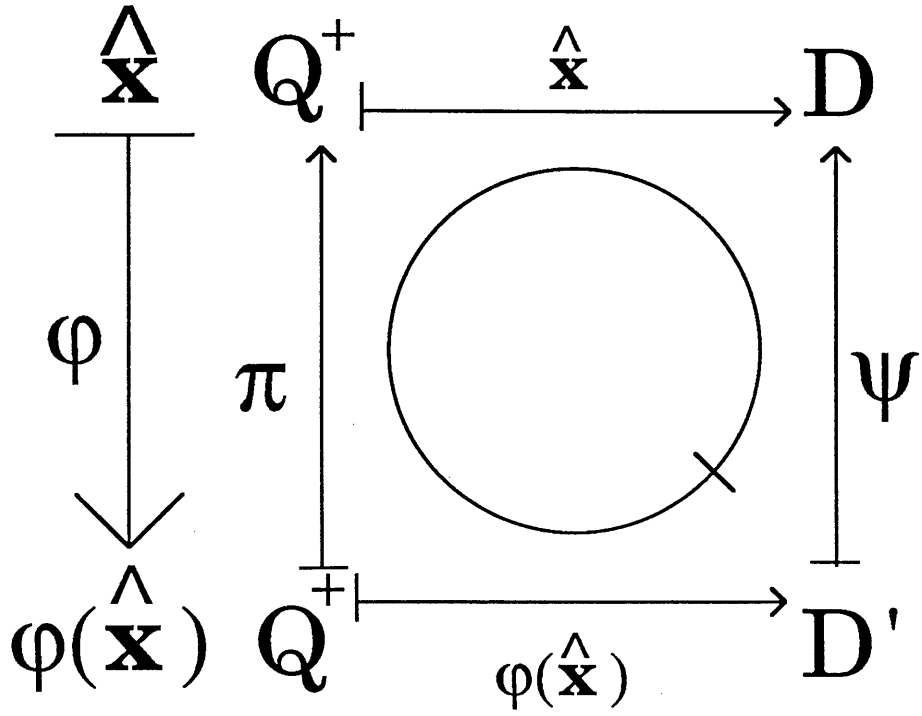

Fig. 2. A commutative diagram of contralocomorphism.

By theorems 3. 5 to 3. 8 below, we obtain a category when objects are sets of loci and morphisms are locomorphisms. In a similar manner, the contralocomorphisms also constitute a category. (Proofs that are evident will be omitted hereafter.)

3. 5. Theorem. An identity function I_L: L $\rightarrow$L is a locomorphism from L to L. □

3. 6. Theorem. If φ is a locomorphism from L to L' and if φ' is a locomorphism from L' to L", then $\varphi' \circ \varphi$ is a locomorphism from L to L". □

3. 7. Theorem. If φ_1, φ_2 and φ_3 be locomorphisms from L to L', from L' to L" and from L" to L"', respectively, then it holds that $\varphi_3 \circ (\varphi_2 \circ \varphi_1)(\hat{x}) = (\varphi_3 \circ \varphi_2) \circ \varphi_1(\hat{x})$ for any $\hat{x} \in L$.

□

3. 8. Theorem. Let $I_{L'}$ be an identity function from L' to L'. If φ and φ' are locomorphisms from L to L' and from L' to L", respectively, then it holds that $I_{L'} \circ \varphi(\hat{x}) = \varphi(\hat{x})$ for any $\hat{x} \in L$ and that $\varphi' \circ I_{L'}(\hat{y}) = \varphi'(\hat{y})$ for any $\hat{y} \in L'$. □

Next, we introduce the concept of equivalence between sets of loci.

3. 9. Definition. Let L and L' be sets of loci on D and D', respectively. Let D_I be $D_1\times \dots \times D_m$ and D_O be $D_1\times \dots \times D_{m'}$, respectively, for some m and m' such that $1\le m\le n$, $1\le m\le n'$, $1\le m'\le n$ and $1\le m'\le n'$. If there exist four projections $\rho_I:D\to D_I$, $\rho'_I:D'\to D_I$, $\rho_O:D\to D_O$ and $\rho'_O:D'\to D_O$, then L is said to be *equivalent* to L' in $<D_I, D_O>$ if and only if

$$\forall\hat{x}\in L\exists\hat{y}\in L'(\rho_I(\hat{x}(0))=\rho'_I(\hat{y}(0))\wedge\exists u\forall t>u(\rho_O(\hat{x}(t))=\rho'_O(\hat{y}(t))))$$

$$\wedge\ \forall\hat{y}\in L'\exists\hat{x}\in L(\rho_I(\hat{x}(0))=\rho'_I(\hat{y}(0))\wedge\exists u\forall t>u(\rho_O(\hat{x}(t))=\rho'_O(\hat{y}(t)))).$$

If L is equivalent to L' in <D, D> in particular, L is simply said to be *equivalent* to L'.

□

Intuitively, L is equivalent to L' in $<D_I, D_O>$ if and only if for any locus $\hat{x}\in L$ there exists a locus $\hat{y}\in L'$ such that $\rho_I(\hat{x}(0))=\rho'_I(\hat{y}(0))$ and $\rho_O(\hat{x}(\infty))=\rho'_O(\hat{y}(\infty))$ (i.e., $\exists u\forall t>u(\rho_O(\hat{x}(t)) = \rho'_O(\hat{y}(t)))$), and vice versa. Specifically, the input and the output values of a certain subsequence of $\hat{x}$ coincide with those of $\hat{y}$.

§ 4. Relationships between ν-definable acts

In this section, we define the concepts of locomorphism, contralocomorphism and equivalence between acts using those between sets of loci introduced in section 3. We recall that any $\hat{x}$ satisfying $Pa(A, \hat{x})$ is a locus, so that $\{\hat{x}|Pa(A, \hat{x})\}$ is a set of loci. Hereafter, type(x) shall denote the type of x.

4. 1. Definition. An act A is said to *terminate* if and only if any locus $\hat{x}$ of A terminates. □

4. 2. Definition. For any pair of acts A and B, a function φ is called a *locomorphism* from A to B on the *precondition* p of A (or 'on p' for simplicity) if and only if φ is a locomorphism from $\{\hat{x}|Pa(A, \hat{x})\wedge p(\hat{x}(0))\}$ to $\{\hat{y}|Pa(B, \hat{y})\}$. An act A is said to be *locomorphic* to an

act B w. r. t. $<\psi, \pi>$ on p if and only if $\{\hat{\mathbf{x}}|Pa(A, \hat{\mathbf{x}})\wedge p(\hat{\mathbf{x}}(0))\}$ is locomorphic to $\{\hat{\mathbf{y}}|Pa(B, \hat{\mathbf{y}})\}$ w. r. t. $<\psi, \pi>$. If $p(\mathbf{x})$ is true for any $\mathbf{x}$, φ is called a locomorphism from A to B and A is said to be locomorphic to B w. r. t. $<\psi, \pi>$.

Similarly, a function φ is called a *contralocomorphism* from A to B on p if and only if φ is a contralocomorphism from $\{\hat{\mathbf{x}}|Pa(A, \hat{\mathbf{x}})\wedge p(\hat{\mathbf{x}}(0))\}$ to $\{\hat{\mathbf{y}}|Pa(B, \hat{\mathbf{y}})\}$. An act A is said to be *contralocomorphic* to an act B *w. r. t.* $<\psi, \pi>$ on p if and only if $\{\hat{\mathbf{x}}|Pa(A, \hat{\mathbf{x}})\wedge p(\hat{\mathbf{x}}(0))\}$ is contralocomorphic to $\{\hat{\mathbf{y}}|Pa(B, \hat{\mathbf{y}})\}$ w. r. t. $<\psi, \pi>$. If $p(\mathbf{x})$ is true for any $\mathbf{x}$, φ is called a contralocomorphism from A to B and A is said to be contralocomorphic to B w. r. t. $<\psi, \pi>$, resepectively. □

Next we introduce the concept of equivalence between acts. Corresponding to the projections used in definition 3. 9, we introduce *input variables* and *output variables* of an acts. We are interested in the values of the former at time 0 and those of the latter on the state when the act terminates. It must be noted that they may not be disjoint.

4. 3. Notation. Whenever we are interested in a sequence $\mathbf{z}$ of variables occurring in $\mathbf{x}$, we may rewrite $\mathbf{x}$ as

$$\mathbf{x}=^*<\mathbf{z}, \mathbf{x}'>,$$

where $=^*$ means the equality of the sequences of variables except for the order of the variables, i.e., the order of the variables of the sequence $\mathbf{x}$ may be different from that of $<\mathbf{z}, \mathbf{x}'>$. If we are interested in two or more sequences of variables $\mathbf{z}$, $\mathbf{z}'$, ... belonging to $\mathbf{x}$, we shall write

$$\mathbf{x}=^*<\mathbf{z}, \mathbf{x}'>=^*<\mathbf{z}', \mathbf{x}''>=^* \ldots .$$

It must be noted that the same variables may occur in both $\mathbf{z}$, $\mathbf{z}'$ and so on. □

4. 4. Definition. Let $\mathbf{x}_I$ and $\mathbf{y}_I$ be $<x_1, \ldots, x_m>$ and $<y_1, \ldots, y_m>$, respectively, where $type(x_i)=type(y_i)$ for each i. Let $\mathbf{x}_O$ and $\mathbf{y}_O$ be $<x'_1, \ldots, x'_k>$ and $<y'_1, \ldots, y'_k>$ respectively, where $type(x'_i)=type(y'_i)$ for each i. Let $\mathbf{x}=^*<\mathbf{x}_I, \mathbf{z}_I>=^*<\mathbf{x}_O, \mathbf{z}_O>$ and $\mathbf{y}=^*<\mathbf{y}_I,$

$\mathbf{w}_I>=*<\mathbf{y}_O, \mathbf{w}_O>$. Then A is said to be *equivalent to* B *on the input variables* $<\mathbf{x}_I, \mathbf{y}_I>$ and *the output variables* $<\mathbf{x}_O, \mathbf{y}_O>$ if and only if

$$\forall\hat{\mathbf{x}}(Pa(A, \hat{\mathbf{x}})\supset\exists\hat{\mathbf{y}}(Pa(B, \hat{\mathbf{y}})\wedge\hat{\mathbf{x}}_I(0)=\hat{\mathbf{y}}_I(0)\wedge\exists u\forall t>u(\hat{\mathbf{x}}_O(t)=\hat{\mathbf{y}}_O(t)))$$

$$\wedge\forall\hat{\mathbf{y}}(Pa(B, \hat{\mathbf{y}})\supset\exists\hat{\mathbf{x}}(Pa(A, \hat{\mathbf{x}})\wedge\hat{\mathbf{x}}_I(0)=\hat{\mathbf{y}}_I(0)\wedge\exists u\forall t>u(\hat{\mathbf{x}}_O(t)=\hat{\mathbf{y}}_O(t))).$$

If A is equivalent to B on the input variables $<\mathbf{x}, \mathbf{y}>$ and the output variables $<\mathbf{x}, \mathbf{y}>$ in particular, we say that A is *equivalent* to an act B for simplicity. □

§ 5. Applications

In this section, we introduce applications of locomorphism, contralocomorphism and equivalence to verification of properties of acts. Throughout this section, for simplicity, we suppose that the preconditions of locomorphisms and contralocomorphisms are true. If an act A is equivalent to an act B on the input variables $<\mathbf{x}_I, \mathbf{y}_I>$ and the output variables $<\mathbf{x}_O, \mathbf{y}_O>$, then it holds that

$$\forall\hat{\mathbf{x}}(Pa(A, \hat{\mathbf{x}})\supset p(\hat{\mathbf{x}}_I(0))\supset\exists u\forall t>u(q(\hat{\mathbf{x}}_O(t))))\equiv\forall\hat{\mathbf{y}}(Pa(B, \hat{\mathbf{y}})\supset p(\hat{\mathbf{y}}_I(0))\supset\exists u\forall t>u(q(\hat{\mathbf{y}}_O(t))))$$

for any formulas p and q.

Similarly, if A is locomorphic to B, then actions of B simulate those of A with appropriate variables of B. We recall that if a function φ is a locomorphism from A to B, then it holds that

$$\forall\hat{\mathbf{x}}(Pa(A, \hat{\mathbf{x}})\supset Pa(B, \varphi(\hat{\mathbf{x}}))).$$

Conversely, if A is locomorphic to B w. r. t. $<\psi, \pi>$ and S is a specification of B, then A also satisfies the specification obtained from S after transforming by φ, ψ and π. Specifically, it holds that

$$\forall\hat{\mathbf{y}}(Pa(B, \hat{\mathbf{y}})\supset S[\hat{\mathbf{y}}])\supset\forall\hat{\mathbf{x}}(Pa(A, \hat{\mathbf{x}})\supset\Phi[S, \varphi, \psi, \pi][\hat{\mathbf{x}}]),$$

where Φ is a transformation of the specification S by φ, ψ and π.

If S is the input-output relationship or the termination in particular, we can define Φ concretely. First, we discuss the preservation of the specifications and the input-output relationships.

5. 1. Theorem. If an act A is locomorphic to an act B w. r. t. $\langle\psi, \pi\rangle$, then it holds that

$$\forall\hat{y}(Pa(B, \hat{y})\supset p(\hat{y}(0))\supset\exists t\forall u{>}t(q(\hat{y}(u))))\supset$$
$$\forall\hat{x}(Pa(A, \hat{x})\supset p(\psi(\hat{x}(0)))\supset\exists t\forall u{>}t(q(\psi(\hat{x}(u)))))$$

for any pair of formulas p and q. □

It must be noted that we do not use the function π in theorem 5. 1 because we are only interested in the values of the input variables at time 0 and those of the output variables at time ∞ when we consider the input-output relationship. By this theorem we can show that if A is locomorphic to B w. r. t. $\langle\psi, \pi\rangle$ and B satisfies the input condition p and the output condition q, then A also satisfies them after mapping the input and the output values of the variables by the function ψ. However, from this fact only, we do not obtain the same input-output relationship satisfied by both A and B. Thus, we introduce the condition that we can derive that two acts satisfy the same input-output relationship.

5. 2. Theorem. If an act A is locomorphic to an act B w. r. t. $\langle\psi, \pi\rangle$ and it holds that

$$\forall\hat{x}(Pa(A, \hat{x})\supset\rho'_I(\psi(\hat{x}(0)))=\rho_I(\hat{x}(0))\wedge\exists t\forall u{>}t(\rho'_O(\psi(\hat{x}(u)))=\rho_O(\hat{x}(u)))), \quad (1)$$

then it holds that

$$\forall\hat{y}(Pa(B, \hat{y})\supset p(\rho'_I(\hat{y}(0)))\supset\exists t\forall u{>}t(q(\rho'_O(\hat{y}(u)))))\supset$$
$$\forall\hat{x}(Pa(A, \hat{x})\supset p(\rho_I(\hat{x}(0)))\supset\exists t\forall u{>}t(q(\rho_O(\hat{x}(u)))))$$

for any pair of formulas p and q. □

The formula (1) is a condition to derive the fact that two acts satisfy the same input-output

relationship. If A is locomorphic to B w. r. t. $\langle\psi, \pi\rangle$, if B is locomorphic to A w. r. t. $\langle\psi', \pi'\rangle$, if ψ satisfies the condition (1) and if ψ' satisfies one similar to (1), then A is equivalent to B. Precisely, theorem 5. 3 shows this fact.

5. 3. Theorem. If an act A is locomorphic to an act B w. r. t. $\langle\psi, \pi\rangle$, if B is locomorphic to A w. r. t. $\langle\psi', \pi'\rangle$, if it holds that

$$\forall\hat{x}(Pa(A, \hat{x})\supset\rho'_I(\psi(\hat{x}(0)))=\rho_I(\hat{x}(0))\wedge\exists t\forall u>t(\rho'_O(\psi(\hat{x}(u)))=\rho_O(\hat{x}(u))))$$

and if

$$\forall\hat{y}(Pa(B, \hat{y})\supset\rho_I(\psi'(\hat{y}(0)))=\rho'_I(\hat{y}(0))\wedge\exists t\forall u>t(\rho_O(\psi'(\hat{y}(u)))=\rho'_O(\hat{y}(u)))),$$

then A is equivalent to B on the input variables $\langle x_I, y_I\rangle$ and the output variables $\langle x_O, y_O\rangle$.

□

Next, we discuss the termination of acts. Again, we do not use π in the discussion on the termination because we are interested in the values of the variables at time ∞.

5. 4. Theorem. If an act A is locomorphic to to an act B w. r. t. $\langle\psi, \pi\rangle$, then it holds that

$$\forall\hat{y}(Pa(B, \hat{y})\supset\exists t\forall u>t(\hat{y}(u)=\hat{y}(t)))\supset$$

$$\forall\hat{x}(Pa(A, \hat{x})\supset\exists t\forall u>t(\psi(\hat{x}(u))=\psi(\hat{x}(t)))).$$

□

Specifically, if A is locomorphic to B w. r. t. $\langle\psi, \pi\rangle$ and B terminates, then for any locus x of A, the value of $\psi(x(t))$ does not change after a certain time.

5. 5. Definition. For an act A, a predicate $term_A(\hat{x}, t)$ satisfying the following formula is called a *termination predicate* of A:

$$\forall\hat{x}(Pa(A, \hat{x})\supset\forall t(term_A(\hat{x}, t)\supset\forall u>t(\hat{x}(u)=\hat{x}(t)))).$$

□

A termination predicate is a sufficient condition of the termination of the corresponding

act. Using this predicate as 'interpolation', we can derive the termination of an act by the following theorem.

5. 6. Theorem. Let $\mathbf{x}=*\langle \mathbf{z}, \mathbf{x}'\rangle$ such that $\hat{\mathbf{x}}(t)\in D$ and $\hat{\mathbf{z}}(t)\in D_0$ for all t. Let ρ : $D\rightarrow D_0$ be a projection. Let $term_A(\hat{\mathbf{x}}, t)$ be a termination predicate of A. If an act A is locomorphic to an act B w. r. t. $\langle\psi, \pi\rangle$, if it holds that $\forall\hat{\mathbf{x}}(Pa(A, \hat{\mathbf{x}})\supset\forall t(\forall u>t(\hat{\mathbf{z}}(u)=\hat{\mathbf{z}}(t))\supset term_A(\hat{\mathbf{x}}, t)))$ and if it holds that $\forall\mathbf{x}_1\in D\forall\mathbf{x}_2\in D(\psi(\mathbf{x}_1)=\psi(\mathbf{x}_2)\supset\rho(\mathbf{x}_1)=\rho(\mathbf{x}_2))$, then it holds that

$$\forall\hat{\mathbf{y}}(Pa(B, \hat{\mathbf{y}})\supset\exists t\forall u>t(\hat{\mathbf{y}}(u)=\hat{\mathbf{y}}(t)))\supset\forall\hat{\mathbf{x}}(Pa(A, \hat{\mathbf{x}})\supset\exists t\forall u>t(\hat{\mathbf{x}}(u)=\hat{\mathbf{x}}(t))).$$

□

Theorem 5. 6 says that if

· A is locomorphic to B w. r. t. $\langle\psi, \pi\rangle$,

· B terminates,

· ψ is identity with respect to the values of $\mathbf{z}$ and

· the fact that values of $\mathbf{z}$ do not change after a certain time implies A terminates,

then A terminates, where $\mathbf{z}$ denotes the *control variables* of A.

In a similar manner to theorems 5. 1 through 5. 6, we can derive theorems 5. 7 thorough 5. 10 on the contralocomorphism.

5. 7. Theorem. If an act A is contralocomorphic to an act B w. r. t. $\langle\psi, \pi\rangle$, then it holds that

$$\forall\hat{\mathbf{y}}(Pa(B, \hat{\mathbf{y}})\supset p(\psi(\hat{\mathbf{y}}(0)))\supset\exists t\forall u>t(q(\psi(\hat{\mathbf{y}}(u)))))\supset$$

$$\forall\hat{\mathbf{x}}(Pa(A, \hat{\mathbf{x}})\supset p(\hat{\mathbf{x}}(0))\supset\exists t\forall u>t(q(\hat{\mathbf{x}}(u))))$$

for any pair of formulas p, q. □

5. 8. Theorem. If an act A is contralocomorphic to an act B w. r. t.$\langle\psi, \pi\rangle$ and it holds that

$$\forall\hat{\mathbf{y}}(Pa(B, \hat{\mathbf{y}})\supset\rho_I(\psi(\hat{\mathbf{y}}(0)))=\rho'_I(\hat{\mathbf{y}}(0))\wedge\exists t\forall u>t(\rho_O(\psi(\hat{\mathbf{y}}(u)))=\rho'_O(\hat{\mathbf{y}}(u)))),$$

then it holds that

$$\forall\hat{\mathbf{y}}(\mathrm{Pa}(\mathrm{B},\hat{\mathbf{y}})\supset p(\rho'_{\mathrm{I}}(\hat{\mathbf{y}}(0)))\supset\exists t\forall u{>}t(q(\rho'_{\mathrm{O}}(\hat{\mathbf{y}}(u)))))\supset$$

$$\forall\hat{\mathbf{x}}(\mathrm{Pa}(\mathrm{A},\hat{\mathbf{x}})\supset p(\rho_{\mathrm{I}}(\hat{\mathbf{x}}(0)))\supset\exists t\forall u{>}t(q(\rho_{\mathrm{O}}(\hat{\mathbf{x}}(u)))))$$

for any pair of formulas p and q. □

5. 9. Theorem. If an act A is contralocomorphic to an act B w. r. t. $\langle\psi, \pi\rangle$, B is contralocomorphic to A w. r. t. $\langle\psi', \pi'\rangle$, it holds that

$$\forall\hat{\mathbf{y}}(\mathrm{Pa}(\mathrm{B},\hat{\mathbf{y}})\supset\rho_{\mathrm{I}}(\psi(\hat{\mathbf{y}}(0)))=\rho'_{\mathrm{I}}(\hat{\mathbf{y}}(0))\wedge\exists t\forall u{>}t(\rho_{\mathrm{O}}(\psi(\hat{\mathbf{y}}(u)))=\rho'_{\mathrm{O}}(\hat{\mathbf{y}}(u))))$$

and that

$$\forall\hat{\mathbf{x}}(\mathrm{Pa}(\mathrm{A},\hat{\mathbf{x}})\supset\rho'_{\mathrm{I}}(\psi'(\hat{\mathbf{x}}(0)))=\rho_{\mathrm{I}}(\hat{\mathbf{x}}(0))\wedge\exists t\forall u{>}t(\rho'_{\mathrm{O}}(\psi'(\hat{\mathbf{x}}(u)))=\rho_{\mathrm{O}}(\hat{\mathbf{x}}(u))))$$

then A is equivalent to B on the input variables $\langle\mathbf{x}_{\mathrm{I}}, \mathbf{y}_{\mathrm{I}}\rangle$ and the output variables $\langle\mathbf{x}_{\mathrm{O}}, \mathbf{y}_{\mathrm{O}}\rangle$.

□

5. 10. Theorem. If an act A is contralocomorphic to an act B w. r. t. $\langle\psi, \pi\rangle$, then it holds that

$$\forall\hat{\mathbf{y}}(\mathrm{Pa}(\mathrm{B},\hat{\mathbf{y}})\supset\exists t\forall u{>}t(\hat{\mathbf{y}}(u)=\hat{\mathbf{y}}(t)))\supset\forall\hat{\mathbf{x}}(\mathrm{Pa}(\mathrm{A},\hat{\mathbf{x}})\supset\exists t\forall u{>}t(\hat{\mathbf{x}}(u)=\hat{\mathbf{x}}(t))).$$

□

Theorem 5. 10 says that if A is contralocomorphic to B and B terminates, then A terminates without any additional condition.

Finally, we show a theorem to derive equivalence between acts from both of the locomorphism and the contralocomorphism.

5. 11. Theorem. If an act A is locomorphic to an act B w. r. t. $\langle\psi, \pi\rangle$, B is contralocomorphic to A w. r. t. $\langle\psi', \pi'\rangle$, it holds that

$$\forall\hat{\mathbf{x}}(\mathrm{Pa}(\mathrm{A},\hat{\mathbf{x}})\supset\rho'_{\mathrm{I}}(\psi(\hat{\mathbf{x}}(0)))=\rho_{\mathrm{I}}(\hat{\mathbf{x}}(0))\wedge\exists t\forall u{>}t(\rho'_{\mathrm{O}}(\psi(\hat{\mathbf{x}}(u)))=\rho_{\mathrm{O}}(\hat{\mathbf{x}}(u))))$$

and that

$$\forall\hat{\mathbf{x}}(\mathrm{Pa}(\mathrm{A},\hat{\mathbf{x}})\supset\rho'_{\mathrm{I}}(\psi'(\hat{\mathbf{x}}(0)))=\rho_{\mathrm{I}}(\hat{\mathbf{x}}(0))\wedge\exists t\forall u{>}t(\rho'_{\mathrm{O}}(\psi'(\hat{\mathbf{x}}(u)))=\rho_{\mathrm{O}}(\hat{\mathbf{x}}(u))))$$

then A is equivalent to B on the input variables $\langle \mathbf{x}_I, \mathbf{y}_I \rangle$ and the output variables $\langle \mathbf{x}_O, \mathbf{y}_O \rangle$.

□

§ 6. Examples

Example 1. Let c_1, c_2, c_3 and n be constants of natural numbers and c_2 be positive. We consider the following 3 acts:

A:: $a(t) \wedge c_2 \leq r \wedge \nu r = r - c_2 \wedge \nu q = q + 1$.

B:: $a(t) \wedge s \leq c_3 \wedge \nu u = u + 1 \wedge \nu s = s + 2\nu u + 1$.

C:: $a(t) \wedge l < n \wedge \nu l = l + 1$.

The formula a(t) is a *spur* expressing a scheduler of each process. The set $\{t \mid a(t)\}$ is discrete. Each of its elements is denoted by t_k ($k \geq 1$). We assume that $0 \leq t_k < t_{k+1}$ for every k. The act A computes a quotient q and a remainder r of c_1 by c_2, where c_1 is an initial value of r. The act B computes the integral part of the square root of c_3. Specifically, $c_1 = q \cdot c_2 + r$ and $u = [\sqrt{c_3}]$. The act C is a loop that simply counts l. The functions $\psi_1 : \langle q, r \rangle \mapsto l$ and $\psi_2 : l \mapsto \langle s, u \rangle$ are given by $l = (c_1 - r)/c_2$ and $\langle s, u \rangle = \langle (l+1)^2, l \rangle$, respectively, and the function ψ is by $\psi_2 \circ \psi_1$. The function I_t is identity from Q^+ to Q^+. The formulas p_1, p_2 are given by $p_1(r, q) \equiv N((c_1 - r)/c_2)$ and $p_2(l) \equiv N(l)$, respectively, where N(x) denotes that x is a natural number. For a formula F, F[t+0] means that $\forall \varepsilon > 0 \exists \delta (0 < \delta < \varepsilon \wedge F[t+\delta])$ and $F[\infty]$ does that $\exists t \forall u > t (F[u])$.

6. 1. Assertion. For any locus $\langle r, q \rangle$ of A, if $p_1(r(0), q(0))$, then it holds that $p_1(r(t), q(t))$ for all t.

Proof. We show this by induction on k such that $a(t_k)$. It holds that $p_1(r(t_1), q(t_1))$ since $r(0) = r(t_1)$ and $q(0) = q(t_1)$ from the predicate of action.

Assume that $p_1(r(t_k), q(t_k))$. We consider 2 cases where $c_2 \leq r(t_k)$ and $c_2 > r(t_k)$.

If $c_2 \leq r(t_k)$, then $r(t_k+0)=r(t_k)- c_2$, which implies $(c_1-r(t_k+0))/c_2=(c_1-r(t_k))/c_2+1$. Hence, $N((c_1-r(t_k+0))/c_2)$, i.e., $p_1(r(t_{k+1}), q(t_{k+1}))$ holds.

If $c_2>r(t_k)$, then $r(t_k+0)=r(t_k)$, which implies $p_1(r(t_{k+1}), q(t_{k+1}))$.

Therefore, it holds that $p_1(r(t), q(t))$ for all t. □

6. 2. Assertion. If $[c_1/c_2]=n$ then A is locomorphic to C w. r. t. $<\psi_1, I_t>$ on p_1.

Proof. We show that l given by $l(t)=(c_1-r(t))/c_2$ is a locus of C by induction on k such that $a(t_k)$.

Assume that $l(t_k)=(c_1-r(t_k))/c_2$. First, we show that $c_2 \leq r(t_k) \equiv l(t_k)<n$. From the assumption, $l(t_k)-[c_1/c_2]$ is $c_1/c_2-[c_1/c_2]- r(t_k)/c_2$. It is trivial that $0 \leq c_1/c_2-[c_1/c_2]<1$. If $c_2 \leq r(t_k)$ then $l(t_k)-[c_1/c_2]<0$, i.e., $l(t_k)<[c_1/c_2]=n$. Conversely, if $l(t_k)<n$ then $l(t_k)-[c_1/c_2]<0$. Because $N(l(t_k))$ holds by assertion 6. 1, $l(t_k)-[c_1/c_2]$ is less that or equal to -1. Hence, it holds that $c_1/c_2-[c_1/c_2]+1 \leq r(t_k)/c_2$, which implies $1 \leq r(t_k)/c_2$, i.e., $c_2 \leq r(t_k)$. Therefore, $c_2 \leq r(t_k) \equiv l(t_k)<n$.

If $c_2 \leq r(t_k)$ then $r(t_k+0)$ is $r(t_k)- c_2$, which implies $(c_1-r(t_k+0))/c_2=(c_1-r(t_k))/c_2+1$. On the other hand, $l(t_k)<n$ implies $l(t_k+0)=l(t_k)+1$. Hence, it holds that $l(t_k+0)=(c_1-r(t_k+0))/c_2$, i.e., $l(t_{k+1})=(c_1-r(t_{k+1}))/c_2$. □

6. 3. Assertion. If $n=[\sqrt{c_3}]$ then C is locomorphic to B w. r. t. $<\psi_2, I_t>$ on p_2.

Proof. We show that $<s, u>$ given by $<s(t), u(t)>=<(l(t)+1)^2, l(t)>$ is a locus of B by induction on t satisfying a(t).

Assume that $<s(t_k), u(t_k)>=<(l(t_k)+1)^2, l(t_k)>$. First, we show that $s(t_k) \leq c_3 \equiv l(t_k)<n$. It is evident that $N(l(t_k))$ holds. If $s(t_k) \leq c_3$ then $l(t_k)+1 \leq \sqrt{c_3}$. It holds that $l(t_k)+1 \leq [\sqrt{c_3}]$ because $N(l(t_k))$ holds. Hence, $l(t_k)<[\sqrt{c_3}]=n$. Conversely, $l(t_k)<n$ implies $l(t_k) \leq n-1=[\sqrt{c_3}]-1$. Hence, it holds that $l(t_k)+1 \leq [\sqrt{c_3}] \leq \sqrt{c_3}$, i.e., $s(t_k)= (l(t_k)+1)^2 \leq c_3$. Therefore, $s(t_k) \leq c_3 \equiv l(t_k)<n$.

If $l(t_k)<[\sqrt{c_3}]$ then $l(t_k+0)$ is $l(t_k)+1$ and $<s(t_k+0), u(t_k+0)>$ are $<s(t_k)+2u(t_k)+3, u(t_k)+1>$, which imply $s(t_k+0) = l(t_k)^2+4l(t_k)+4 = (l(t_k)+2)^2 = (l(t_k+0)+1)^2$. Hence, it holds that $<s(t_{k+1}), u(t_{k+1})>=<(l(t_{k+1})+1)^2, l(t_{k+1})>$. □

6. 4. Assertion. If $[c_1/c_2]=[\sqrt{c_3}]$ then A is locomorphic to B w. r. t. $<\psi, I_t>$ on p_1.

Proof. It is trivial that $p_1(r, q)$ is equivalent to $p_2(\psi_1(r, q))$. Hence, it holds that $\{r, q \mid Pa(A, <r, q>)\wedge p_1(r(0), q(0))\}$ is locomorphic to $\{l \mid Pa(C, l) \wedge p_2(l(0))\}$ w. r. t. $<\psi_1, I_t>$ from assertion 6. 2. Therefore, A is locomorphic to B w. r. t. $<\psi, I_t>$ on p_1 by theorem 3. 6.

□

6. 5. Assertion. Let $[c_1/c_2]=[\sqrt{c_3}]$. If $s(0)=1\wedge u(0)=0$ implies $u(\infty)=[\sqrt{c_3}]$ then $r(0)=c_1$ implies $(c_1-r(\infty))/c_2=[c_1/c_2]$.

Proof. By theorem 5. 1. □

Example 2. Let α be an array of type [0, 0]. The value of each element $\alpha(1), \ldots, \alpha(n)$ is either 0 or 1 and both $\alpha(0)$ and $\alpha(n+1)$ are equal to 1. The acts P_1 and P_2 are the following, each of which checks whether $\forall i\in\{1, \ldots, n\}.\alpha(i)=1$ or not:

$$P_1:: ((a_1(t)\wedge\exists z\exists w R_1[x, y; z, w] \supset R_1[x, y; vx, vy])$$

$$\wedge (a_2(t)\wedge\exists z\exists w R_2[x, y; z, w] \supset R_2[x, y; vx, vy]))^{\#}$$

and

$$P_2: :b(t)\wedge T[v, D; vv, vD],$$

where

$$R_1[x, y; x', y']:: \alpha(x)\cdot\alpha(y)=1\wedge x'<y\wedge x'=x+1,$$

$$R_2[x, y; x', y']:: \alpha(x)\cdot\alpha(y)=1 \wedge x<y'\wedge y'=y-1$$

and

$$T[v, D; v', D']:: v=1\wedge\exists z(z\in\{0, \ldots, n+1\}-D\wedge D'=D+\{z\}\wedge v'=\alpha(z))$$

respectively. The symbol # is the *sharping* operator given in [9]. For an act A, actions of $A^{\#}$ keep values of the variables as long as possible in accordance with a certain optimization strategy called the *principle of the least action.*

The function $\psi : \langle x, y\rangle \mapsto \langle v, D\rangle$ is given by

$$v=\alpha(x)\cdot\alpha(y),$$

and

$$D=\begin{cases}\{0, \ldots, x\}\cup\{y, \ldots, n+1\}, & \text{if } \alpha(x)\neq 0 \text{ or } \alpha(y)\neq 0,\\ \{0, \ldots, x-1\}\cup\{y, \ldots, n+1\}, & \text{if } \alpha(x)=\alpha(y)=0.\end{cases}$$

U[x, y] is the formula

$$N(x)\wedge N(y)\wedge 0\leq x\leq y\leq n+1\wedge\alpha(x)\in\{0, 1\}\wedge\alpha(y)\in\{0, 1\}.$$

Although P_1 would be executed with the initial value $\langle x(0), y(0)\rangle=\langle 0, n+1\rangle$ in practice, we assume only U[x(0), y(0)] for the purpose of explanation.

6. 6. Assertion. P_1 is locomorphic to P_2 w. r. t. $\langle\psi, \pi\rangle$ on U for some π and for any combination of spurs a_1, a_2 and b.

Proof. The proof is given in [10]. □

§7. Discussion

We have introduced the concepts of locomorphism, contralocomorphism and equivalence between acts and have given some applications. The locomorphism and the contralocomorphism are extensions of 'homomorphism' of programs and of their 'simulation' discussed by McCarthy, Milner, etc., in the late 1960's [15], [16]. We verify specifications of a parallel program by investigating images of the locomorphism.

Acknowledgements. This work was supported in part by the Grant-in-Aid for the

Scientific Research of Ministry of Education, Science and Culture (Nos. 62302005 and 01750315).

References.

[1] de Bakker, J. W.: *Mathematical theory of program correctness*, Prentice-Hall, Englewood Cliffs, NJ, 1980.

[2] Elrad, T. and Francez, N.: A weakest precondition semantics for communicating processes, *Theor. Comput. Sci.*, 29 (1984), pp. 231-250.

[3] Hoare, C. A. R.: An axiomatic basis for computer programming, *Comm. ACM*, Vol. 12, No. 10 (1969), pp. 579-580, 583.

[4] Hoare, C. A. R.: Procedures and parameters: an axiomatic approach, In Engeler, E. (ed.), *Symposium on semantics of algorithmic language, Lecture notes in Mathematics* 188, Berlin-Heidelberg-New York:Springer (1971), pp. 102-116.

[5] Igarashi, S.: An axiomatic approach to the equivalence problems of algorithms with applications, *Rep. Compt, Univ. Tokyo*, 1 (1968), pp. 1-101.

[6] Igarashi, S.: A natural deduction system for assertion, in M. Nivat (ed.), *théorie des algorithmes des langages et de la programmation, Séminaires IRIA* (1974), pp. 39-45.

[7] Igarashi, S., London, R. L. and Luckhum, D. C.: Automatic program verification I: a logical basis and its implementation, *Acta Inform.*, 4 (1975), pp. 145-182.

[8] Igarashi, S.: The ν-conversion and an analytic semantics, *Inf. Proc.* 83, R. E. A. Mason (ed.), Elsevier Science Publishers B.V. (North-Holland), IFIP (1983), pp. 769-774.

[9] Igarashi, S., Mizutani T. and Tsuji T.: An analytical semantics of parallel program system by ν-conversion, *Tensor, N. S.*, Vol. 45 (1987), pp. 222-228.

[10] Igarashi, S., Mizutani T. and Tsuji T.: Specifications of parallel program processes in an-

alytical semantics, *Tensor, N. S.*, Vol. 45 (1987), pp. 240-244.

[11] Igarashi, S., Tsuji T. and Mizutani T.: A sufficient condition for two programs to be locomorphic in analytical equivalence theory, to appear.

[12] Kröger, F.: *Temporal logic of programs*, Springer-Verlag, 1987.

[13] Lamport, L.: What good is temporal logic?, *Inf. Proc.* 83, R. E. A. Mason (ed.), Elsevier Science Publishers B.V. (North-Holland), IFIP (1983), pp. 657-668.

[14] Lamport, L.: Specifying concurrent program modules, *ACM Trans. of Prog. Lang. Syst.*, Vol. 5, No. 2 (1983), pp. 190-222.

[15] McCarthy, J.: Priv. comm., 1969.

[16] Milner, R.: Priv. comm., 1969.

[17] Mizutani, T., Hosono, C, and Igarashi, S.: Verification of programs using ν-definable acts, *Computer Software*, Vol. 2, No. 3 (1985), pp. 529-538 (in Japanese).

[18] Soundararajan, N.: Denotational semantics of CSP, *Theor. Comput., Sci.*, 33 (1984), pp. 279-304.

[19] Takeuti, G.: *Two applications of logic to Mathematics*, Princeton University Press, 1978.

INSTITUTE OF INFORMATION SCIENCES AND ELECTRONICS
UNIVERSITY OF TSUKUBA
TSUKUBA-SHI, IBARAKI 305 JAPAN

REPORT DOCUMENTATION PAGE

REPORT NUMBER
ISE-TR-90-80

TITLE

An analytical equivalence theory of computer programs

AUTHOR(S)

Tetsuya MIZUTANI*, Shigeru IGARASHI** and Takashi TSUJI**

* Department of Information Processing, Saitama College

** Institute of Information Sciences and Electronics, University of Tsukuba

REPORT DATE
February 20th, 1990

NUMBER OF PAGES
19

MAIN CATEGORY
Theory of Computation

CR CATEGORIES
F.3.1, F.3.2, D.2.4

KEY WORDS

analytic semantics, ν-definable act, locomorphism, contralocomorphism, equivalence

ABSTRACT

A ν-definable act is a program, both logical and procedural, and is almost a specification. Its semantics, called analytic semantics, are given in a completely logical manner. Two concepts of homomorphism between acts, called locomorphism and contralocomorphism, which are generalizations of the concept of equivalence, are introduced. Applications of locomorphism to program verification are discussed.

SUPPLEMENTARY NOTES