STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM
REKENAFDELING

MR 94

Axiomatics of simple assignment statements

by

J.W. de Bakker

The Mathematical Centre at Amsterdam, founded the 11th of February, 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.) and the Central Organization for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

1. Introduction

Machine independent programming languages contain a large number of concepts which form a source of inspiration for mathematical investigation. In this introduction we first make a few historical remarks on the work which has been performed concerning theoretical properties of programming languages, and then give a summary of the contents of our paper, which contains a study of an important concept in programming, i.e. the assignment statement.

During the first years of the development of programming languages, little attention was paid to theoretical considerations. The first language, FORTRAN, was not very suitable for this purpose, since most concepts were not yet introduced in their full generality, and many exceptions obscured the possibilities of mathematical analysis. The introduction of ALGOL 60, and especially the use in its definition of the syntactic formalism of Backus, initiated the first extensive theoretical investigations. These investigations were initially mainly concerned with syntactical problems. The theory of context free languages, introduced by Chomsky for the study of natural languages, was developed further. This theory has many important applications in the construction of compilers and the automation of the syntactical analysis of programs. Much less attention has been paid to semantical problems. By this we mean theories which deal with the meaning of programs. Such theories are of importance e.g. for the formal definition of programming languages, for the construction of compilers, and for proving the correctness of programs. For a survey of the work in this field we refer to [1] and [2]. We restrict ourselves here to a few remarks.

The theory of computability, i.e. of Turing machines, recursive functions etc., is since long an important branch of mathematical logic. There is of course no doubt that this theory has led to many fundamental results, which are also applicable to the semantics of programming languages. However, there are many basic notions in programming which have no direct counterpart in the theory of computability. Therefore, several other approaches have been proposed, not directly related to this theory, but corresponding more closely to the essential concepts

of programming. (For references see [1] and [2].)
In this paper we use the axiomatic method, which has, up to now, been rather neglected. This method was, as far as we know, first used by S. Igarashi in his Ph.D. thesis: "An axiomatic approach to the equivalence problems of algorithms, with applications" [4]. Igarashi introduces axiom systems, with corresponding rules of inference, for assignment statements, conditional constructions, and goto statements, and then gives several applications. The basis of his axiom system is the notion of equivalence. The above mentioned concepts are defined implicitly by the way in which the equivalence of (sequences of) statements is defined. He also proves several completeness theorems which are, in a sense, a guarantee that his axiom systems confirm to our "a priori" knowledge of these concepts.
For a recent paper, advocating the axiomatic approach, see [3].

Our paper is restricted to an analysis of simple assignment statements. Section 2 contains the definitions of a variable, a (sequence of) assignment statement(s), and some auxiliary concepts.
In section 3 we introduce the axiom system, consisting of four axioms and three rules of inference, and we derive several fundamental properties of assignment statements from this system. In particular, we prove some theorems on the interchanging of the values of two or more variables.
In section 4 we prove the completeness and independence of our axiom system. We introduce a function which defines the effect of a sequence of assignment statements upon a variable, and then prove that our system is complete in the following sense: The equivalence of two sequences of assignment statements can be derived from the axiom system if and only if they have the same effect upon each variable. Next, we show that the axiom system is independent, by exhibiting, for each axiom $A_i (1 \leq i \leq 4)$, a property (P_i), which is shared by the axioms $A_j (1 \leq j \leq 4, j \neq i)$, which is preserved by the rules of inference, but is such that A_i does not have property (P_i).
The results of sections 5 and 6 are more of purely mathematical interest. In section 5 we investigate the possibility of replacing the set of axioms introduced in section 3 by a smaller set. First we show that

three axioms suffice, and then we introduce an infinity of pairs of axioms, each "equipollent" with the system of section 3 (i.e. the same equivalences can be derived from them).
Section 6 contains some results on axiom systems which are closely related to the systems of section 5. However, it turns out that some of these systems are not equipollent with the original system, whereas the equipollence of the remaining systems with the original system is still an open problem. The last theorem of this section shows that the concept of the interchanging of the values of two variables is fundamental.

As mentioned above, the idea of using the axiomatic method, and also the idea of a completeness proof, are due to Igarashi. However, we have defined a considerably simpler axiom system (this was possible mainly because of the use of a more powerful rule of inference); also, most theorems (exceptions are lemmas 3.1 to 3.4 and theorem (4.1.1) and all proofs are new.
A judgment on the merits of the axiomatic method in the theory of semantics can only be given after (much) more study. The present paper may be considered as a first experiment.

2. Definitions

Let V be an infinite set. The elements of V will be denoted by lower case letters, possibly with indices, e.g. a, b, ..., s_1, t_1, ..., x, y, z, etc.

Let V^2 be the set of all ordered pairs of elements of V, i.e. elements of V^2 are pairs such as (a, b), (s_1, t_1), (x, y), etc. For shortness sake, however, we shall use in the sequel the simpler notation ab, s_1t_1, xy, etc.

Let V^{2*} be the set of all finite non-empty sequences of elements of V^2, i.e. elements of V^{2*} are e.g. ab cd, pq, x_1y_1 z_2t_2, ab bc ca, etc. Arbitrary elements of V^{2*} are denoted by S, S_1, S_2, S_3, etc.

Definition 2.1.

1. The elements of V are called variables.
2. The elements of V^2 are called assignment statements.
3. The elements of V^{2*} are called sequences of assignment statements.

The elements of V correspond to the (simple) variables of e.g. ALGOL 60; the elements of V^2 to assignment statements such as a:=b, s_1:=t_1, x:=y, etc., and the elements of V^{2*} to sequences of assignment statements such as a:=b; c:=d; p:=q; x_1:=y_1; z_2:=t_2, or a:=b; b:=c; c:=a, etc. (Since we are not interested in this paper in syntactical problems, we suppose that variables are always denoted by only one letter, possibly with an index. We do not introduce identifiers; hence, a sequence such as ab cd can only be interpreted as a:=b; c:=d, and not as ab:=cd.)

Apparently, we only consider "simple" assignment statements, i.e. assignment statements containing nothing but variables. Some reasons for this restriction are:

1. We feel that most of the essential properties of "simple" assignment statements, i.e. assignment statements with expressions on the right-hand side, are already contained in this simple case.
2. It simplifies the mathematical analysis of the following sections considerably.

Definition 2.2. The functions $p_i : V^2 \to V$ $(i = 1, 2)$ are defined as follows:
Let $S \in V^2$. Then, for $i = 1, 2$, $p_i(S)$ is the i-th element of the ordered pair denoted by S.

Definition 2.3. Let $S \in V^{2*}$. The set of left parts of S, $\lambda(S)$, and the set of right parts of S, $\rho(S)$, are defined as follows:
1. If $S \in V^2$, then $\lambda(S) = \{p_1(S)\}$, and $\rho(S) = \{p_2(S)\}$.
2. If $S = S_1S_2$, $S_1 \in V^2$, $S_2 \in V^{2*}$, then
   $\lambda(S) = \lambda(S_1) \cup \lambda(S_2)$, and
   $\rho(S) = \rho(S_1) \cup \rho(S_2)$.

Definition 2.4. Let $S \in V^{2*}$. The length $l(S)$ of S is defined as follows:
1. If $S \in V^2$, then $l(S) = 1$.
2. If $S = S_1S_2$, $S_1 \in V^2$, $S_2 \in V^{2*}$, then $l(S) = 1 + l(S_2)$.

Definition 2.5. The functions $f_i : V^{2*} \to V$ $(i = 1, 2)$ are defined as follows:
1. If $S \in V^2$, then $f_i(S) = p_i(S)$, $i = 1, 2$.
2. If $S = S_1S_2$, $S_1 \in V^2$, $S_2 \in V^{2*}$, then $f_i(S) = f_i(S_1)$, $i = 1, 2$.

(Clearly, $f_i(S)$ is the first variable occurring in S, and $f_2(S)$ the second.)

Definition 2.6. Let S_i, $1 \leq i \leq n$, be elements of V^{2*}.
$\prod_{i=1}^{n} S_i$ is defined as follows:
$\prod_{i=1}^{1} S_i = S_1$, and $\prod_{i=1}^{n} S_i = \prod_{i=1}^{n-1} S_i \, S_n$, for $n \geq 2$.
We shall also use obvious notations such as $\prod_{\substack{i=1 \\ i \neq j}}^{n} S_i$, etc. If it is clear from the context which bounds are meant, they are occasionally omitted.

Definition 2.7. $\prod_{i=1}^{n} S$ is denoted by $(S)^n$.

3. An axiom system for assignment statements

We now introduce the axiom system for assignment statements in terms of the equivalence relation "~".
The axiom system consists of the axioms A_1 to A_4, and the rules of inference R_1, R_2 and R_3.

A_1 : For all a, $b \in V$:
    ab ba ~ ab.

A_2 : For all a, b, $c \in V$:
    ab ac ~ ac, provided that $a \neq c$.

A_3 : For all a, b, $c \in V$:
    ab ca ~ ab cb.

A_4 : For all a, b, $c \in V$:
    ab cb ~ cb ab.

R_1 : For all S_1, $S_2 \in V^{2*}$:
    If there exist a, b, c, $d \in V$, $a \neq b$, such that S_1 ac ~ S_2 ac and S_1 bd ~ S_2 bd, then $S_1 \sim S_2$.

R_2 : For all S, S_1, S_2, $S_3 \in V^{2*}$:
    a. S ~ S.
    b. If $S_1 \sim S_2$, then $S_2 \sim S_1$.
    c. $S_1 \sim S_2$ and $S_2 \sim S_3$ imply $S_1 \sim S_3$.

R_3 : For all S, S_1, $S_2 \in V^{2*}$:
    $S_1 \sim S_2$ implies $SS_1 \sim SS_2$ and $S_1S \sim S_2S$.

Remarks:

1. It is clear that axioms A_1 to A_4 correspond to properties of assignment statements as used in programming languages.
2. Rule R_1 may be understood intuitively as follows:
   If two sequences of assignment statements S_1 and S_2 have the following properties:
   a. they attribute the same values to all variables which occur in their left parts, with the possible exception of the variable a, and
   b. they attribute the same values to all variables which occur in their left parts, with the possible exception of the variable b($b \neq a$),
   then S_1 and S_2 attribute the same values to all variables

occurring in their left parts, i.e., they are equivalent. (Of course, this interpretation of rule R_1 will not be used in the formal theory below; e.g. we do not yet know what it means that an assignment statement attributes a value to a variable.)

3. The rules R_2 and R_3 will be used in the sequel without explicit mentioning.

Definition 3.1.

1. The set of axioms $\{A_1, A_2, A_3, A_4\}$ is denoted by $\mathcal{A}$.
2. The left-hand side and right-hand side of the axioms A_1, A_2, A_3, A_4 are denoted by:

   A_{l1} = ab ba, A_{r1} = ab,
   A_{l2} = ab ac, A_{r2} = ac,
   A_{l3} = ab ca, A_{r3} = ab cb,
   A_{l4} = ab cb, A_{r4} = cb ab.

Lemma 3.1. If $a \neq c$, $a \neq d$ and $b \neq c$, then ab cd ~ cd ab.
(In this and the following lemmas or theorems we omit the obvious clauses such as: for all a, b, c, $d \in V$ ...).

Proof

(1) ab cd cb ~ ab cb ($b \neq c$)	, A_2,
(2) cd ab cb ~ cd cb ab	, A_4,
(3) cd cb ab ~ cb ab ($b \neq c$)	, A_2,
(4) ab cd cb ~ cd ab cb ($b \neq c$)	, (1), (2), (3), A_4,
(5) ab cd ad ~ cd ab ad ($a \neq d$)	, (4) with a and c, and b and d interchanged,

(6) ab cd ~ cd ab ($a \neq c$, $a \neq d$, $b \neq c$) , (4), (5) and R_1.

Lemma 3.2. If $\lambda(S_1) \cap \lambda(S_2) = \lambda(S_1) \cap \rho(S_2) = \lambda(S_2) \cap \rho(S_1) = \emptyset$, then $S_1S_2 \sim S_2S_1$.

Proof. By repeated application of lemma 3.1.
(Using the completeness theorem of section 4.1, it can be proved that the assertion of the lemma also holds with "if" replaced by "only if".)

Lemma 3.3. aa bc ~ bc aa ~ bc.

Proof.

1. First we show that aa bc ~ bc.

(1)	aa bc ac ~ aa ac bc ~ ac bc $(a \neq c)$	, A_4, A_2,
(2)	bc ac ~ ac bc	, A_4,
(3)	aa bc ac ~ bc ac $(a \neq c)$	, (1), (2),
(4)	aa bc ba ~ aa ba ~ ba aa ~ ba ab ~ ba $(a \neq b)$	, A_2, A_4, A_3, A_1,
(5)	bc ba ~ ba $(a \neq b)$	, A_2
(6)	aa bc ba ~ bc ba $(a \neq b)$	, (4), (5),
(7)	aa bc ~ bc $(a \neq b,\ a \neq c)$	, (3), (6), R_1,
(8)	aa ac ~ ac $(a \neq c)$	, A_2,
(9)	aa ba ~ ba aa ~ ba ab ~ ba	, A_4, A_3, A_1,
(10)	aa bc ~ bc	, (7), (8), (9).

2. Now we prove that bc aa ~ bc.

(11)	bc aa ~ aa bc ~ bc $(a \neq b,\ a \neq c)$	, lemma 3.1 and part 1,
(12)	ac aa ~ ac ac ~ ac $(a \neq c)$	, A_3, A_2,
(13)	ba aa ~ ba ab ~ ba	, A_3, A_1,
(14)	bc aa ~ bc	, (11), (12), (13).

Lemma 3.4. aa S ~ S aa ~ S.

Proof. Follows by lemma 3.3.

The next lemmas are concerned with sequences of assignment statements which interchange the values of two (or more) variables. It is known that in order to achieve this, one must use an auxiliary variable. In lemma 3.5, we prove that, in a sense, this variable may be chosen freely.

Lemma 3.5. xa ab bx yx ~ ya ab by xy $(x \neq a, b$ and $y \neq a, b)$.

(x and y are the auxiliary variables which are used for the interchange of the values of a and b).

Proof. xa ab bx yx ~ xa ab yx bx ~ xa yx ab bx ~
xa ya ab bx ~ ya xa ab bx ~ ya xy ab bx ~
ya ab xy bx ~ ya ab xy by ~ ya ab by xy.

(by repeated use of A_3 and lemma 3.1).

Lemma 3.6 shows the effect of two successive interchanges of the values of b and c:

Lemma 3.6. ab bc ca ab bc ca ~ ac (a ≠ c).

Proof. It is easy to verify that the assertion holds if a = b or b = c. Now suppose that a, b, c differ from each other. Let x, y, z be three variables, different from a, b, c. Then:

ab bc ca ab bc ca ax by ~ ab bc ca ab bc by ca ax ~
ab bc ca ab by ca ax ~ ab bc ca ab ca by ax ~
ab bc ca ab cb by ax ~ ab bc ca cb ab by ax ~
ab bc cb ab by ax ~ ab bc ab by ax ~ ab bc ac by ax ~
ab ac bc by ax ~ ac by ax ~ ac ax by.

Hence,

(1) ab bc ca ab bc ca ax by ~ ac ax by.

Similarly, we prove that

(2) ab bc ca ab bc ca ax cz ~ ac ax cz,

and

(3) ab bc ca ab bc ca by cz ~ ac by cz.

By (1), (2) and R_1,

(4) ab bc ca ab bc ca ax ~ ac ax.

By (1), (3) and R_1,

(5) ab bc ca ab bc ca by ~ ac by.

By (4), (5) and R_1,

ab bc ca ab bc ca ~ ac.

Remark. Lemma 3.6 is a fundamental property of assignment statements. In fact, we can show that it may replace axiom A_2:

(1) ab ab ~ ab ba ab ~ ab ba ~ ab , A_1, A_1, A_1,

(2) ab ac ~ ab ab bc ca ab bc ca ~
ab bc ca ab bc ca ~ ac (a ≠ c) , lemma 3.6, (1), lemma 3.6.

Hence, A_2 can be proved from the remaining axioms, together with lemma 3.6.

It is easy to show that lemma 3.6 is equivalent with:

ab bc ca ab ~ ac cb ba.

Lemma 3.7. gives a generalization of this result:

Lemma 3.7. For each integer $n \geq 2$, and each i, $1 \leq i < n$:

$ax_1\ x_1x_2\ x_2x_3\ \ldots\ x_{n-1}x_n\ x_na\ ax_i \sim$

$ax_{i+1}\ x_{i+1}x_{i+2}\ \ldots\ x_nx_1\ \ldots\ x_{i-1}x_i\ x_ia$

$(a \neq x_i,\ 1 \leq i \leq n$, and $x_i \neq x_j,\ 1 \leq i, j \leq n)$.

The proof of this lemma will not be given here. We might give a proof similar to that of lemma 3.6. However, the lemma will follow almost immediately as a result of the completeness theorem of section 4.1.

The next lemma is an example taken from a class of equivalences which can all be proved using the completeness theorem. However, we give here another proof which uses only lemmas 3.6 and 3.7.

Lemma 3.8. ab bc ca ad de ea ab bc ca ad de ea ~ ae ($a \neq e$ and $\{b, c\} \cap \{d, e\} = \emptyset$).

Proof. It is easy to verify that the lemma holds for a = b, a = c, a = d, b = c or d = e. From now on we suppose that a, b, c, d, e are all different.

Let S = ab bc ca ad de ea ab bc ca ad de ea.

By lemma 3.6:

ad ~ ac cd da ac cd da. Hence,

S ~ ab bc ca ac cd da ac cd da de ea ab bc ca ad de ea

~ ab bc cd da ac cd de ea ab bc ca ad de ea.

By lemma 3.7:

ab bc cd da ac ~ ad db bc ca. Hence,

S ~ ad db bc ca cd de ea ab bc ca ad de ea

~ ad db bc cd de ea ab bc ca ad de ea.

By lemma 3.7:

bc cd de ea ab bc ~ bd de ea ac cb. Hence,

S ~ ad db bd de ea ac cb ca ad de ea

~ ad db de ea ac ca ad de ea

~ ad de ea ad de ea

~ ae, by lemma 3.6.

4. Completeness and independence of the axiom system

In this section we prove the completeness and independence of the axiom system which was introduced in section 3. The sense in which the notion of "completeness" is meant here, will be made precise below.

4.1. Completeness of the axiom system.

In section 3 we showed that several basic properties of assignment statements can be derived from the axioms A_1 to A_4 by means of the rules of inference R_1 to R_3. However, two important questions concerning this axiom system were not yet discussed:

1. Is it possible to derive an equivalence $S_1 \sim S_2$ from the system which contradicts our "à priori" notion of the meaning of assignment?
2. If two sequences S_1 and S_2 are equivalent according to our "à priori" notion of assignment, is it then possible to derive this equivalence from the axiom system?

In order to answer these questions, it is necessary to make precise our intuitive notion of the meaning of assignment. This is done by the following definition:

Definition 4.1. The function $E : V \times V^{2*} \to V$ is defined (recursively) by:

1. Let $a \in V$ and $S \in V^2$. Then
   $E(a, S) = p_2(S)$, if $a = p_1(S)$,
   $\quad = a \quad$, if $a \neq p_1(S)$ (cf. def. 2.2.)
2. Let $a \in V$ and $S = S_1S_2$, with $S_1 \in V^{2*}$ and $S_2 \in V^2$. Then
   $E(a, S) = E(E(a, S_2), S_1)$.

It is clear that the function E describes the effect of a (sequence of) assignment statement(s) upon a variable, as it is defined in programming languages. E.g. the effect of b := c upon the variable a is:

if $a = b$, then a has from now on the value of c;

if $a \neq b$, then a keeps its value.

The recursive clause in the definition of E is also in agreement with the usual definition of assignment statements.

Lemma 4.1. Let S_1, $S_2 \in V^{2*}$ and $a \in V$. Then
$E(a, S_1S_2) = E(E(a, S_2), S_1)$.

Proof. Follows easily from the definition of E.

We now state the completeness theorem:

Theorem 4.1.1. Let S_1, S_2 be two sequences of assignment statements. Then the following two assertions are equivalent:

1. $S_1 \sim S_2$.
2. For all $a \in V$: $E(a, S_1) = E(a, S_2)$.

For the proof we need the following auxiliary theorem:

Theorem 4.1.2. Let $S \in V^{2*}$, $\lambda(S) = \{a_1, a_2, \ldots, a_m\}$, $m \geq 1$. Let X be a subset of V such that $X \cap \lambda(S) = \emptyset$. Then for each i, $1 \leq i \leq m$, and each $x_1, x_2, \ldots, x_m \in X$:

$$S \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j \sim a_i\ E(a_i, S) \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j.$$

(The idea of this theorem was already used in the proof of lemma 3.6. For the definition of "Π", see definition 2.6.)

Proof. We use induction on the length of S.

1. $l(S) = 1$, i.e. $S = ab$, for some $a, b \in V$. Then, clearly, $ab \sim aE(a, ab)$.

2. Let the assertion be proved for all $S' \in V^{2*}$ with $l(S') = n$. Now consider an element S of V^{2*} with $l(S) = n+1$. Then $S = S'\ ab$, for some $ab \in V^2$, and $S' \in V^{2*}$ with $l(S') = n$. Let $\lambda(S') = \{a_1, a_2, \ldots, a_m\}$, $m \leq n$. We distinguish two cases, $a \in \lambda(S')$, and $a \notin \lambda(S')$.

2.1. $a \in \lambda(S')$, i.e. $a = a_k$, for some k, $1 \leq k \leq m$.
We have to prove that for each i, $1 \leq i \leq m$:

$$(1) \quad S'\ a_k b \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j \sim a_i\ E(a_i, S'\ a_k b) \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j.$$

Again there are two possibilities, $a_i = a_k$ and $a_i \neq a_k$.

2.1.1. $a_i = a_k$. We distinguish three cases:

(α) $b \notin \lambda(S')$. Then we have:

$$S' \ a_i b \prod_{j \neq i} a_j x_j \sim S' \prod_{j \neq i} a_j x_j \ a_i b \sim a_i \ E(a_i, S') \prod_{j \neq i} a_j x_j \ a_i b \sim$$

$$a_i \ E(a_i, S') \ a_i b \prod_{j \neq i} a_j x_j \sim a_i b \prod_{j \neq i} a_j x_j,$$

by repeated use of lemma 3.2, by the induction hypothesis, and by A_2. On the other hand,

$$a_i \ E(a_i, S' \ a_i b) \prod_{j \neq i} a_j x_j \sim a_i \ E(b, S') \prod_{j \neq i} a_j x_j \sim a_i b \prod_{j \neq i} a_j x_j,$$

since it is clear that $E(b, S') = b$, if $b \notin \lambda(S')$.
We conclude that $S' \ a_i b \prod_{j \neq i} a_j x_j \sim a_i \ E(a_i, S' \ a_i b) \prod_{j \neq i} a_j x_j$; hence, (1) holds.

(β) $b = a_i$. Then

$$S' \ a_i a_i \prod_{j \neq i} a_j x_j \sim S' \prod_{j \neq i} a_j x_j, \text{ and}$$

$$a_i \ E(a_i, S' \ a_i a_i) \prod_{j \neq i} a_j x_j \sim a_i \ E(a_i, S') \prod_{j \neq i} a_j x_j.$$

However,

$$S' \prod_{j \neq i} a_j x_j \sim a_i \ E(a_i, S') \prod_{j \neq i} a_j x_j, \text{ by the induction hypothesis.}$$

Hence, (1) also holds in this case.

(γ) $b = a_h$, for some h, $1 \leq h \leq m$, $h \neq i$. Then (1) becomes:

(2) $$S' \ a_i a_h \prod_{j \neq i} a_j x_j \sim a_i \ E(a_i, S' \ a_i a_h) \prod_{j \neq i} a_j x_j.$$

Let x_i be an arbitrary element of X. Then:

$$S' \ a_i a_h \prod_{j \neq i} a_j x_j \sim S' \ a_i x_i \ a_i a_h \prod_{j \neq i} a_j x_j \sim$$

$$S' \ a_i x_i \ a_i a_h \prod_{j \neq i,h} a_j x_j \ a_h x_h \sim S' \ a_i x_i \prod_{j \neq i,h} a_j x_j \ a_i a_h \ a_h x_h \sim$$

$$S' \prod_{j \neq h} a_j x_j \ a_i a_h \ a_h x_h \sim \text{(ind. hyp.)} \ a_h \ E(a_h, S') \prod_{j \neq h} a_j x_j \ a_i a_h \ a_h x_h \sim$$

$$a_h \ E(a_h, S') \prod_{j \neq h,i} a_j x_j \ a_i x_i \ a_i a_h \ a_h x_h \sim$$

$$a_h \ E(a_h, S') \prod_{j \neq h,i} a_j x_j \ a_i a_h \ a_h x_h \sim$$

$$a_h\ E(a_h,\ S')\ a_i a_h \prod_{j\neq h,i} a_j x_j\ a_h x_h \sim$$

$$a_h\ E(a_h,\ S')a_i\ E(a_h,\ S') \prod_{j\neq h,i} a_j x_j\ a_h x_h \sim$$

$$a_i\ E(a_h,\ S')\ a_h\ E(a_h,\ S')\ a_h x_h \prod_{j\neq h,i} a_j x_j \sim$$

$a_i\ E(a_h,\ S')\ a_h x_h \prod_{j\neq h,i} a_j x_j \sim a_i\ E(a_h,\ S') \prod_{j\neq i} a_j x_j$. Hence,

$S'\ a_i a_h \prod_{j\neq i} a_j x_j \sim a_i\ E(a_h,\ S') \prod_{j\neq i} a_j x_j$. Also,

$$a_i\ E(a_i,\ S'\ a_i a_h) \prod_{j\neq i} a_j x_j \sim a_i\ E(a_h,\ S') \prod_{j\neq i} a_j x_j.$$

This proves (2).

2.1.2. $a_i \neq a_k$. Here we have to prove:

(3) $\quad S'\ a_k b \prod_{j\neq i} a_j x_j \sim a_i\ E(a_i,\ S'\ a_k b) \prod_{j\neq i} a_j x_j.$

However,

$S'\ a_k b \prod_{j\neq i} a_j x_j \sim S' \prod_{j\neq i} a_j x_j \sim a_i\ E(a_i,\ S') \prod_{j\neq i} a_j x_j$, by the induction hypothesis. Also,

$$a_i\ E(a_i,\ S'\ a_k b) \prod_{j\neq i} a_j x_j \sim a_i\ E(a_i,\ S') \prod_{j\neq i} a_j x_j.$$

This proves (3).

2.2. $a \notin \lambda(S')$, i.e. $\lambda(S) = \{a_1,\ a_2,\ \ldots,\ a_m,\ a_{m+1}\}$, with $a = a_{m+1}$.

We now have to prove:

(4) $\quad S'\ ab \prod_{\substack{j=1\\ j\neq i}}^{m+1} a_j x_j \sim a_i\ E(a_i,\ S'\ ab) \prod_{\substack{j=1\\ j\neq i}}^{m+1} a_j x_j.$

We distinguish the cases $a_i = a_{m+1}$ and $a_i \neq a_{m+1}$.

2.2.1. $a_i = a_{m+1}$. Thus, (4) becomes:

$$S'\ ab \prod_{j=1}^{m} a_j x_j \sim a_i\ E(a_i,\ S'\ ab) \prod_{j=1}^{m} a_j x_j.$$

(α) $\quad b \notin \{a_1,\ a_2,\ \ldots,\ a_{m+1}\}$. Then

$S'\ ab \prod_{j=1}^{m} a_j x_j \sim S' \prod_{j=1}^{m} a_j x_j\ ab$. By the induction hypothesis

$S' \prod_{j=1}^{m} a_j x_j \sim \prod_{j=1}^{m} a_j x_j$. Hence,

(5) $S'\ ab \prod_{j=1}^{m} a_j x_j \sim \prod_{j=1}^{m} a_j x_j\ ab$. Also,

(6) $a_i\ E(a_i, S'\ ab) \prod_{j=1}^{m} a_j x_j \sim a_i\ E(b, S') \prod_{j=1}^{m} a_j x_j \sim$

$ab \prod_{j=1}^{m} a_j x_j \sim \prod_{j=1}^{m} a_j x_j\ ab$, since $a = a_i$, and $b \notin \lambda(S')$.

From (5) and (6), (4) follows.

(β) $b = a = a_{m+1}$. Then

$$S'\ ab \prod_{j=1}^{m} a_j x_j \sim S' \prod_{j=1}^{m} a_j x_j \sim \prod_{j=1}^{m} a_j x_j \text{ (induction hypothesis)},$$

and

$$a_i\ E(a_i, S'\ ab) \prod_{j=1}^{m} a_j x_j \sim a_i\ E(b, S') \prod_{j=1}^{m} a_j x_j \sim$$

$$a_i b \prod_{j=1}^{m} a_j x_j \sim \prod_{j=1}^{m} a_j x_j \text{ (since } b \notin \lambda(S'),\ E(b, S') = b).$$

Hence, (4) follows.

(γ) $b = a_h$, for some h, $1 \leq h \leq m$.

The proof of this case is similar to 2.1.1. (γ).

2.2.2. $a_i \neq a_{m+1}$. We have

$$S'\ ab \prod_{\substack{j=1 \\ j\neq i}}^{m+1} a_j x_j \sim S' \prod_{\substack{j=1 \\ j\neq i}}^{m+1} a_j x_j \sim S' \prod_{\substack{j=1 \\ j\neq i}}^{m} a_j x_j\ a_{m+1} x_{m+1} \sim$$

$$a_i\ E(a_i, S') \prod_{\substack{j=1 \\ j\neq i}}^{m} a_j x_j\ a_{m+1} x_{m+1} \sim a_i\ E(a_i, S'\ ab) \prod_{\substack{j=1 \\ j\neq i}}^{m+1} a_j x_j.$$

This proves (4).

Thus, the proof of theorem 4.1.2. is completed.

We can now give the proof of theorem 4.1.1.

<u>Proof of theorem 4.1.1.</u>

1. First we show: $S_1 \sim S_2$ implies that for all $a \in V$: $E(a, S_1) = E(a, S_2)$. It is easy to verify that for all $a \in V$: $E(a, A_{li}) = E(a, A_{ri})$, $i = 1, 2, 3, 4$ (cf. definition 3.1). Clearly, it is now sufficient to prove that this property is preserved by application of the rules of inference. First we consider rule R_1. Suppose that $S_1\ ac \sim S_2\ ac$,

$S_1bd \sim S_2\, bd$ ($a \neq b$), and that for all $e \in V$: $E(e, S_1\, ac) = E(e, S_2\, ac)$, and $E(e, S_1\, bd) = E(e, S_2\, bd)$. We show that then for all $e \in V$: $E(e, S_1) = E(e, S_2)$. First suppose $e \neq a$. Then $E(e, S_1) = E(e, S_1 ac) = E(e, S_2 ac) = E(e, S_2)$. If $e = a$, then $E(e, S_1) = E(e, S_1\, bd) = E(e, S_2\, bd) = E(e, S_2)$. The proof that R_2 preserves the above mentioned property is also straightforward. Finally, we show that R_3 preserves this property. Suppose that $S_1 \sim S_2$, and that for all $a \in V$: $E(a, S_1) = E(a, S_2)$. Then for all $S \in V^{2*}$: $E(a, SS_1) = E(E(a, S_1), S) = E(E(a, S_2), S) = E(a, SS_2)$ by lemma 4.1. Similarly, for all S: $E(a, S_1S) = E(a, S_2S)$.

2. Now suppose that for all $a \in V$: $E(a, S_1) = E(a, S_2)$. We prove that then $S_1 \sim S_2$. Without loss of generality we may assume that $\lambda(S_1) = \lambda(S_2)$, say $\lambda(S_1) = \lambda(S_2) = \{a_1, a_2, \ldots, a_m\}$ (if e.g. $a_i \in \lambda(S_1)$, $a_i \notin \lambda(S_2)$, then replace S_2 by $S_2\, a_i a_i$, etc). Let $X \subset V$ be such that $X \cap \lambda(S_1) = \emptyset$. By theorem 4.1.2 we have, for $x_1, x_2, \ldots, x_m \in X$, and for each i, $1 \leq i \leq m$:

$$S_1 \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j \sim a_i\, E(a_i, S_1) \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j, \text{ and}$$

$$S_2 \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j \sim a_i\, E(a_i, S_2) \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j.$$

Since $E(a_i, S_1) = E(a_i, S_2)$, we conclude that

$$S_1 \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j \sim S_2 \prod_{\substack{j=1 \\ j \neq i}}^{m} a_j x_j.$$

From this we obtain, for example,

$$S_1 \prod_{j=1}^{m-2} a_j x_j\, a_{m-1} x_{m-1} \sim S_2 \prod_{j=1}^{m-2} a_j x_j\, a_{m-1} x_{m-1}, \text{ and}$$

$$S_1 \prod_{j=1}^{m-2} a_j x_j\, a_m x_m \sim S_2 \prod_{j=1}^{m-2} a_j x_j\, a_m x_m.$$

Application of R_1 gives: $S_1 \prod_{j=1}^{m-2} a_j x_j \sim S_2 \prod_{j=1}^{m-2} a_j x_j$.

Generally, we can prove:

For each $\{j_1, j_2\} \subset \{1, 2, \ldots, m\}$:

$$S_1 \prod_{\substack{j=1 \\ j \neq j_1, j_2}}^{m} a_j x_j \sim S_2 \prod_{\substack{j=1 \\ j \neq j_1, j_2}}^{m} a_j x_j.$$

Repeating the argument gives, for some h, k, $1 \leq h, k \leq m$, $h \neq k$:
$S_1 \, a_h x_h \sim S_2 \, a_h x_h$, and
$S_1 \, a_k x_k \sim S_2 \, a_k x_k$.
Application of R_1 yields $S_1 \sim S_2$.
This completes the proof of theorem 4.1.1.

4.2. Independence of the axiom system.

In order to prove the independence of our axiom system, we need some new concepts and notations.
First we introduce an auxiliary function:
Let N be the set of non-negative integers.

Definition 4.2.1. The function $F: V \times V^{2*} \to N$, is defined (recursively) by:
1. Let $a \in V$ and $S \in V^2$. Then
$F(a, S) = 1$, if $a = p_1(S)$, and $a \neq p_2(S)$,
$= 0$, otherwise.
2. Let $a \in V$ and $S = S_1 S_2$, with $S_1 \in V^{2*}$ and $S_2 \in V^2$. Then
$F(a, S) = F(a, S_2) + F(E(a, S_2), S_1)$.

Example: Let a, b, c, d, be four different variables. Then
F(b, ab ca bc) = F(b, bc) + F(E(b, bc), ab ca) = 1 + F(c, ab ca) =
1 + F(c, ca) + F(E(c, ca), ab) = 2 + F(a, ab) = 3.
F(d, ab ca bc) = 0.

F(a, S) may be described to yield the number of non-trivial steps which have to be made in order to obtain the final value which is attributed to a by S.

Lemma 4.2.1. Let $S_1, S_2 \in V^{2*}$ and $a \in V$. Then:
$F(a, S_1 S_2) = F(a, S_2) + F(E(a, S_2), S_1)$.

Proof. Follows easily from the definition of F.

Definition 4.2.2. The sets of axioms $\mathcal{A} \setminus \{A_i\}$, i = 1, 2, 3, 4, are denoted by $\mathcal{A}_i$.

In the remainder of this section and in the following sections we shall consider sets of axioms for assignment statements which differ from the set $\mathcal{A}$. (The rules of inference R_1, R_2 and R_3 remain unchanged throughout the whole paper.) Therefore, the following notation is introduced:

Definition 4.2.3. Let $\mathfrak{F}$ be a set of axioms for assignment statements, and let $S_1, S_2 \in V^{2*}$.
$\mathfrak{F} \vdash S_1 \sim S_2$ means that the equivalence of S_1 and S_2 can be derived from the set of axioms $\mathfrak{F}$ by application of the rules of inference R_1, R_2 and R_3.
(i.e. $\vdash$ has the usual meaning of mathematical logic).

Usually, it will be clear from the context which set of axioms is meant. Explicit mentioning of the set of axioms is then omitted. E.g. in the preceding sections, $S_1 \sim S_2$ always meant $\mathcal{A} \vdash S_1 \sim S_2$.

We now prove the independence of the axiom system $\mathcal{A}$, by means of four lemmas:

Lemma 4.2.2. A_1 is independent of A_2, A_3 and A_4.

Proof. Suppose that $\mathcal{A}_1 \vdash S_1 \sim S_2$. We shall show that then S_1 and S_2 have the following property:
(P_1) : $\lambda(S_1) = \lambda(S_2)$.
It is easily seen that A_{li} and A_{ri} $i = 2, 3, 4$, have property (P_1).
Next, we prove that (P_1) is preserved by rule R_1: Suppose that $\mathcal{A}_1 \vdash S_1\ ac \sim S_2\ ac$, and $\mathcal{A}_1 \vdash S_1\ bd \sim S_2\ bd$, $a \neq b$, and suppose that $S_1\ ac$ and $S_2\ ac$, and $S_1\ bd$ and $S_2\ bd$ have property (P_1). This means that $\lambda(S_1) \cup \{a\} = \lambda(S_2) \cup \{a\}$, and $\lambda(S_1) \cup \{b\} = \lambda(S_2) \cup \{b\}$. Since $a \neq b$, it follows that $\lambda(S_1) = \lambda(S_2)$; hence, S_1 and S_2 have property (P_1).
That R_2 and R_3 preserve (P_1) follows immediately from the definition of (P_1). Since $\lambda(ab\ ba) = \{a, b\} \neq \{a\} = \lambda(ab)$, A_1 does not have property (P_1). Thus, A_1 is independent of A_2, A_3 and A_4.

Lemma 4.2.3. A_2 is independent of A_1, A_3 and A_4.

Proof. Suppose that $\mathcal{A}_2 \vdash S_1 \sim S_2$. Then S_1 and S_2 have the following property:
(P_2) : $f_2(S_1) = f_2(S_2)$ (cf. definition 2.5).

Clearly, this holds for A_1, A_3 and A_4. The proof that R_1, R_2 and R_3 preserve (P_2) is also straightforward. Since $f_2(ab\ ac) = b \neq c = f_2(ac)$, it follows that A_2 is independent of A_1, A_3 and A_4.

Lemma 4.2.4. A_3 is independent of A_1, A_2 and A_4.

Proof. Suppose that $\mathfrak{A}_3 \vdash S_1 \sim S_2$. Then S_1 and S_2 have the following property:

(P_3): For all $a \in V$: $F(a, S_1) + F(a, S_2) \equiv 0$ (mod. 2).

It is again easy to verify that A_1, A_2 and A_4 have property (P_3), and that (P_3) is preserved by application of the rules of inference. As an example, we prove: If S_1 and S_2 have property (P_3), then so have SS_1 and SS_2: Choose $a \in V$. Then $F(a, SS_1) + F(a, SS_2) = F(a, S_1) + F(E(a, S_1), S) + F(a, S_2) + F(E(a, S_2), S)$. However, $F(a, S_1) + F(a, S_2) \equiv 0$ (mod. 2). Also, $E(a, S_1) = E(a, S_2)$; hence, $F(E(a, S_1), S) = F(E(a, S_2), S)$. We conclude that $F(a, SS_1) + F(a, SS_2) \equiv 0$ (mod. 2). Since $F(c, ab\ ca) + F(c, ab\ cb) = 2 + 1 = 3 \not\equiv 0$ (mod. 2), it follows that A_3 is independent of A_1, A_2 and A_4.

Lemma 4.2.5. A_4 is independent of A_1, A_2 and A_3.

Proof. Suppose that $\mathfrak{A}_4 \vdash S_1 \sim S_2$. Then S_1 and S_2 have the following property:

(P_4) : $f_1(S_1) = f_1(S_2)$ (cf. definition 2.5).

This can be shown as above. Since $f_1(ab\ cb) = a \neq c = f_1(cb\ ab)$, it follows that A_4 is independent of A_1, A_2 and A_3.

Theorem 4.2. The axiom system $\mathfrak{A}$ is independent.

Proof. Follows from lemmas 4.2.2, 4.2.3, 4.2.4, and 4.2.5.

5. Equipollent axiom systems

In this section we investigate several (in fact, an infinity of) smaller sets of axioms for assignment statements, and we prove that from these systems the same equivalences can be derived as from $\mathcal{A}$. (We do not change the rules of inference R_1, R_2 and R_3.)

Definition 5.1. Let $\mathcal{F}_1$, $\mathcal{F}_2$ be two sets of axioms for assignment statements. $\mathcal{F}_1 \Rightarrow \mathcal{F}_2$ is used as an abbreviation for : For all S_1, $S_2 \in V^{2*}$, we have: $\mathcal{F}_1 \vdash S_1 \sim S_2$ implies that $\mathcal{F}_2 \vdash S_1 \sim S_2$.
The sets of axioms $\mathcal{F}_1$ and $\mathcal{F}_2$ are called equipollent, denoted by $\mathcal{F}_1 \Leftrightarrow \mathcal{F}_2$, if $\mathcal{F}_1 \Rightarrow \mathcal{F}_2$ and $\mathcal{F}_2 \Rightarrow \mathcal{F}_1$.

It is easy to show that the number of axioms can be reduced to three:

Definition 5.2. $\mathcal{B} = \{B_1, B_2, B_3\}$ consists of the following axioms:
B_1 : ab ba ~ ab , i.e., $B_1 = A_1$;
B_2 : ab ac ~ ac $(a \neq c)$, i.e., $B_2 = A_2$;
B_3 : ab ca ~ cb ab.

Lemma 5.1. $\mathcal{A} \Leftrightarrow \mathcal{B}$.

Proof.
1. Clearly, $\mathcal{A} \vdash$ ab ca ~ cb ab. Hence, $\mathcal{B} \Rightarrow \mathcal{A}$.
2. In order to prove that $\mathcal{A} \Rightarrow \mathcal{B}$, it is sufficient to show that $\mathcal{B} \vdash A_3$ and $\mathcal{B} \vdash A_4$. This is shown as follows:

(1) ab ca ac ~ cb ab ac , B_3,
(2) ab ca ~ cb ac $(a \neq c)$, (1), B_1, B_2,
(3) ab aa ~ ab aa ,
(4) ab ca ~ cb ac , (2), (3),
(5) cb ac ~ cb ab , B_3, (4).
Hence, $\mathcal{B} \vdash A_3$.
(6) ab ca ~ ab cb , A_3
(7) ab cb ~ cb ab , (6), B_3.
Hence, $\mathcal{B} \vdash A_4$.

We now introduce sets of axioms, each consisting of only two elements (definitions 5.3, 5.4 and 5.5).

Definition 5.3. Let n be an integer ≥ 1.

$\mathcal{C}_n = \{C_{1,n}, C_2\}$ consists of the following two axioms:

$C_{1,n}$: $(ab\ ca\ bc)^n \sim cb\ ab$, (cf. definition 2.7),

C_2 : $ab\ ac \sim ac\ (a \neq c)$, i.e. $C_2 = A_2$.

Theorem 5.1. For each integer $n \geq 1$, $\mathcal{C}_n \Longleftrightarrow \mathcal{A}$.

Proof.

1. In order to prove that $\mathcal{C}_n \Rightarrow \mathcal{A}$, for each $n \geq 1$, it is sufficient to show that $\mathcal{A} \vdash (ab\ ca\ bc)^n \sim cb\ ab$. However, $ab\ ca\ bc \sim ab\ cb\ bc \sim ab\ cb \sim cb\ ab$. Hence, $(ab\ ca\ bc)^n \sim (cb\ ab)^n \sim (cb)^n\ (ab)^n \sim cb\ ab$.

2. We now show that $\mathcal{A} \Rightarrow \mathcal{C}_n$.

(1)	$(ab\ ca\ bc)^n\ bc \sim cb\ ab\ bc$	, $C_{1,n}$,
(2)	$(ab\ ca\ bc)^n\ bc \sim (ab\ ca\ bc)^n\ (b \neq c)$	, C_2,
(3)	$cb\ ab\ bc \sim cb\ ab\ (b \neq c)$	, (1), (2), $C_{1,n}$,
(4)	$(ab\ ca\ bc)^n\ ab \sim cb\ ab\ ab$	, $C_{1,n}$,
(5)	$(ab\ ca\ bc)^n\ ab \sim ab(ca\ bc\ ab)^n \sim ab\ ba\ ca$	, $C_{1,n}$,
(6)	$cb\ ab\ ab \sim ab\ ba\ ca$	, (4), (5),
(7)	$ab\ ab\ ba \sim ab\ ab\ (a \neq b)$	, (3) with $a = c$,
(8)	$ab\ ba \sim ab\ (a \neq b)$	, (7), C_2,
(9)	$bb\ ab\ ab \sim ab\ ba\ ba$	, (6) with $b = c$,
(10)	$bb\ ab \sim ab\ (a \neq b)$	, (8), (9), C_2,
(11)	$aa\ aa\ ab \sim aa\ ab\ (a \neq b)$	, C_2,
(12)	$aa\ aa\ ba \sim aa\ ba\ (a \neq b)$	, (10)
(13)	$aa\ aa \sim aa$	, (11), (12), R_1,
(14)	$ab\ ba \sim ab$	, (8), (13).
	Hence, $\mathcal{C}_n \vdash A_1$.	
(15)	$ab\ ab \sim ab$	, C_2, (13),
(16)	$cb\ ab \sim ab\ ca$	, (6), (14), (15).

By (16), we can now apply lemma 5.1, from which we conclude that $\mathcal{C}_n \vdash A_3$ and $\mathcal{C}_n \vdash A_4$.

Definition 5.4. Let n be an integer ≥ 1.

$\mathcal{D}_n = \{D_{1,n}, D_2\}$ consists of the following two axioms:

$D_{1,n}$: $(ab\ ca\ bc)^n\ ab \sim cb\ ac$,

D_2 : $ab\ ac \sim ac\ (a \neq c)$, i.e. $D_2 = A_2$.

Theorem 5.2. For each $n \geq 1$, $\mathfrak{D}_n \iff \mathcal{A}$.

Proof.

1. In order to prove that $\mathfrak{D}_n \Rightarrow \mathcal{A}$, it is sufficient to show that $\mathcal{A} \vdash (ab\ ca\ bc)^n\ ab \sim cb\ ac$. As above, we have $(ab\ ca\ bc)^n \sim cb\ ab$. Hence, $(ab\ ca\ bc)^n\ ab \sim cb\ ab\ ab \sim cb\ ab \sim cb\ ac$.

2. We now show that $\mathcal{A} \Rightarrow \mathfrak{D}_n$.

(1) $(ab\ ca\ bc)^n\ ab\ ab \sim cb\ ac\ ab$, $D_{1,n}$,
(2) $(ab\ ca\ bc)^n\ ab\ ab \sim (ab\ ca\ bc)^n\ ab\ (a \neq b)$, D_2,
(3) $cb\ ab \sim cb\ ac\ (a \neq b)$, (1), (2), $D_{1,n}$, D_2,
(4) $(ab\ ca\ bc)^n\ ab\ ca \sim cb\ ac\ ca$, $D_{1,n}$,
(5) $(ab\ ca\ bc)^n\ ab\ ca \sim ab(ca\ bc\ ab)^n\ ca \sim ab\ ba\ cb$, $D_{1,n}$,
(6) $cb\ ac\ ca \sim ab\ ba\ cb$, (4), (5),
(7) $cb\ ac\ ca \sim cb\ ab\ ca\ (a \neq b)$, (3),
(8) $cb\ ab\ ca \sim cb\ ab\ cb\ (b \neq c)$, (3),
(9) $cb\ ab\ cb \sim ab\ ba\ cb\ (a \neq b,\ b \neq c)$, (6), (7), (8),
(10) $ab\ ab\ ab \sim ab\ ba\ ab\ (a \neq b)$, (9),
(11) $ab\ ab \sim ab\ ba\ ab\ (a \neq b)$, (10), D_2,
(12) $ab\ ba \sim ab\ ba\ ba\ (a \neq b)$, D_2,
(13) $ab \sim ab\ ba\ (a \neq b)$, (11), (12), R_1,
(14) $ba\ aa \sim ba\ ab$, (3),
(15) $ba\ aa \sim ba\ (a \neq b)$, (14), (13),
(16) $bb\ ab\ ba \sim ab\ ba\ bb$, (6) with $b = c$,
(17) $bb\ ab \sim ab\ bb$, (16), (13),
(18) $bb\ ab \sim ab\ (a \neq b)$, (17), (15),
(19) $aa\ aa\ ab \sim aa\ ab\ (a \neq b)$, D_2,
(20) $aa\ aa\ ba \sim aa\ ba\ (a \neq b)$, (18),
(21) $aa\ aa \sim aa$, (19), (20), R_1,
(22) $ab\ ba \sim ab$, (13), (21).

Hence, $\mathfrak{D}_n \vdash A_1$.

(23) $cb\ ac \sim ab\ cb$, (6), (22).

From (23) and lemma 5.1 it follows that $\mathfrak{D}_n \vdash A_3$ and $\mathfrak{D}_n \vdash A_4$.

Definition 5.5. Let n be an integer ≥ 1.

$\mathcal{E}'_n = \{E'_{1,n}, E'_2\}$ consists of the following two axioms:

$E'_{1,n}$: $(ab\ ca\ bc)^n\ ab\ ca \sim cb\ ac$,
E'_2 : $ab\ ac \sim ac\ (a \neq c)$, i.e. $E'_2 = A_2$.

$\mathcal{E}''_n = \{E''_{1,n}, E''_2\}$ consists of the following two axioms:
$E''_{1,n}$: $(ab\ ca\ bc)^n\ ab\ ca \sim cb\ ab$,
E''_2: $ab\ ac \sim ac\ (a \neq c)$, i.e. $E''_2 = A_2$.

Theorem 5.3. For each $n \geq 1$, $\mathcal{E}'_n \Longleftrightarrow \mathcal{A}$.

Proof.

1. As above, it follows that $\mathcal{A} \vdash E'_{1,n}$, i.e. $\mathcal{E}'_n \Rightarrow \mathcal{A}$.
2. We now show that $\mathcal{A} \Rightarrow \mathcal{E}'_n$.

(1) $cb\ ac\ ca \sim cb\ ac\ (a \neq c)$, similar to (3) in the proof of theorem 5.2,
(2) $cb\ ac\ bc \sim ab\ ba\ cb$, similar to (6) in the proof of theorem 5.2,
(3) $ab\ aa\ ba \sim ab\ ba\ ab$, (2) with $a = c$,
(4) $ba\ ab\ ba \sim ba\ ab\ (a \neq b)$, (1) with $a = b$ and c replaced by b,
(5) $(ab\ aa\ ba)^n\ ab\ aa \sim ab\ aa$, $E'_{1,n}$ with $a = c$,
(6) $(ab\ aa\ ba)^n\ ab\ aa\ ab \sim ab\ aa\ ab$, (5),
(7) $(ab\ aa\ ba)^n\ ab \sim ab\ (a \neq b)$, (6), E'_2,
(8) $(ab\ ba\ ab)^n\ ab \sim ab\ (a \neq b)$, (7), (3),
(9) $(ab\ ba\ ab)^n \sim ab\ (a \neq b)$, (8), E'_2,
(10) $(ab\ ba)^n \sim ab\ (a \neq b)$, (9), (4),
(11) $(ab\ ba\ ab)^n \sim ab(ba\ ab)^n\ (a \neq b)$, n-1 applications of E'_2,
(12) $ab\ ba \sim ab\ (a \neq b)$, (9), (10), (11),
(13) $(ba\ ab\ aa)^n\ ba\ ab \sim aa\ ba$, $E'_{1,n}$,
(14) $(ba\ ab\ aa)^n\ ba\ ab \sim ba\ (ab\ aa\ ba)^n\ ab \sim ba\ (ab\ ba\ ab)^n\ ab \sim ba\ ab\ ab \sim ba\ (a \neq b)$, (3), (12), E'_2,
(15) $aa\ ba \sim ba\ (a \neq b)$, (13), (14),
(16) $aa\ aa\ ab \sim aa\ ab\ (a \neq b)$, E'_2,
(17) $aa\ aa\ ba \sim aa\ ba\ (a \neq b)$, (15),
(18) $aa\ aa \sim aa$, (16), (17), R_1,
(19) $ab\ ba \sim ab$, (12), (18).

Hence, $\mathcal{E}'_n \vdash A_1$.

(20) ab ab ~ ab , E'_2, (18),

(21) cb ac bc ~ ab cb , (2), (19),

(22) bc ab cb ~ ac bc , (21),

(23) bc cb ac bc ~ bc ab cb , (21),

(24) bc ac bc ~ ac bc , (23), (19), (22),

(25) bc ac bc ~ ac bc bc , (24), (20),

(26) bc ac ac ~ ac bc ac , (25),

(27) bc ac ~ ac bc , (25), (26), R_1.

Hence, $\mathcal{E}'_n \vdash A_4$.

(28) cb ab ~ ab cb ~ cb ac bc ~ cb bc ac ~ cb ac , (27), (21), (27), (19).

Hence, $\mathcal{E}'_n \vdash A_3$.

<u>Theorem 5.4</u>. For each $n \geq 1$, $\mathcal{E}''_n \Longleftrightarrow \mathcal{A}$.

<u>Proof</u>.

1. $\mathcal{E}''_n \Longrightarrow \mathcal{A}$ is proved as above.
2. We now prove that $\mathcal{A} \Longrightarrow \mathcal{E}''_n$.

(1) cb ab bc ~ ab ba ca , similar to (2) in the proof of theorem 5.3,

(2) $(ab\ aa\ ba)^n$ ab aa ~ ab ab , $E''_{1,n}$,

(3) $(ab\ aa\ ba)^n$ ab aa ab ~ ab ab ab , (2),

(4) $(ab\ aa\ ba)^n$ ab ~ ab $(a \neq b)$, (3), E''_2,

(5) $(ba\ ab\ aa)^n$ ba ab ~ aa ba , $E''_{1,n}$,

(6) $(ba\ ab\ aa)^n$ ba ab ~ ba $(ab\ aa\ ba)^n$ ab ,

(7) ba ab ~ aa ba $(a \neq b)$, (4), (6), (5),

(8) ba ab ba ~ ba ab $(a \neq b)$, (7), E''_2,

(9) $(ab\ ba)^n$ ~ $(ab\ ba\ ab)^n$ ~ $(ab\ ba\ ab)^n$ ab ~ $(ab\ aa\ ba)^n$ ab ~ ab $(a \neq b)$, (8), E''_2, (7), (4),

(10) ab ba ~ ab $(ba\ ab)^n$ ~ $(ab\ ba\ ab)^n$ ~ $(ab\ ba)^n$ ~ ab $(a \neq b)$, (9), n-1 applications of E''_2, (8), (9),

(11) aa aa ab ~ aa ab $(a \neq b)$, E''_2,

(12) aa aa ba ~ aa ba $(a \neq b)$, (7), (10),

(13) aa aa ~ aa , (11), (12), R_1,

(14) ab ba ~ ab , (10), (13).

Hence, $\mathcal{E}''_n \vdash A_1$.

(15) $ab\ ab \sim ab$, E''_2, (13),

(16) $ab\ cb\ ab \sim cb\ ab\ ab$, $E''_{1,n}$, (15),

(17) $cb\ ab\ cb \sim ab\ cb\ cb$, (16),

(18) $cb\ ab \sim ab\ cb$, (16), (17), R_1.

Hence, $\mathcal{E}''_n \vdash A_4$.

(19) $ab\ ca \sim ab\ ba\ ca \sim cb\ ab\ bc \sim ab\ cb\ bc \sim$
$ab\ cb$, A_1, (1), A_4, A_1.

Hence, $\mathcal{E}''_n \vdash A_3$.

6. Non-equipollent axiom systems

In section 5 we studied the following axiom systems:

$\mathcal{C}_n = \{C_{1,n}, C_2\}$, with $C_{1,n}$: $(ab\ ca\ bc)^n \sim cb\ ab$, and $C_2 = A_2$,

$\mathcal{D}_n = \{D_{1,n}, D_2\}$, with $D_{1,n}$: $(ab\ ca\ bc)^n\ ab \sim cb\ ac$, and $D_2 = A_2$,

$\mathcal{E}'_n = \{E'_{1,n}, E'_2\}$, with $E'_{1,n}$: $(ab\ ca\ bc)^n\ ab\ ca \sim cb\ ac$, and $E'_2 = A_2$,

$\mathcal{E}''_n = \{E''_{1,n}, E''_2\}$, with $E''_{1,n}$: $(ab\ ca\ bc)^n\ ab\ ca \sim cb\ ab$, and $E''_2 = A_2$,

and we proved that all these systems are equipollent with axiom system $\mathcal{A}$. In this section we consider two related axiom systems, introduced by:

Definition 6. Let n be an integer ≥ 1.
$\mathcal{C}'_n = \{C'_{1,n}, C'_2\}$ consists of the following two axioms:
$C'_{1,n}$: $(ab\ ca\ bc)^n \sim cb\ ac$, and $C'_2 = A_2$;
$\mathcal{D}'_n = \{D'_{1,n}, D'_2\}$ consists of the following two axioms:
$D'_{1,n}$: $(ab\ ca\ bc)^n\ ab \sim cb\ ab$, and $D'_2 = A_2$.

One might expect, analogous to theorem 5.3 and 5.4, that $\mathcal{C}'_n \Longleftrightarrow \mathcal{A}$ and $\mathcal{D}'_n \Longleftrightarrow \mathcal{A}$. However, this appears to be not true in general. The main results of this section, contained in theorems 6.1 and 6.2, can be summarized as follows:

1. For all $n \geq 1$: $\mathcal{C}'_n \Longleftrightarrow \mathcal{D}'_n$.
2. For all $n \geq 1$: $\mathcal{C}'_n \Longrightarrow \mathcal{A}$.
3. For all $n \geq 1$: $\mathcal{C}'_n \vdash A_1$ and $\mathcal{C}'_n \vdash A_4$.
4. $\mathcal{A} \Longrightarrow \mathcal{C}'_1$, hence $\mathcal{A} \Longleftrightarrow \mathcal{C}'_1$.
5. For no even $n \geq 2$, $\mathcal{A} \Longrightarrow \mathcal{C}'_n$.

Thus we have obtained the result that, for even n, $\mathcal{C}_n \Longleftrightarrow \mathcal{A}$ is not true. The problem for odd $n \geq 3$ is still open. We conjecture that in this case as well, $\mathcal{C}_n \Longleftrightarrow \mathcal{A}$ does not hold.
Theorem 6.3 gives some consequences of omitting (or weakening) C'_2. It is used in the proof of theorem 6.4, which is the analogon of lemma 3.6.

<u>Theorem 6.1</u>. For each $n \geq 1$:

a. $\mathcal{C}'_n \vdash A_1$ and $\mathcal{C}'_n \vdash A_4$.

b. $\mathcal{D}'_n \vdash A_1$ and $\mathcal{D}'_n \vdash A_4$.

c. $\mathcal{C}'_n \iff \mathcal{D}'_n$.

<u>Proof</u>.

a.

(1)	cb ac ab ~ ab ba cb	, similar to (1) in the proof of theorem 5.4,
(2)	cb ab ~ ab ba cb $(a \neq b)$	, (1), C'_2,
(3)	ab ab ~ ab ba ab $(a \neq b)$	, (2) with a = c,
(4)	ab ba ~ ab ba ba $(a \neq b)$	, C'_2,
(5)	ab ~ ab ba $(a \neq b)$	, (3), (4), R_1,
(6)	cb ab ~ ab cb $(a \neq b)$	, (2), (5),
(7)	bb ab ~ ab bb	, (6),
(8)	cb ab ~ ab cb	, (6), (7).

Hence, $\mathcal{C}'_n \vdash A_4$.

(9)	ca ac aa ~ aa aa ca	, (1) with a = b,
(10)	aa ca ~ aa aa ca $(a \neq c)$	, (5), (7), (9),
(11)	aa ac ~ aa aa ac $(a \neq c)$	, C'_2,
(12)	aa ~ aa aa	, (10), (11), R_1,
(13)	ab ~ ab ba	, (5), (12).

Hence, $\mathcal{C}'_n \vdash A_1$.

For later use, we prove that aa ca ~ ca.

(14)	$(\text{aa ca ac})^n$ ~ ca ac	, $C'_{1,n}$ with a = b,
(15)	$(\text{aa ca})^n$ ~ ca	, A_1, (14),
(16)	$(\text{aa ca})^n$ ~ $(\text{aa})^n$ $(\text{ca})^n$ ~ aa ca	, A_4, A_1, C'_2,
(17)	aa ca ~ ca	, (15), (16).

b.

(1)	cb ab ca ~ ab ba ca	, similar to (1) of part a,
(2)	ab ab aa ~ ab ba aa	, (1) with a = c,
(3)	ab ba ~ ab ba ba $(a \neq b)$	, D'_2,
(4)	ab ~ ab ba $(a \neq b)$	, (2), (3), D'_2, R_1,
(5)	cb ab ca ~ ab ca $(a \neq b)$	, (1), (4),
(6)	cb ab cb ~ ab cb $(a \neq b, b \neq c)$	, (5), D'_2.

As in the proof of theorem 5.3 ((24) to (27)) we derive from this:

(7)	ab cb ~ cb ab ($a \neq b$, $a \neq c$, $b \neq c$)	,
(8)	bb ab ba ~ ab ba ba	, (1) with b = c,
(9)	bb ab ~ ab ($a \neq b$)	, (8), (4),
(10)	ab bb ba ~ ab ba ($a \neq b$)	, D'_2,
(11)	ab bb ab ~ ab ab ($a \neq b$)	, (9),
(12)	ab bb ~ ab ($a \neq b$)	, (10), (11), R_1,
(13)	ab bb ~ bb ab	, (9), (12),
(14)	ab cb ~ cb ab	, (7), (13).

Hence, $\mathfrak{D}'_n \vdash A_4$. It follows as usual that $\mathfrak{D}'_n \vdash A_1$.

c. First we show that $\mathfrak{D}'_n \Rightarrow \mathfrak{C}'_n$.

(1)	$(ab\ ca\ bc)^n$ ab ~ cb ac ab	, $C'_{1,n}$,
(2)	$(ab\ ca\ bc)^n$ ab ~ cb ab ($a \neq b$)	, (1), C'_2,
(3)	$(aa\ ca\ ac)^n$ aa ~ $(ca)^n$ aa	, (13) of part a, (17) of part a,
(4)	$(aa\ ca\ ac)^n$ aa ~ ca aa	, (3),
(5)	$(ab\ ca\ bc)^n$ ab ~ cb ab	, (2), (4).

Hence, $\mathfrak{C}'_n \vdash D'_{1,n}$.

Next we prove that $\mathfrak{C}'_n \Rightarrow \mathfrak{D}'_n$.

(1)	$(ab\ ca\ bc)^n$ ab ac ~ cb ab ac	, $D'_{1,n}$,
(2)	$(ab\ ca\ bc)^n$ ac ~ cb ac ($a \neq c$)	, D'_2,
(3)	$(ab\ ca\ bc)^{n-1}$ ab ca bc ac ~ $(ab\ ca\ bc)^{n-1}$ ab ca ac bc	, A_4,
(4)	$(ab\ ca\ bc)^n$ ~ cb ac ($a \neq c$)	, (2), (3), A_1,
(5)	$(ab\ aa\ ba)^n$ ~ $(ab)^n$ ($a \neq b$)	, (9) of part b, A_1,
(6)	ba ab bb ~ ba ab ($a \neq b$)	, (12) of part b,
(7)	$(ab\ aa\ ba)^n$ ~ ab aa ($a \neq b$)	, (5), (6), A_1,
(8)	$(aa\ aa\ aa)^n$ ~ aa aa	, A_1,
(9)	$(ab\ ca\ bc)^n$ ~ cb ac	, (4), (7), (8).

Hence, $\mathfrak{D}'_n \vdash C'_{1,n}$.

This completes the proof of theorem 6.1.

Theorem 6.2.

1. For each integer $n \geq 1$, $\mathcal{C}'_n \Rightarrow \mathcal{A}$.
2. $\mathcal{A} \Rightarrow \mathcal{C}'_1$.
3. For no even integer $n \geq 2$: $\mathcal{A} \Rightarrow \mathcal{C}'_n$.

Proof.

1. Evident.

2. It is only necessary to prove that $\mathcal{C}'_1 \vdash A_3$.

(1) ab ba ~ ab ~ bb ab ~ ab bb , A_1, (17) of theorem 6.1, A_4,

(2) ab aa ab ~ ab ab ($a \neq b$) , C'_2,

(3) ab aa ba ~ ab ba , (17) of theorem 6.1,

(4) ab aa ~ ab ($a \neq b$) , (2), (3), R_1,

(5) ab aa ~ ab ab , (4), C'_2.

From (1) and (5), A_3 follows for $b = c$ or $a = c$. If $a = b$, we have nothing to prove. We now suppose that a, b, c are all different and that x, y, z are arbitrary variables, different from a, b, c.

(6) ab cd ~ cd ab ($a \neq c$, $a \neq d$, $b \neq c$) , the proof of lemma 3.1 does not use A_3,

(7) ab ca ax by ~ cb ac ba ax by ~ cb ax by ~ ab cb ax by , $C'_{1,1}$, (6), C'_2,

(8) ab ca ax cz ~ ax cz ~ ab cb ax cz , (6), C'_2,

(9) ab ca by cz ~ ab by cz ~ ab cb by cz , (6), C'_2,

(10) ab ca ax ~ ab cb ax , (7), (8), R_1,

(11) ab ca by ~ ab cb by , (7), (9), R_1,

(12) ab ca ~ ab cb , (10), (11), R_1.

Hence $\mathcal{C}'_1 \vdash A_3$.

3. Let n be an even integer ≥ 2. Suppose $\mathcal{C}'_n \vdash S_1 \sim S_2$. Then S_1 and S_2 have the following property:

(P): For all $a \in V$: $F(a, S_1) + F(a, S_2) \equiv 0 \pmod 2$.

This is clearly true for C'_{12} and C'_{r2}. Next we consider $C'_{1,n}$. First suppose that a, b, c are all different. Then

$F(d, (ab\ ca\ bc)^n) = F(d, cb\ ac) = 0$, for all $d \neq a, b, c$,

$F(a, (ab\ ca\ bc)^n) = 3n - 2$, and $F(a, cb\ ac) = 2$,

$F(b, (ab\ ca\ bc)^n) = 3n$, and $F(b, cb\ ac) = 0$,

$F(c, (ab\ ca\ bc)^n) = 3n - 1$, and $F(c, cb\ ac) = 1$.

Hence, in all cases $F(d, (ab\ ca\ bc)^n) + F(d, cb\ ac) \equiv 0 \pmod 2$, since n is even. It is also easy to verify that (P) holds if two (or more) variables of $C'_{1,n}$ are equal. Moreover, it is clear that (P) is preserved by application of the rules of inference.
Since $F(c, ab\ ca) + F(c, ab\ cb) = 2 + 1 = 3$, it follows that A_3 does not have property (P), and hence cannot be derived from $\mathcal{C}'_n$. This means that $\mathcal{A} \Rightarrow \mathcal{C}'_n$ holds for no even integer n.

This completes the proof of theorem 6.2.

In theorem 6.1 we proved that $\mathcal{C}'_n \vdash A_1$ and A_4 and $\mathcal{D}'_n \vdash A_1$ and A_4, i.e. we showed that A_1 and A_4 can be derived from $C'_{1,n}$ ($D'_{1,n}$) and C'_2(D'_2). We have also investigated whether it is possible to derive A_1 or A_4 using only $C'_{1,n}$ ($D'_{1,n}$). Although we did not succeed in this, it appeared that it is not necessary to use all of C'_2 (D'_2).
It is sufficient to assume, instead of C'_2, the following axiom:

$$C'_{2,n} : (ab)^{3n-2} \sim ab,$$

and instead of D'_2:

$$D'_{2,n} : (ab)^{3n-1} \sim ab.$$

A precise formulation now follows:

<u>Theorem 6.3</u>. For each integer $n \geq 1$:
a. $\{C'_{1,n}\} \vdash (ab)^{3n-1} \sim ab$.
b. $\{C'_{1,n}, C'_{2,n}\} \vdash A_1, A_4$.
c. $\{D'_{1,n}\} \vdash (ab)^{3n} \sim ab$.
d. $\{D'_{1,n}, D'_{2,n}\} \vdash A_1, A_4$.
(Since $C'_{2,n}$ always holds if n = 1, it follows that $\{C'_{1,1}\} \vdash A_1, A_4$. In this special case a much shorter (direct) proof is also possible, which we omit here.)

<u>Proof</u>.

a.

(1) cb ac ab ~ ab ba cb , see (1) of part a of theorem 6.1,

(2) ba ab aa ~ aa aa ba , (1),

(3) $ab\ aa\ ab \sim ab\ ba\ ab$, (1),

(4) $aa\ ba\ ba \sim ba\ ab\ aa$, (1),

(5) $(aa\ ba\ ab)^n \sim ba\ ab$, $C'_{1,n}$,

(6) $(ab\ aa\ ba)^n \sim ab\ aa$, $C'_{1,n}$,

(7) $(ba\ ab\ aa)^n \sim aa\ ba$, $C'_{1,n}$,

(8) $aa\ ba\ ab\ aa\ ba\ ab \sim ba\ ab\ ba\ ab\ ba\ ab$, (2), (3), (4),

(9) $(aa\ ba\ ab)^{2n} \sim (ba\ ab)^{3n}$, (8),

(10) $(ba\ ab)^2 \sim (ba\ ab)^{3n}$, (9), (5),

(11) $(ba\ ab\ aa)^n\ aa\ ba \sim (ba\ ab\ aa)^n\ ba\ ba$, (2), (4),

(12) $aa\ ba\ aa\ ba \sim aa\ ba\ ba\ ba$, (11), (7),

(13) $aa\ ba\ aa\ ba \sim ba\ ab\ aa\ ba$, (12), (4),

(14) $aa\ ba\ ba\ aa\ ba\ ba \sim ba\ ab\ aa\ ab\ aa\ ba$, (2), (3), (4),

(15) $(aa\ ba\ ba)^{2n} \sim (ba\ ab\ aa\ ab\ aa\ ba)^n$, (14),

(16) $ba\ ab\ aa\ ab\ aa\ ba \sim (aa\ ba)^3$, (13), (3),

(17) $(aa\ ba)^{3n} \sim (aa\ ba)^2$, (15), (16), (4), (7),

(18) $(ab\ ba)^{3n-1}\ ab\ ba \sim ab\ ba\ ab\ ba$, (10),

(19) $(ab\ ba)^{3n-1}\ ab\ aa\ ab \sim ab\ ba\ ab\ aa\ ab$, (3), (10),

(20) $(ab\ ba)^{3n-1}\ ab\ aa\ ba \sim ab(aa\ ba)^{3n}$, (13),

(21) $(ab\ ba)^{3n-1}\ ab\ aa\ ba \sim ab\ ba\ ab\ aa\ ba$, (20), (17), (13),

(22) $(ab\ ba)^{3n-1}\ ab\ aa \sim ab\ ba\ ab\ aa\ (a \neq b)$, (19), (21), R_1,

(23) $(ab\ ba)^{3n-1}\ ab \sim ab\ ba\ ab\ (a \neq b)$, (18), (22), R_1,

(24) $(ba\ ab)^{3n-1}\ aa\ ab \sim ba\ ab\ aa\ ab$, (10), (3),

(25) $(ba\ ab)^{3n-1}\ aa\ ba \sim ba\ ab\ aa\ ba$, (17), (13),

(26) $(ba\ ab)^{3n-1}\ aa \sim ba\ ab\ aa\ (a \neq b)$, (24), (25), R_1,

(27) $(ba\ ab)^{3n-1} \sim ba\ ab(a \neq b)$, (23), (26), R_1,

(28) $(ba\ ab)^{3n-2}\ (ba\ ab\ aa)^n \sim (ba\ ab\ aa)^n\ (a \neq b)$, (27),

(29) $(ba\ ab)^{3n-2}\ aa\ ba \sim (aa\ ba)^{3n-1}$, (13),

(30) $(aa\ ba)^{3n-1} \sim aa\ ba$, (28), (29), (7),

(31) $(ab\ ba)^{3n-2}\ ab\ aa\ ab \sim ab\ aa\ ab\ (a \neq b)$, (27), (3),

(32) $(ab\ ba)^{3n-2}\ ab\ aa\ ba \sim ab\ aa\ ba$, (30), (13),

(33) $(ab\ ba)^{3n-2}\ ab\ aa \sim ab\ aa\ (a \neq b)$, (31), (32), R_1,

(34) $(ab\ ba)^{3n-2}\ ab \sim ab\ (a \neq b)$, (27), (33), R_1,

(35) $aa\ ba\ ba \sim aa\ ba\ ba\ (ab\ ba)^{3n-2}\ (a \neq b)$, (34),

(36) $aa\ ba\ ba\ (ab\ ba)^{3n-2} \sim ba\ ab\ ba\ (ab\ ba)^{3n-2}$, (3), (4),

(37) $ba\ ab\ aa \sim ba\ ab\ ba\ (a \neq b)$, (4), (35), (36),

(38) $(ba\ ab)^{3n-2}\ aa \sim ba\ (a \neq b)$, (34), (37),

(39) $(ba\ ab)^{3n-2}\ aa\ ba \sim aa\ ba$, (30), (13),

(40) $ba\ ba \sim aa\ ba\ (a \neq b)$, (38), (39),

(41) $(ba)^{3n} \sim (ba)^2$, (7), (4), (40),

(42) $(aa\ ba\ ab)^n \sim aa(ba\ ab\ aa)^{n-1}\ ba\ ab$,

(43) $ba\ ab \sim (ba)^{3n-1}\ ab$, (42), (5), (40),

(44) $(ba)^{3n-1} \sim ba\ (a \neq b)$, (41), (43), R_1,

(45) $(aa)^{3n} \sim aa\ aa$, $C'_{1,n}$,

(46) $(aa)^{3n-1}\ ba \sim aa\ ba\ (a \neq b)$, (40), (41),

(47) $(aa)^{3n-1} \sim aa$, (45), (46), R_1,

(48) $(ab)^{3n-1} \sim ab$, (44), (47).

Hence, $\{C'_{1,n}\} \vdash (ab)^{3n-1} \sim ab$.

b.

(49) $(ab)^{3n-2} \sim ab$, $C'_{2,n}$,

(50) $(ab)^{3n-2}\ ab \sim ab$, (48),

(51) $ab\ ab \sim ab$, (49), (50),

(52) $ab\ ba\ ab \sim ab\ ab\ ab$, (37), (4), (40),

(53) $ab\ ba\ ba \sim ab\ ab\ ba$, (51),

(54) $ab\ ba \sim ab$, (52), (53), R_1, (51).

Hence, $\{C'_{1,n}, C'_{2,n}\} \vdash A_1$.

(55) $cb\ ac\ ab \sim ab\ cb$, (1), (54),

(56) $ab\ cb\ ac \sim cb\ ac$, $C'_{1,n}$, (51),

(57) $bc\ ab\ cb \sim bc\ ab$, $C'_{1,n}$, (51),

(58) $bc\ ab\ cb\ ac \sim bc\ ac$, (56), (54),

(59) $bc\ ab\ cb\ ac \sim bc\ ab\ ac$, (57),

(60) $bc\ ab\ ac \sim ac\ bc$, (55),

(61) $ac\ bc \sim bc\ ac$, (58), (59), (60).

Hence, $\{C'_{1,n}, C'_{2,n}\} \vdash A_4$.

c.

(62) $cb\ ab\ ca \sim ab\ ba\ ca$, $D'_{1,n}$,

(63) $ba\ aa\ ba \sim aa\ aa\ ba$, (62),

(64) $ab\ ab\ aa \sim ab\ ba\ aa$, (62),

(65) $aa\ ba\ ab \sim ba\ ab\ ab$, (62),

(66) $(aa\ ba\ ab)^n\ aa \sim ba\ aa$, $D'_{1,n}$,

(67) $(ab\ aa\ ba)^n\ ab \sim ab\ ab$, $D'_{1,n}$,
(68) $(ba\ ab\ aa)^n\ ba \sim aa\ ba$, $D'_{1,n}$,
(69) $ba\ (aa\ ba\ ab)^n\ aa \sim aa\ (aa\ ba\ ab)^n\ aa$, (63),
(70) $ba\ ba\ aa \sim aa\ ba\ aa$, (69), (66),
(71) $ab\ ab\ (aa\ ba\ ab)^n\ aa \sim ab\ ba\ (aa\ ba\ ab)^n\ aa$, (64),
(72) $ab\ ab\ ba\ aa \sim ab\ ba\ ba\ aa$, (71), (66),
(73) $ba\ aa\ ba\ ab \sim ba\ ba\ ab\ ab$, (65),
(74) $ba\ aa\ ba\ ab \sim aa\ aa\ ba\ ab \sim aa\ ba\ ab\ ab \sim$
$ba\ ab\ ab\ ab$, (63), (65), (65),
(75) $ba\ ba\ ab\ ab \sim ba\ ab\ ab\ ab$, (73), (74),
(76) $ba\ ba\ ab\ bb \sim ba\ ab\ ab\ bb$, (72),
(77) $ba\ ba\ ab \sim ba\ ab\ ab$, (75), (76), R_1,
(78) $ba\ ba\ bb \sim ba\ ab\ bb$, (64),
(79) $ba\ ba \sim ba\ ab$, (77), (78), R_1,
(80) $aa\ ba\ ba \sim ba\ ba\ ba$, (65), (79),
(81) $aa\ ba\ ab \sim ba\ ba\ ab$, (80), (79),
(82) $aa\ ba \sim ba\ ba$, (80), (81), R_1,
(83) $(ab)^{3n+1} \sim ab\ ab$, (67), (79), (82),
(84) $(ab)^{3n}\ ba \sim ab\ ba$, (83), (79),
(85) $(ab)^{3n} \sim ab\ (a \neq b)$, (83), (84), R_1,
(86) $(aa)^{3n}\ aa \sim aa\ aa$, $D'_{1,n}$,
(87) $(aa)^{3n}\ ba \sim aa\ ba$, (85), (82),
(88) $(aa)^{3n} \sim aa$, (86), (87), R_1,
(89) $(ab)^{3n} \sim ab$, (85), (88).

Hence, $\{D'_{1,n}\} \vdash (ab)^{3n} \sim ab$.

d. Follows as usual.

This completes the proof of theorem 6.3.

Finally, theorem 6.4 gives the analogon of lemma 3.6.
Consider the following equivalence:

$$C'_{3,n} : (ab\ bc\ ca)^{2n} \sim ac\ (a \neq c).$$

We shall show that $C'_{3,n}$ can be derived from $C'_{1,n}$ and C'_2, and, conversely, that C'_2 can be derived from $C'_{1,n}$ and $C'_{3,n}$:

Theorem 6.4. For each integer $n \geq 1$:

1. $\{C'_{1,n}, C'_2\} \vdash C'_{3,n}$.

2. $\{C'_{1,n}, C'_{3,n}\} \vdash C'_2$.

Proof.

1. We prove that $(ab\ bc\ ca)^{2n} \sim ac\ (a \neq c)$ can be derived from $C'_{1,n}$ and C'_2. It is easy to verify this for $a = b$ or $b = c$. From now on we suppose that a, b, c are all different, and that x, y, z are arbitrary variables, different from a, b, c.

(1) A_1 , theorem 6.1,

(2) A_4 , theorem 6.1,

(3) $(ab\ bc\ ca)^{2n-2}\ (ba\ cb\ ac)^{n-1} \sim$
$(ab\ bc\ ca)^{2n-4}\ ab\ bc\ ca\ ab\ bc\ ca\ ba\ cb\ ac\ (ba\ cb\ ac)^{n-2} \sim$
$(ab\ bc\ ca)^{2n-4} \sim (ba\ cb\ ac)^{n-2} \sim$
$\ldots \sim (ab\ bc\ ca)^2\ ba\ cb\ ac \sim$
$bc\ ac$, A_1, A_4, C'_2,

(4) $(ab\ bc\ ca)^{2n-2}\ (cb\ ac\ ba)^{n-1} \sim$
$(ab\ bc\ ca)^{2n-4}\ ab\ bc\ ca\ ab\ bc\ ca\ cb\ ac\ ba\ (cb\ ac\ ba)^{n-2} \sim$
$(ab\ bc\ ca)^{2n-4} \sim (cb\ ac\ ba)^{n-2} \sim$
$\ldots \sim (ab\ bc\ ca)^2\ cb\ ac\ ba \sim$
$ab\ ca$, A_1, A_4, C'_2,

(5) $ab\ cd \sim cd\ ab\ (a \neq c,\ a \neq d,\ b \neq c)$, A_3 is not used in the proof of lemma 3.1,

(6) $(ab\ bc\ ca)^{2n}\ ax\ by \sim$
$(ab\ bc\ ca)^{2n-1}\ ab\ bc\ ca\ ax\ by \sim$
$(ab\ bc\ ca)^{2n-1}\ ab\ ca\ ax\ by \sim$
$(ab\ bc\ ca)^{2n-1}\ (cb\ ac\ ba)^n\ ax\ by \sim$
$ab\ bc\ ca\ ab\ ca\ cb\ ac\ ba\ ax\ by \sim$
$ax\ by$, A_1, A_4, C'_2, (5), (4),

(7) $(ab\ bc\ ca)^{2n}\ ax\ cz \sim$
$(ab\ bc\ ca)^{2n-2}\ ab\ bc\ ca\ ab\ bc\ ca\ ax\ cz \sim$
$(ab\ bc\ ca)^{2n-2}\ ab\ bc\ (ba\ cb\ ac)^n\ ax\ cz \sim$
$(ab\ bc\ ca)^{2n-2}\ ab\ ba\ cb\ ac\ (ba\ cb\ ac)^{n-1}\ ax\ cz \sim$
$(ab\ bc\ ca)^{2n-2}\ (cb\ ac\ ba)^{n-1}\ ax\ cz \sim$
$ab\ ca\ ax\ cz$, A_1, A_4, C'_2, (5), (4),

(8) $(ab\ bc\ ca)^{2n}\ by\ cz \sim$

$(ab\ bc\ ca)^{2n-2}\ ab\ bc\ ca\ ab\ bc\ ca\ by\ cz \sim$

$(ab\ bc\ ca)^{2n-2}\ ab\ (ac\ ba\ cb)^{n}\ by\ cz \sim$

$(ab\ bc\ ca)^{2n-2}\ ab\ ac\ ba\ cb\ (ac\ ba\ cb)^{n-1} by\ cz \sim$

$(ab\ bc\ ca)^{2n-2}\ (ba\ cb\ ac)^{n-1}\ by\ cz \sim$

$bc\ ac\ by\ cz$, A_1, A_4, C'_2, (5), (3),

(9) $(ab\ bc\ ca)^{2n}\ ax \sim ac\ ax$, (6), (7), R_1,

(10) $(ab\ bc\ ca)^{2n}\ by \sim ac\ by$, (6), (8), R_1,

(11) $(ab\ bc\ ca)^{2n} \sim ac$, (9), (10), R_1.

Hence, $\{C'_{1,n}, C'_2\} \vdash C'_{3,n}$.

2. We now prove that $\{C'_{1,n}, C'_{3,n}\} \vdash C'_2$.

(1) $(ab)^{3n-1} \sim ab$, theorem 6.3,

(2) $(ab\ bc\ ca)^{2n}\ ab \sim ac\ ab\ (a \neq c)$, $C'_{3,n}$,

(3) $(ab\ bc\ ca)^{2n}\ ab \sim ab(bc\ ca\ ab)^{2n} \sim ab\ ba$

$(a \neq b)$, $C'_{3,n}$,

(4) $ac\ ab \sim ab\ ba\ (a \neq b,\ a \neq c)$, (2), (3),

(5) $ab\ ab \sim ab\ ba$, (4) with $b = c$,

(6) $ab\ aa\ ab \sim ab\ ba\ ab$, theorem 6.3 (3),

(7) $aa\ ba \sim ba\ ba$, theorem 6.3 (40),

(8) $(aa\ ab\ ba)^{2n} \sim ab\ (a \neq b)$, $C'_{3,n}$ with $a = b$ and c replaced by b,

(9) $(aa\ ab\ ba\ aa\ ab\ ba)^{n} \sim ab\ (a \neq b)$, (8),

(10) $(aa\ ab\ ab\ aa\ ab\ ab)^{n} \sim ab\ (a \neq b)$, (5), (9),

(11) $(aa\ (ab)^5)^{n} \sim ab\ (a \neq b)$, (10), (6), (5),

(12) $aa\ (ab)^{6n-1} \sim ab\ (a \neq b)$, (11), (6), (5),

(13) $aa\ (ab)^3 \sim ab\ (a \neq b)$, (12), (1),

(14) $ab\ aa\ (ab)^3 \sim (ab)^2\ (a \neq b)$, (13),

(15) $(ab)^5 \sim (ab)^2\ (a \neq b)$, (14), (6),

(16) $(ab)^4\ ba \sim ab\ ba\ (a \neq b)$, (5),

(17) $(ab)^4 \sim ab\ (a \neq b)$, (15), (16), R_1,

(18) $(ab)^6 \sim (ab)^3\ (a \neq b)$, (17),

(19) $(ab)^{6n} \sim (ab)^{3n}\ (a \neq b)$, (18),

(20) $(ab)^4 \sim (ab)^2\ (a \neq b)$, (19), (1),

(21) $(ab)^2 \sim ab\ (a \neq b)$, (17), (20),

(22) aa aa ab ~ aa ab $(a \neq b)$, (13), (21),

(23) aa aa ba ~ aa ba $(a \neq b)$, (7), (21),

(24) aa aa ~ aa , (22), (23), R_1,

(25) ab ab ~ ab , (21), (24),

(26) ab ac ~ ab $(ab\ bc\ ca)^{2n}$ ~ $(ab\ bc\ ca)^{2n}$ ~
ac $(a \neq c)$, $C'_{3,n}$, (25),

(27) ab ac ~ ac $(a \neq c)$, (26).

Hence, $\{C'_{1,n}, C'_{3,n}\} \vdash C'_2$.

This completes the proof of theorem 6.4.

References

1. J.W. de Bakker, Formal definition of programming languages, with an application to the definition of ALGOL 60. Mathematical Centre Tracts 16, Amsterdam, Mathematisch Centrum, 1967.

2. J.W. de Bakker, Problems in the theory of programming languages, to appear in Proceedings of the 3 rd international congress for logic, methodology and philosophy of science (Ed. B. van Rootselaar), Amsterdam, North-Holland Publ. Comp., 1968.

3. C.A.R. Hoare, The axiomatic method, Part I. Computing Research Laboratory of Elliott-Automation Computers Ltd.

4. S. Igarashi, An axiomatic approach to the equivalence problems of algorithms with applications. Ph. D. Thesis, University of Tokyo, 1964.