IBM

IBM United Kingdom
Laboratories Limited

The Formal Development of an Algorithm

C.D. Allen
C.B. Jones

March 1973

215-8058-0

Technical Report TR.12.110

Unrestricted

Technical Report TR.12.110

The Formal Development of an Algorithm

C.D. Allen
C.B. Jones

Unrestricted

March 1973

215-8058-0

IBM United Kingdom Laboratories Limited
Hursley Park
Winchester Hampshire

The Formal Development of an Algorithm

C. D. Allen,
C. B. Jones.

Product Test Laboratory
IBM U.K. Laboratories Ltd.
Hursley Park
Nr Winchester
Hampshire

ABSTRACT

Formal Development is a method of going from a formal specification of a task to an algorithm which (correctly) performs that task. The method is illustrated in this paper on Hoare's sorting algorithm (FIND).

INTRODUCTION

Programs have been, and still are, first written completely and then tested by running testcases, i.e. examining executions each using some specific data of a type for which the program specification requires certain results. This process suffers from the fundamental limitation that, as programs become more complex, the classes of data on which they are required to act in specific ways become very large, and often potentially infinite. Since only a limited number of testcases can be run, this form of testing is ultimately inadequate to guarantee an error-free product. This has been the situation for some time now.

Recent developments in formal studies of programs and programming languages have offered the possibility of proving programs correct in the same kind of way that theorems of mathematics are proved true. The advantage of such techniques is that the formal theory used can be sufficiently general, as in mathematics, to cover an infinite number of cases in a single proof, thus overcoming the limitation above. However, this method has its own limitations, both in theory and in practice. The main one is that while a correct program can be proved correct, an incorrect program is difficult to prove incorrect except by construction of a counter-example - i.e. a suitable testcase. (This remark applies with particular force to attempts to make the proving process automatic.) Even if the proofs are constructed manually, difficulty in producing one does not generally indicate the nature of an error in the program. Additionally, the attempt to construct a proof for a completed program can make little use of the analysis of the problem and possible solutions that went into the design of the particular program - even where this is still available - since the problem statement and analysis was not originally in form with the data types and operations actually used.

Consideration of these points - and the continuing demand for more complete and informative documentation of program design - leads to the idea that the design process itself should make use of the formal techniques now available. Also that using these techniques the process should be made more systematic. The adequacy of a method of solution for the given problem should be verified as a first step of the design, and the correctness of each subsequent step should also be checked. From such a process should emerge not only a guaranteed correct program, but also a formal proof of its correctness, and a complete description and justification of each design decision.

Several proposals for particular techniques of program design have been described in the recent literature (refs 1,3,6). This

paper, together with ref 4. adds another, based on the ideas above which are similar to those underlying other proposals. There are undoubtedly many possibilities, and much more development needs to be done on all of them (including the present one) before specific design rules can be laid down. The present paper is therefore intended as a contribution to the discussion and evaluation of these possibilities.

So far, the extremes of the range of possibilities seem to be represented in the papers of Dijkstra (ref 1) and Waldinger (ref 6). Dijkstra proposes step by step development of the programs, each step being small enough to be comprehended as a whole and reliably judged correct. (A later paper of Dijkstra, ref 2, does however include proofs at each step of development.) Waldinger, on the other hand, shows that a constructive proof of a suitable existence theorem can be systematically translated into a correct program. The example of Hoare (ref 3) lies between these two extremes - perhaps closer to Dijkstra in that algorithms are used early in the process. The present example also lies between the extremes - perhaps closer to Waldinger, in that actual algorithms and data representations appear later than in ref 3, while proofs appear immediately.

The problem dealt with here is that of ref 3. This choice was deliberate, to facilitate comparative evaluation (but note that in the present paper the proofs are given in full, and cover all aspects of the problem - including the fact that the final set is a rearrangement of the original). For the same reason, the final program aimed at is the program of ref 3, (although that actually reached is slightly different).

1. Notation

In this section we introduce the notation to be used throughout. It includes notation used in the problem specification, given in the next section.

A set of objects U is given, whose members are a,b,c,... . Subsets of U are denoted by V,W,X,... and we use:

$V \cup W$	the union of V and W
$a \in V$	a is a member of V
$\emptyset$	the empty set
$\|V\|$	the number of members of V
$\{a \mid p(a)\}$	the set of elements satisfying p
I	the set of integers
$\beta(U)$	the set of subsets of U

with their usual meaning.
A total ordering relation $\leq.$ between members of U is given :-

$$\leq.: U \times U \rightarrow \{T,F\}$$

- where T and F are truth values. (This notation means that $\leq.$ is an operation taking two arguments, each from the set U, and giving a result from the set {T,F}, i.e. a truth value.) The relation is a total ordering, i.e. it has the following properties:

1. $a \leq.b \vee b \leq.a$
2. $a \leq.b \ \& \ b \leq.c \supset a \leq.c$
3. $a \leq.a$

We also use a strict order relation $<.$ between members of U, defined as follows:

$$<.: U \times U \rightarrow \{T,F\}$$

4. $a <.b = a \leq.b \ \& \ \neg(b \leq.a)$

We also use the notation of formal logic; specifically:-

&	and
$\vee$	or
$\supset$	implies
$\neg$	not
$\equiv$	equivalence
$\exists$	existential quantifier ($(\exists x)(p(x))$ meaning "there exists an x such that p(x) is true".)
$\vdash$	deducibility ($exp_1 \vdash exp_2$ meaning that exp_2 is deducible from exp_1 under the normal rules of logical deduction.)

In writing assumptions on functions, we use the form:-

$$p(\underline{X}) \;\&\; X' = F(\underline{X}) \supset expr$$

This is taken to include the existence of a value of $F(\underline{X})$ under the conditions $p(\underline{X})$, i.e.:

$$p(\underline{X}) \supset (\exists \underline{X}')(\underline{X}' = F(\underline{X}))$$

2. Specification

For the approach used here, which uses formal proofs from the very beginning, a completely formal statement of the problem is essential. Preparation of such a specification is itself a useful informative exercise; in particular it ensures both a thorough understanding of what is required, and a realisation of what is not essential. The formal specification, while being complete, should not include suggestions of a method of solution - these belong to a later stage, since they require justification, while the problem specification is accepted just as it is. What is required is sufficient information for a solution of the problem to be recognised as adequate when it is found. (Equivalence to a certain algorithm gives this, but generally in much too strong a form, making the proofs unnecessarily difficult.)

Informally, the problem is to arrange the set V in some order such that the element in position f is the element which belongs in this position under the order $\leq$., and the elements below it are less than or equal to it and the elements above it are greater than or equal to it. If we denote this element by V[f], we must put the f-1 elements that are less than or equal to it below V[f], and the remaining elements above it. We are given that the initial set V is not empty, nor infinite, and that the number f we are given is a positive integer not greater than the number of elements in V.

Formally, the problem is to develop a program FIND, such that:-

$$\text{FIND: } \beta(U) \times I \rightarrow \beta(U)^3$$

and has the properties:-

1. $\alpha(V,f) \vdash \omega(V,f,\text{FIND}(V,f))$

where:-

2. $\alpha(V,f) =$
   $|V| \in I \;\&$ i.e. V is finite
   $|V| \geq 1 \;\&$
   $1 \leq f \leq |V|$

3. $\omega(V,f,V_1,V_2,V_3) =$
   $\text{pdis}(V_1,V_2,V_3) \;\&$
   $V_1 \cup V_2 \cup V_3 = V \;\&$
   $|V_1| = f-1 \;\&\; |V_2| = 1 \;\&$
   $V_1 \leq^* V_2 \leq^* V_3$

4. $\text{pdis}(X_1,X_2,\ldots,X_n) = \text{dis}(X_1,X_2) \;\&\; \text{dis}(X_1,X_3) \;\&\; \text{dis}(X_2,X_3) \;\&\; \ldots$

5. $\text{dis}(V,W) = \neg(\exists a)(a \in V \;\&\; a \in W)$

The relation $\leq^*$ is defined as:-

$$\leq^*: \beta(U) \times \beta(U) \rightarrow \{T,F\}$$

such that:-

6. $V \leq^* W = (a \in V \ \& \ b \in W \supset a \leq . b)$

We have the following two lemmas on pdis:-

7. $pdis(V_1,V_2,V_3) \ \& \ V_2 = X_4 \cup X_5 \cup X_6 \ \& \ pdis(X_4,X_5,X_6) \supset pdis(V_1,X_4,X_5,X_6,V_3)$

8. $pdis(V_1,X_4,X_5,X_6,V_3) \supset pdis(V_1 \cup X_4,X_5,X_6 \cup V_2) \ \& \ pdis(V_1,X_4,X_5 \cup X_6 \cup V_3) \ \& \ pdis(V_1 \cup X_4 \cup X_5,X_6,V_3)$

These follow simply from the definition of pdis.

Note that the specification does not exclude pairs of elements that are "equal" under the ordering, i.e. elements v_1 and v_2 such that:

$$v_1 \leq . v_2 \ \& \ v_2 \leq . v_1$$

However such elements are not regarded as identical, i.e.

$$v_1 \neq v_2$$

and they are distinct elements in the set V.

We shall use V and f throughout to denote the given data, hence we always have $\alpha(V,f)$. Where use is made of this fact, we quote 2.2 as the appropriate reference.

3. Formal Development

The above problem specification meets the requirements noted in Section 2, and the first requirement of formal development - namely that we should start at the most abstract level. Our initial stage of development will remain at this abstract level, and so will its formal justification. This enables the proof to use powerful, general, theorems of set theory and ordering relations directly, without translating them into theorems concerning other data types and relations. (In the example we do not introduce arrays at this point; the correspondence between integer subscripts and elements which they provide is not an essential part of the problem, but a part of the method of solution to be developed).

Starting from this most abstract form of the problem, we add details of the proposed method of solution stage by stage. Some stages will consist of mapping the data into more practical data-types, e.g. sets into one-dimensional arrays. Some may replace properties defining data by algorithms producing data having such properties. Some may replace operations having certain properties by other operations or algorithms having these properties. Each change requires a formal proof that the entities introduced do have the properties required of those at the previous stage that they replace. Thus the only proof of the overall correctness required is the first; successive stages then only involve proofs of theorems concerning the entities introduced at that stage, whose specification is drawn from the previous stage. In this way all proofs are kept as simple as possible, using concepts and results appropriate to the current step in development. Ultimately we aim to produce an algorithm which, given data with the properties stated in the problem specification, produces data having all the properties required of the result. The formal verification of each stage of the development then guarantees the correctness of the algorithm.

Experience indicates that at each stage, the minimum of additional constraints, in the form of specialized data types, operations or algorithms should be imposed (compare Dijkstra, ref 1). This has the merits of keeping the proofs simple, enabling the consequences of each particular decision to be assessed in isolation, and allowing as much freedom of choice as possible for later decisions.

Stage 1

The direction of development is towards an iterative process, in which three sets are initialized to $(\emptyset, V, \emptyset)$ and then iteratively recomputed so as to reduce the middle set, preserving the order

relations on the contents of the three sets and keeping V[f] in the middle set. We shall therefore require a predicate on three sets, such that when the middle set becomes a unit set it will ensure that we have a solution. In this section, we show that β_1 is such a predicate. (In subsequent sections we shall show that it is satisfied by $(\emptyset,V,\emptyset)$, and put a requirement on the function which recomputes the sets that it preserves the truth of this predicate.)

Assumptions

Suppose a function F1 can be found such that:-

$F1 : \beta(U) \times I \rightarrow \beta(U)^3$

1. $\alpha(V,f)\ \&\ (V_1,V_2,V_3)=F1(V,f) \vdash \beta_1(V,f,V_1,V_2,V_3)\ \&\ |V_2|=1$

where:-

2. $\beta_1(V,f,V_1,V_2,V_3) =$
$pdis(V_1,V_2,V_3)\ \&$
$V_1 \cup V_2 \cup V_3 = V\ \&$
$|V_1| < f \leq |V_1|+|V_2|\ \&$
$V_1 \leq^* V_2 \leq^* V_3$

Assertion

3. $FIND(V,f) = F1(V,f)$
satisfies 2.1.

Justification

The assertion follows from:-

4. $\alpha(V,f) \vdash \omega(V,f,F1(V,f))$

Proof

5.	$\alpha(V,f)$	Hyp

Writing:-

6. $(V_1,V_2,V_3) = F1(V,f)$

then:-

7.	$\beta_1(V,f,V_1,V_2,V_3)\ \&\ \|V_2\|=1$	5,6,1
8.	$pdis(V_1,V_2,V_3)$	7,2
9.	$V_1 \cup V_2 \cup V_3 = V$	7,2
10.	$\|V_1\| < f \leq \|V_1\|+\|V_2\|$	7,2
11.	$\|V_1\| = f-1$	10,7
12.	$V_1 \leq^* V_2 \leq^* V_3$	7,2
13.	$\omega(V,f,V_1,V_2,V_3)$	2.3,8,9,11,7,12
14.	$\omega(V,f,F1(V,f))$	13,6

This stage has merely changed the specifications of the overall function to a form more in keeping with the developments envisaged. The justification consists of showing that the new specification is at least as strong as the original.

4. Stage 2

In this stage we specify the initialisation of the three sets mentioned in section 3, and the overall requirements on the iteration. The initialisation function is $F2_1$, and the function computed by the complete sequence of iterations is $F2_2$.

Assumptions

Suppose functions can be found, such that:-

$F2_1 : \beta(U) \rightarrow \beta(U)^3$

1. $F2_1(V) = (\emptyset, V, \emptyset)$

$F2_2 : \beta(U)^3 \times I \rightarrow \beta(U)^3$

2. $\alpha(V,f)$ & $\beta_1(V,f,V_1,V_2,V_3)$ & $|V_2| \geq 1$ & $(V_1',V_2',V_3') = F2_2(V_1,V_2,V_3,f) \vdash \beta_1(V,f,V_1',V_2',V_3')$ & $|V_2'|=1$

Assertion

3. $F1(V,f) = F2_2(F2_1(V),f)$ satisfies 3.1.

Justification

The assertion follows from:-

4. $\alpha(V,f)$ & $(V_1',V_2',V_3') = F2_2(F2_1(V),f) \vdash \beta_1(V,f,V_1',V_2',V_3')$ & $|V_2'| = 1$

Proof

5.	$\alpha(V,f)$	Hyp
6.	$(V_1',V_2',V_3') = F2_2(F2_1(V),f)$	Hyp
	The empty set is disjoint from any set thus:-	
7.	$pdis(\emptyset,V,\emptyset)$	2.5,2.4
8.	$\emptyset \cup V \cup \emptyset = V$	
9.	$\|\emptyset\| = 0$	
10.	$0 < f \leq \|V\|$	5,2.2
11.	$\|\emptyset\| < f \leq \|\emptyset\| + \|V\|$	9,10
12.	$\emptyset \leq^* V \leq^* \emptyset$	2.6
13.	$\beta_1(V,f,\emptyset,V,\emptyset)$	3.2,7,8,11,12
14.	$\|V\| \geq 1$	5,2.2
	Using 2 with $(\emptyset,V,\emptyset)$ substituted for (V_1,V_2,V_3):-	
15.	$\beta_1(V,f,V_1',V_2',V_3')$ & $\|V_2'\| = 1$	5,13,14,6,1

The justification consists of showing that β_1 is true of the initialised sets, and therefore since its truth is preserved by

the iteration which also guarantees the extra condition $|V_2| = 1$, then the overall scheme satisfies the specification of F1 of the previous stage.

5. Stage 3

In this stage we develop the body of the iterated part of the algorithm, and the way in which the iteration is to be controlled so as to achieve a computation of $F2_2$ of the previous stage. We use a recursive definition of a function $(F3_2)$ for the latter purpose as a convenient notation at this point. This does not imply a commitment to use recursion in the final program; the choice of methods to implement the iteration is still open, and will depend on the facilities available in the programming language.

Assumptions

Suppose functions can be found such that:-

$P3 : \beta(U)^3 \rightarrow \{T,F\}$

1. $P3(V_1,V_2,V_3) = |V_2| > 1$

$F3_1 : \beta(U)^3 \times I \rightarrow \beta(U)^3$

2. $\beta_1(V,f,V_1,V_2,V_3) \;\&\; |V_2|>1 \;\&\; (V_1^1,V_2^1,V_3^1) = F3_1(V_1,V_2,V_3,f)$
$\vdash \beta_1(V,f,V_1^1,V_2^1,V_3^1) \;\&\; 0<|V_2^1|<|V_2|$

$F3_2 : \beta(U)^3 \times I \rightarrow \beta(U)^3$

3. $\neg P3(V_1,V_2,V_3) \vdash F3_2(V_1,V_2,V_3,f) = (V_1,V_2,V_3)$
4. $P3(V_1,V_2,V_3) \vdash F3_2(V_1,V_2,V_3,f) = F3_2(F3_1(V_1,V_2,V_3,f),f)$

Assertions

5. $F2_2(V_1,V_2,V_3,f) = F3_2(V_1,V_2,V_3,f)$
satisfies 4.2.

Justification

The assertion follows from:-

6. $\alpha(V,f) \;\&\; \beta_1(V,f,V_1,V_2,V_3) \;\&\; |V_2| \geq 1 \;\&\;$
$(V_1^1,V_2^1,V_3^1) = F3_2(V_1,V_2,V_3,f) \vdash$
$\beta_1(V,f,V_1^1,V_2^1,V_3^1) \;\&\; |V_2^1| = 1$

Proof

7.	$\alpha(V,f)$	Hyp
8.	$\beta_1(V,f,V_1,V_2,V_3)$	Hyp
9.	$\|V_2\| \geq 1$	Hyp
10.	$(V_1^1,V_2^1,V_3^1) = F3_2(V_1,V_2,V_3,f)$	Hyp

Now proceed by induction on $n = |V_2|$

Basis, assuming:-

11.	$\|V_2\| = 1$	
12.	$\neg P3(V_1,V_2,V_3)$	11,1

13. $F3_2(V_1,V_2,V_3,f) = (V_1,V_2,V_3)$ 3,12
14. $(V_1^1,V_2^1,V_3^1) = (V_1,V_2,V_3)$ 10,13
15. $\beta_1(V,f,V_1^1,V_2^1,V_3^1)$ & $|V_2^1| = 1$ 8,14,11

Now assume that the theorem holds for V_1,V_2,V_3 where $1 \leq |V_2| < n$. Then assuming:-

16. $|V_2| > 1$
17. $P3(V_1,V_2,V_3)$ 16,1
18. $F3_2(V_1,V_2,V_3,f) = F3_2(F3_1(V_1,V_2,V_3,f),f)$ 4,17
19. $(V_1^1,V_2^1,V_3^1) = F3_2(F3_1(V_1,V_2,V_3,f),f)$ 10,18

writing:-

20. $(V_1^{11},V_2^{11},V_3^{11}) = F3_1(V_1,V_2,V_3,f)$

then:-

21. $\beta_1(V,f,V_1^{11},V_2^{11},V_3^{11})$ & $0 < |V_2^{11}| < |V_2|$ 16,8,20,2
22. $(V_1^1,V_2^1,V_3^1) = F3_2(V_1^{11},V_2^{11},V_3^{11},f)$ 19,20

The assumption that the theorem holds for sets in which $|V_2^{11}| < n$ gives, writing $(V_1^{11},V_2^{11},V_3^{11})$ for (V_1,V_2,V_3):-

23. $\beta_1(V,f,V_1^1,V_2^1,V_3^1)$ & $|V_2^1| = 1$ 6,7,21,22

Hence by 15 and 23, 6 is true for all $|V_2|$.

The justification consists of an inductive proof, over the recursive structure of $F3_2$, that the truth of β_1 is preserved down to the point at which $|V_2| = 1$. At this point, by the definition of $F3_2$ the algorithm terminates. Note that the additional condition on $F3_1$, that $|V_2|$ is reduced by it, guarantees termination.

6. Stage 4

In this stage we develop $F3_1$ into a construction from two other functions, $F4_1$ and $F4_2$, where $F4_1$ breaks up V_2 into three subsets, and $F4_2$ recombines these with V_1 and V_3 to obtain new V_1, V_2, V_3 satisfying β_1.

Assumptions

Suppose functions $F4_1$ and $F4_2$ can be found, such that:-

$$F4_1 : \beta(U) \rightarrow \beta(U)^3$$

1. $|V_2|>1 \;\&\; |V_1|<f\leq|V_1|+|V_2| \;\&\; (X_4,X_5,X_6) = F4_1(V_2) \vdash \omega_4(V_2,X_4,X_5,X_6)$

$$F4_2 : \beta(U)^5 \times I \rightarrow \beta(U)^3$$

2. $\beta_1(V,f,V_1,V_2,V_3) \;\&\; \omega_4(V_2,X_4,X_5,X_6) \;\&\; (V_1^1,V_2^1,V_3^1) = F4_2(V_1,X_4,X_5,X_6,V_3,f) \vdash \beta_1(V,f,V_1^1,V_2^1,V_3^1) \;\&\; 0<|V_2^1|<|V_2|$

where:-

3. $\omega_4(V_2,X_4,X_5,X_6) =$
$\quad pdis(X_4,X_5,X_6) \;\&$
$\quad X_4 \cup X_5 \cup X_6 = V_2 \;\&$
$\quad (|X_4|\neq 0 \vee |X_5|\neq 0) \;\&$
$\quad (|X_5|\neq 0 \vee |X_6|\neq 0) \;\&$
$\quad (|X_4|\neq 0 \vee |X_6|\neq 0) \;\&$
$\quad X_4 \leq^* X_5 \leq^* X_6 \;\&$
$\quad X_4 \leq^* X_6$

(Note. The last term is necessary since X_5 can be $\emptyset$, and $\leq^*$ is not transitive across $\emptyset$.)

Assertion

4. $F3_1(V_1,V_2,V_3,f) = F4_2(V_1,F4_1(V_2),V_3,f)$
satisfies 5.2.

Justification

The assertion follows from:-

5. $\beta_1(V,f,V_1,V_2,V_3) \;\&\; |V_2|>1 \;\&\; (V_1^1,V_2^1,V_3^1) = F4_2(V_1,F4_1(V_2),V_3,f) \vdash \beta_1(V,f,V_1^1,V_2^1,V_3^1) \;\&\; 0<|V_2^1|<|V_2|$

Proof

6. $\beta_1(V,f,V_1,V_2,V_3)$ Hyp
7. $|V_2| > 1$ Hyp

writing:-

8. $(X_4, X_5, X_6) = F4_1(V_2)$

then:-

9.	$(V_1', V_2', V_3') = F4_2(V_1, X_4, X_5, X_6, V_3, f)$	Hyp,8
10.	$\|V_1\| < f \leq \|V_1\| + \|V_2\|$	6,3.2
11.	$\omega_4(V_2, X_4, X_5, X_6)$	7,8,10,1
12.	$\beta_1(V, f, V_1', V_2', V_3')$ & $0 < \|V_2'\| < \|V_2\|$	6,11,9,2

The justification shows that an appropriate combination of $F4_1$ and $F4_2$ has the properties required of $F3_1$. We continue with the development of $F4_2$.

7. Stage 5

In this stage we show that $F4_2$ can be defined by cases, depending on which of the three sets X_4, X_5, X_6 given by $F4_1$ contains the f th element. There results an explicit definition, in terms of operations on sets, of a function F5 that will serve as $F4_2$.

Assumptions

$$F5 : \beta(U)^5 \times I \to \beta(U)^3$$

1. $(V_1^1, V_2^1, V_3^1) = F5(V_1, X_4, X_5, X_6, V_3, f) \vdash$
$[\, f \leq |V_1| + |X_4| \supset (V_1^1, V_2^1, V_3^1) = (V_1, X_4, X_5 \cup X_6 \cup V_3) \,] \;\&$
$[\, |V_1| + |X_4| + |X_5| < f \supset (V_1^1, V_2^1, V_3^1) = (V_1 \cup X_4 \cup X_5, X_6, V_3) \,] \;\&$
$[\, |V_1| + |X_4| < f \leq |V_1| + |X_4| + |X_5| \supset$
$(V_1^1, V_2^1, V_3^1) = (V_1 \cup X_4, X_5, X_6 \cup V_3) \,]$

Assertion

2. $F4_2(V_1, X_4, X_5, X_6, V_3, f) = F5(V_1, X_4, X_5, X_6, V_3, f)$
satisfies 6.2.

Justification

The assertion follows from:-

3. $\beta_1(V, f, V_1, V_2, V_3) \;\&\; \omega_4(V_2, X_4, X_5, X_6) \;\&$
$(V_1^1, V_2^1, V_3^1) = F5(V_1, X_4, X_5, X_6, V_3, f) \vdash$
$\beta_1(V, f, V_1^1, V_2^1, V_3^1) \;\&\; 0 < |V_2^1| < |V_2|$

Proof

4.	$\beta_1(V, f, V_1, V_2, V_3)$	Hyp
5.	$\omega_4(V_2, X_4, X_5, X_6)$	Hyp
6.	$(V_1^1, V_2^1, V_3^1) = F5(V_1, X_4, X_5, X_6, V_3, f)$	Hyp
7.	$pdis(V_1, V_2, V_3)$	4,3.2
8.	$V_1 \cup V_2 \cup V_3 = V$	4,3.2
9.	$\|V_1\| < f \leq \|V_1\| + \|V_2\|$	4,3.2
10.	$V_1 \leq^* V_2 \leq^* V_3$	4,3.2
11.	$pdis(X_4, X_5, X_6)$	5,6.3
12.	$X_4 \cup X_5 \cup X_6 = V_2$	5,6.3
13.	$\|X_4\| \neq 0 \vee \|X_5\| \neq 0$	5,6.3
14.	$\|X_5\| \neq 0 \vee \|X_6\| \neq 0$	5,6.3
15.	$\|X_4\| \neq 0 \vee \|X_6\| \neq 0$	5,6.3
16.	$X_4 \leq^* X_5 \leq^* X_6$	5,6.3
17.	$X_4 \leq^* X_6$	5,6.3
18.	$pdis(V_1, X_4, X_5, X_6, V_3)$	7,11,12,2.7

Consider the three cases of the definition 1 of F5, first:-

19.	$f \leq \|V_1\|+\|X_4\|$	
20.	$(V_1^1,V_2^1,V_3^1) = (V_1, X_4, X_5 \cup X_6 \cup V_3)$	6,19,1
21	pdis(V_1^1,V_2^1,V_3^1)	18,2.8,20
22.	$V_1^1 \cup V_2^1 \cup V_3^1 = V_1 \cup X_4 \cup X_5 \cup X_6 \cup V_3$	20
23.	$= V$	22,12,8
24.	$\|V_1^1\| < f \leq \|V_1^1\|+\|V_2^1\|$	9,20,19
25.	$V_1 \leq^* X_4$	10,12,2.6
26.	$V_1^1 \leq^* V_2^1$	25,20
27.	$X_4 \leq^* V_3$	10,12,2.6
28.	$V_2^1 \leq^* V_3^1$	27,20,16,17,2.6
29.	$\beta_1(V,f,V_1^1,V_2^1,V_3^1)$	21,23,24,26,28,3.2
30.	$\|V_1\| < f \leq \|V_1\|+\|X_4\|$	9,19
31.	$0 < \|X_4\|$	30
32.	$\|X_4\| < \|V_2\|$	12,14,11
33.	$0 < \|V_2^1\| < \|V_2\|$	31,32,20
	which concludes the case.	29,33

The second case:-

34.	$\|V_1\|+\|X_4\|+\|X_5\| < f$	

is justified in a similar way.

The third case:-

35.	$\|V_1\|+\|X_4\| < f \leq \|V_1\|+\|X_4\|+\|X_5\|$	
36.	$(V_1^1,V_2^1,V_3^1) = (V_1 \cup X_4, X_5, X_6 \cup V_3)$	6,1,35
37.	pdis(V_1^1,V_2^1,V_3^1)	18,36,2.8
38.	$V_1^1 \cup V_2^1 \cup V_3^1 = V_1 \cup X_4 \cup X_5 \cup X_6 \cup V_3$	36
39.	$= V$	8,12
40.	$\|V_1^1\| < f \leq \|V_1^1\|+\|V_2^1\|$	35,36,18
41.	$V_1 \cup X_4 \leq^* X_5$	10,12,16
42.	$X_5 \leq^* X_6 \cup V_3$	10,12,16
43.	$V_1^1 \leq^* V_2^1 \leq^* V_3^1$	41,42,36
44.	$\beta_1(V,f,V_1^1,V_2^1,V_3^1)$	37,39,40,43,3.2
45.	$\|X_5\| > 0$	35
46.	$\|X_5\| < \|V_2\|$	15,12,11
47.	$0 < \|V_2^1\| < \|V_2\|$	45,46,36
	which concludes the case.	44,47

The justification shows that F5 as defined has the properties required of $F4_2$. Since we now have an explicit definition for F5 in terms of operations on sets, and the remaining functions $F4_2$ and $F3_1$ cannot be further developed in terms of sets, we must now consider mapping the algorithm as so far developed into data types which can be used in the programming language. For convenience we summarise the algorithm as developed in the next section, postponing the mapping until section 9.

8. Summary of Development

At this point we summarise the outstanding assumptions about functions not yet developed, and summarise the current state of development of the overall function FIND. We also provide an overall justification, based on the assertions proved in the preceding sections.

Assumptions

Suppose we have functions:-

1. $FIND1 : \beta(U) \times I \rightarrow \beta(U)^3$
2. $FIND1(V,f) = F3_2(F2_1(V),f)$ — 3.3, 4.3, 5.5

3. $F2_1 : \beta(U) \rightarrow \beta(U)^3$
4. $F2_1(V) = (\emptyset, V, \emptyset)$ — 4.1

5. $P3 : \beta(U)^3 \rightarrow \{T,F\}$
6. $P3(V_1,V_2,V_3) = |V_2|>1$ — 5.1

7. $F3_2 : \beta(U)^3 \times I \rightarrow \beta(U)^3$
8. $\neg P3(V_1,V_2,V_3) \vdash F3_2(V_1,V_2,V_3,f) = (V_1,V_2,V_3)$ — 5.3
9. $P3(V_1,V_2,V_3) \vdash F3_2(V_1,V_2,V_3,f) = F3_2(F5(V_1,F4_1(V_2),V_3,f),f)$ — 5.4, 6.4, 7.2

10. $F4_1 : \beta(U) \rightarrow \beta(U)^3$
11. $|V_2|>1 \;\&\; |V_1|<f\leq|V_1|+|V_2| \;\&\; (X_4,X_5,X_6) = F4_1(V_2) \vdash \omega_4(V_2,X_4,X_5,X_6)$ — 6.1

— where ω_4 is defined in 6.3,

12. $F5 : \beta(U)^5 \times I \rightarrow \beta(U)^3$
13. $(V_1',V_2',V_3') = F5(V_1,X_4,X_5,X_6,V_3,f) \vdash$
$[f\leq|V_1|+|X_4| \supset (V_1',V_2',V_3') = (V_1,X_4,X_5 \cup X_6 \cup V_3)] \;\&$
$[|V_1|+|X_4|+|X_5|<f \supset (V_1',V_2',V_3') = (V_1 \cup X_4 \cup X_5, X_6, V_3)] \;\&$
$[|V_1|+|X_4|<f\leq|V_1|+|X_4|+|X_5| \supset (V_1',V_2',V_3') = (V_1 \cup X_4, X_5, X_6 \cup V_3)]$ — 7.1

Assertion

14. $FIND(V,f) = FIND1(V,f)$ satisfies 2.1.

Justification

In justifying this assertion, we can use the assertions of previous sections provided their assumptions are shown to be met (or maintained as assumptions in this section).

Putting:-

15. $F4_2(V_1,X_4,X_5,X_6,V_3,f) = F5(V_1,X_4,X_5,X_6,V_3,f)$

we have:-

16. $F4_2(V_1,X_4,X_5,X_6,V_3,f)$ satisfies 6.2. 7.2,13

Putting:-

17. $F3_1(V_1,V_2,V_3,f) = F4_2(V_1,F4_1(V_2),V_3,f)$

we have:-

18. $F3_1(V_1,V_2,V_3,f) = F5(V_1,F4_1(V_2),V_3,f)$ 17,15
19. $F3_1(V_1,V_2,V_3,f)$ satisfies 5.2. 6.4,11,16
20. $P3(V_1,V_2,V_3) \vdash F3_2(V_1,V_2,V_3,f) = F3_2(F3_1(V_1,V_2,V_3,f),f)$ 9,18

Putting:-

21. $F2_2(V_1,V_2,V_3,f) = F3_2(V_1,V_2,V_3,f)$

we have:-

22. $F2_2(V_1,V_2,V_3,f)$ satisfies 4.2. 5.5,6,9,8,20

Putting:-

23. $F1(V,f) = F3_2(F2_1(V),f)$
24. $= FIND1(V,f)$ 23,21,4

we have:-

25. $F1(V,f)$ satisfies 3.1. 4.3,4,22

Finally, putting:-

26. $FIND(V,f) = F1(V,f)$
27. $= FIND1(V,f)$ 26,24

we have:-

28. $FIND(V,f)$ satisfies 2.1. 3.3,25

Since 2.1 is the original specification for the function FIND, the development so far is correct.

9. Stage 6

This stage maps the sets of section 8 into a new data type (available in the programming language) consisting of "duplicate free" arrays, and the functions from sets to sets into corresponding functions from arrays and indices to arrays and indices. The domain of arrays will be denoted by D:

$D: I \rightarrow U$

- i.e. the arrays are basically functions from I to U. We have:

1. $A \in D \supset (A = (A[1],A[2],\ldots,A[|V|])) \ \& \ \delta(A,1,|V|)$

- i.e. the arrays are indexed from 1 to $|V|$, and

$\delta : D \times I^2 \rightarrow \{T,F\}$

2. $\delta(A,x,y) = (x \leq u,v \leq y \ \& \ A[u]=A[v] \supset u=v)$

Various maps from $\beta(U)$ to D will be used, such that, if X maps into $A[x], A[x+1],\ldots,A[y]$, then $\theta(X,A,x,y)$, where:

$\theta : \beta(U) \times D \times I^2 \rightarrow \{T,F\}$

3. $\theta(X,A,x,y) = 1 \leq x \ \& \ x-1 \leq y \ \& \ y \leq |V| \ \& \ \delta(A,x,y) \ \& \ X = \{A[u] \mid x \leq u \leq y\}$

Note that, under this definition:

4. $\theta(X,A,x,y) \ \& \ \theta(Y,A,x,y) \supset X = Y$

that is, a particular part of an array is a map of the same set under any of these mappings.

A generalization of θ is also used:

5. $\theta((X_1,X_2,\ldots,X_n), (A,x_0,x_1,\ldots,x_n)) = \theta(X_1,A,x_0,x_1) \ \& \ \theta(X_2,A,x_1+1,x_2) \ \& \ \theta(X_3,A,x_2+1,x_3) \ \& \ \ldots \ \& \ \theta(X_n,A,x_{n-1}+1,x_n))$

The mappings used are not completely specified at this point; the order in which the elements of the set appear in the array may be different in different situations. The essential fact about the mappings, included formally in the definition of θ, is that the array obtained from a set shall have exactly the same elements, no more, no less, and none duplicated. With this property, it can be ensured that the requirements on the set arguments and results of the various functions which guarantee the correctness of the algorithm are satisfied, since these refer only to the sets - the order of elements within the arrays is immaterial.

Assumptions

Suppose we have functions:

$F6_0 : \beta(U) \rightarrow D$ (mapping V)

6. $A = F6_0(V) \vdash \theta(V,A,1,|V|)$

$F6_1 : D \rightarrow D \times I^2$ (mapping $F2_1$)

7. $\vdash F6_1(A) = (A,1,|V|))$

$P6 : D \times I^2 \rightarrow \{T,F\}$ (mapping P3)

8. $\vdash P6(A,m,n) \equiv m<n$

$F6_3 : D \times I^2 \rightarrow D \times I^2$ (mapping $F4_1$)

9. $0 \leq m-1 \leq n \leq |V| \ \& \ \delta(A,m,n) \ \& \ m<n \ \& \ m \leq f \leq n \ \&$
$(A',i',j') = F6_3(A,m,n) \vdash$
$\gamma_6(A,A',m,n) \ \& \ \delta(A',m,n) \ \& \ \omega_6(A',m,n,i',j')$

where:

10. $\gamma_6(A,A',m,n) =$
$(1 \leq u \leq m-1 \ \vee \ n+1 \leq u \leq |V| \supset A'[u] = A[u]) \ \&$
$\{A'[u] | \ m \leq u \leq n \ \} = \{A[u] | \ m \leq u \leq n\}$

11. $\omega_6(A,m,n,i,j) =$
$m-1 \leq j \leq i-1 \leq n \ \& \ \neg(i-1<m) \ \& \ \neg(n<j+1) \ \&$
$(m<j+1 \ \vee \ i-1<n) \ \&$
$(m \leq x \leq j \ \& \ j+1 \leq y \leq i-1 \supset A[x] \leq . A[y]) \ \&$
$(m \leq x \leq j \ \& \ i \leq y \leq n \supset A[x] \leq . A[y]) \ \&$
$(j+1 \leq x \leq i-1 \ \& \ i \leq y \leq n \supset A[x] \leq . A[y])$

$F6_4 : I^5 \rightarrow I^2$ (mapping F5)

12. $0 \leq m-1 \leq j \leq i-1 \leq n \leq |V| \ \& \ \delta(A,m,n) \ \&$
$(m',n') = F6_4(m,n,i,j,f) \vdash$
$(f \leq j \supset m'=m \ \& \ n'=j) \ \&$
$(i-1<f \supset m'=i \ \& \ n'=n) \ \&$
$(j<f \leq i-1 \supset m'=j+1 \ \& \ n'=i-1)$

$F6_2 : D \times I^3 \rightarrow D \times I^2$ (mapping $F3_2$)

13. $0 \leq m-1 \leq n \leq |V| \ \& \ m<n \ \& \ m \leq f \leq n \ \& \ \delta(A,m,n) \ \&$
$\neg P6(A,m,n) \vdash F6_2(A,m,n,f) = (A,m,n)$

14. $0 \leq m-1 \leq n \leq |V| \ \& \ m<n \ \& \ m \leq f \leq n \ \& \ \delta(A,m,n) \ \&$
$P6(A,m,n) \ \& \ (A',i',j') = F6_3(A,m,n) \vdash$
$F6_2(A,m,n,f) = F6_2(A',F6_4(m,n,i',j',f),f)$

$F6_5 : D \times I^2 \rightarrow \beta(U)^3$ (mapping the results)

15. $0 \leq m-1 \leq n \leq |V| \ \& \ \delta(A,1,m-1) \ \& \ \delta(A,m,n) \ \&$
$\delta(A,n+1,|V|) \ \& \ (V_1',V_2',V_3') = F6_5(A,m,n) \vdash$
$\theta((V_1',V_2',V_3'),(A,1,m-1,n,|V|))$

In the justifications below, we make use of the following lemmas:

16. $V_1 \cup V_2 \cup V_3 = V \ \& \ pdis(V_1,V_2,V_3) \supset$
$(\exists A,m,n)(\theta((V_1,V_2,V_3),(A,1,m-1,n,|V|)))$

Proof:

a. $V_1 \cup V_2 \cup V_3 = V$ Hyp

b. $pdis(V_1,V_2,V_3)$ Hyp

Let:
c. $m_1 = |V_1|+1$

and $(A_1,1,m_1)$ be such that:
d. $V_1 = \{A_1[u] | 1 \leq u \leq m_1-1\}$

This is possible, since V_1 contains m_1-1 elements. Since there are no duplicated elements in V_1, and $(A_1,1,m_1-1)$ contains each element of V_1 once and once only:
e. $\delta(A_1,1,m_1-1)$

Also:

f.	$0 \leq |V_1| \leq |V|$	a
g.	$0 \leq m_1-1$ & $m_1-1 \leq |V|$	c,f
h.	$\theta(V_1,A_1,1,m_1-1)$	g,e,d,3

Similarly with:
j. $n_1 = |V_1|+|V_2|$
k. $V_2 = \{A[u] | m_1 \leq u \leq n_1\}$

and
l. $V_3 = \{A[u] | n_1+1 \leq u \leq |V|\}$

we have:

m.	$\delta(A_1,m_1,n_1)$ & $\delta(A_1,n_1+1,|V|)$	
n.	$1 \leq m_1$ & $m_1-1 \leq n_1 \leq |V|$ & $1 \leq n_1+1$ & $n_1 \leq |V|$	
p.	$\theta(V_2,A_1,m_1,n_1)$	m,n,k,3
q.	$\theta(V_3,A_1,n_1+1,|V|)$	m,n,l,3
r.	$\theta((V_1,V_2,V_3),(A_1,1,m_1-1,n_1,|V|))$	h,p,q,5

- which proves the lemma, with $A = A_1$, $m = m_1$ and $n = n_1$.

17. $0 \leq m-1 \leq n \leq |V|$ & $\delta(A,1,m-1)$ & $\delta(A,m,n)$ & $\delta(A,m+1,|V|) \supset$
$(\exists V_1,V_2,V_3)(\theta((V_1,V_2,V_3),(A,1,m-1,n,|V|)))$

Proof:

a.	$0 \leq m-1 \leq n \leq |V|$	Hyp
b.	$\delta(A,1,m-1)$	Hyp
c.	$\delta(A,m,n)$	Hyp
d.	$\delta(A,n+1,|V|)$	Hyp
e.	$0 \leq m-1 \leq |V|$	a

Let:
f. $V_1 = \{A[u] | 1 \leq u \leq m-1\}$
g. $\theta(V_1,A,1,m-1)$ e,b,f

Similarly, let:
h. $V_2 = \{A[u] | m \leq u \leq n\}$
j. $\theta(V_2,A,m,n)$ a,c,h

and let:

k. $V_3 = \{A[u] | n+1 \leq u \leq |V|\}$

l. $\theta(V_3, A, n+1, |V|)$ a,d,k

m. $\theta((V_1, V_2, V_3), (A, 1, m-1, n, |V|))$ g,j,l,5

- and the conclusion follows.

Next we show that, whenever $F3_2$ (and hence F5 and $F4_1$) is used by the algorithm with arguments V_1, V_2, V_3, f, we have:

18. $\beta_1(V, f, V_1, V_2, V_3)$

Also that, whenever F5 and $F4_1$ are used, it is in the expression:

19. $F3_2(F5(V_1, F4_1(V_2), V, f), f)$

and in such cases:

20. $(X_4, X_5, X_6) = F4_1(V_1) \supset X_4 \cup X_5 \cup X_6 = V_2 \ \& \ pdis(X_4, X_5, X_6)$

For proofs, we note that all assumptions made prior to section 8 are justified by the definitions and assumptions of section 8. Under these assumptions we have:

21. $FIND(V, f) = F3_2(F2_1(V), f)$ 8.27,8.2

22. $\beta_1(V, f, \emptyset, V, \emptyset)$

- as shown in section 4 (4.13) from the hypothesis $\alpha(V, f)$ (2.2). Thus:

23. $(V_1, V_2, V_3) = F2_1(V) \supset \beta_1(V, f, V_1, V_2, V_3) \ \& \ |V_2| > 1$ 8.4,22,2.2

- so the conclusion is true for the initial arguments to $F3_2$. All other uses of $F3_2$ arise from 8.9 (as do all uses of $F4_1$ and F5). In such cases we have:

24. $P3(V_1, V_2, V_3)$

- where V_1, V_2, V_3 are prior arguments to $F3_2$. We assume for these prior arguments:

25. $\beta_1(V, f, V_1, V_2, V_3)$

Then, by 7.2, F5 satisfies the conditions of 6.2 on $F4_2$ of these arguments; thence, by 6.4, $F5(V_1, F4_1(V_2), V_3, f)$ satisfies the conditions of 5.2 on $F3_1(V_1, V_2, V_3)$, i.e.:

26. $\beta_1(V, f, V_1, V_2, V_3) \ \& \ |V_2| > 1 \ \&$
$(V_1'', V_2'', V_3'') = F5(V_1, F4_1(V_2), V_3, f) \supset$
$\beta_1(V, f, V_1'', V_2'', V_3'') \ \& \ 0 < |V_2''| < |V_2|$

27. $|V_2| > 1$ 24,8.6

28. $(V_1'', V_2'', V_3'') = F5(V_1, F4_1(V_2), V_3, f) \supset \beta_1(V, f, V_1'', V_2'', V_3'')$ 25,27,26

- i.e. β_1 is true of the new arguments to $F3_2$. Since it is true of the initial arguments, by 23, then by induction it is true for all arguments to $F3_2$.

Also, since β_1 is true of all arguments to $F3_2$, we have, for such arguments:

29. $|V_1|<f\leq|V_1|+|V_2|$

$F4_1$ is used on these arguments if and only if:

30. $|V_2|>1$ 8.9,8.6

(i.e. $P3(V_1,V_2,V_3)$ is true) thus:

31. $(X_4,X_5,X_6) = F4_1(V_2) \supset \omega_4(V_2,X_4,X_5,X_6)$ 8.11,29,30

32. $\supset X_4 \cup X_5 \cup X_6 = V_2 \ \&\ pdis(X_4,X_5,X_6)$ 31,6.3.

Thus, in mapping the functions $F3_2$, F5,F4, we may use 18 as an hypothesis on the arguments to $F3_2$, and 18 and 20 as hypothesis on those of F5 and $F4_1$.

We now show that the various functions specified in this section map those of the development so far. In general, for a function $F'(\underline{Y})$ of arguments $\underline{Y}$ to map a function $F(\underline{X})$ of arguments $\underline{X}$ under a relation $MAP(\underline{X},\underline{Y})$ we require:

$$PRE\text{-}F(\underline{X}) \supset (\exists \underline{Y})(MAP(\underline{X},\underline{Y}))$$
$$PRE\text{-}F(\underline{X}) \ \&\ MAP(\underline{X},\underline{Y}) \supset PRE\text{-}F'(\underline{Y})$$
$$PRE\text{-}F(\underline{X}) \ \&\ MAP(\underline{X},\underline{Y}) \ \&\ \underline{Y}' = F'(\underline{Y}) \supset (\exists \underline{X}')(MAP(\underline{X}',\underline{Y}'))$$
$$PRE\text{-}F(\underline{X}) \ \&\ MAP(\underline{X},\underline{Y}) \ \&\ \underline{Y}' = F'(\underline{Y}) \ \&\ MAP(\underline{X}',\underline{Y}') \supset POST\text{-}F(\underline{X},\underline{X}')$$

- where the specifications for $F(\underline{X})$ and $F'(\underline{Y})$ are of the forms:

$$PRE\text{-}F(X) \ \&\ X'=F(X) \supset POST\text{-}F(\underline{X},\underline{X}')$$
$$PRE\text{-}F'(\underline{Y}) \ \&\ \underline{Y}' = F'(\underline{Y}) \supset POST\text{-}F'(\underline{Y},\underline{Y}')$$

The assertions that follow are the non-trivial cases of the four relations above.

Assertion 1

33. $(\exists A,m,n)(\theta(V,A,m,n))$

34. $\theta(V,A,m,n) \ \&\ (A',m',n') = F6_1(A) \supset$
$(\exists V_1^1,V_2^1,V_3^1)(\theta((V_1^1,V_2^1,V_3^1),(A_1^1,1,m'-1,n',|V|)))$

35. $\theta(V,A,m,n) \ \&\ (A',m',n') = F6_1(A) \ \&$
$\theta((V_1^1,V_2^1,V_3^1),(A',1,m'-1,n',|V|)) \supset$
$V_1^1=\emptyset \ \&\ V_2^1=V \ \&\ V_3^1=\emptyset$

- and hence $F6_1$ maps $F2_1$.

Justification

36. $(\exists A)(\theta(V,A,1,|V|))$

- and 33 follows, with 1 as the m and $|V|$ as the n. For 34 we have:

37.	$\theta(V,A,m,n)$	Hyp
38.	$(A',m',n') = F6_1(A)$	Hyp
39.	$A'=A \ \& \ m'=1 \ \& \ n'=\|V\|$	38,7
40.	$0\leq m'-1\leq n'\leq\|V\|$	39,2.2
41.	$1\leq m \ \& \ m-1\leq n \ \& \ n\leq\|V\|$	37,3
42.	$\delta(A,m,n)$	37,3
43.	$V = \{A[u] \mid m\leq u\leq n\}$	37,3
44.	$\|V\| = n-m+1$	42,43
45.	$m>1 \supset n>\|V\|$	44
46.	$m\leq 1$	45,41
47.	$m = 1$	46,41
48.	$n = \|V\|$	47,44
49.	$\delta(A',1,\|V\|)$	42,39,47,48
50.	$\delta(A',1,m'-1) \ \& \ \delta(A',m',n') \ \& \ \delta(A',n'+1,\|V\|)$	49,40,2
51.	$(\exists V_1^1,V_2^1,V_3^1)(\theta(((V_1^1,V_2^1,V_3^1),(A',1,m'-1,n',\|V\|))))$	40,50,17

- which proves 34. For 35, we have the hypotheses 37,38 above, and hence the results 39 - 51 of that proof, and also:

52.	$\theta((V_1^1,V_2^1,V_3^1),(A',1,m'-1,n',\|V\|))$	Hyp
53.	$\theta(V_1^1,A',1,m'-1)$	52,5
54.	$V_1^1 = \emptyset$	53,39,3
55.	$\theta(V_2^1,A',m',n')$	52,5
56.	$V_2^1 = V$	55,39,3
57.	$\theta(V_3^1,A',m'+1,\|V\|)$	52,5
58.	$V_3^1 = \emptyset$	57,39,3

and the conclusion follows from 54, 56, 58.

Assertion 2

59. $(\exists A,m,n)(\theta((V_1,V_2,V_3),(A,1,m-1,n,|V|))$
60. $\theta((V_1,V_2,V_3),(A,1,m-1,n,|V|)) \supset m<n \equiv |V_2|>1$

and hence P6 maps P3.

Justification

61. $V_1 \cup V_2 \cup V_3 = V \ \& \ pdis(V_1,V_2,V_3)$ 18

- and 59 follows from this and 16.

For 60:

62.	$\theta(((V_1,V_2,V_3),(A,1,m-1,n,\|V\|))$	Hyp
63.	$\theta(V_2,A,m,n)$	62,5
64.	$\delta(A,m,n)$	63,3
65.	$V_2 = \{A[u] \mid m \leq u \leq n\}$	63,3
66.	$\|V_2\| = n-m+1$	64,65
67.	$m<n \equiv \|V_2\|>1$	66

- proving 60.

Assertion 3

68. $|V_2|>1 \ \& \ |V_1|<f\leq|V_1|+|V_2| \supset$
$(\exists A,m,n)(\theta(((V_1,V_2,V_3),(A,1,m-1,n,|V|)))$

69. $|V_2|>1 \ \& \ |V_1|<f\leq|V_1|+|V_2| \ \& \ \theta((V_1,V_2,V_3)|(A,1,m-1,n,|V|)) \supset$
$0\leq m-1\leq n\leq|V| \ \& \ \delta(A,m,n) \ \& \ m<n \ \& \ m\leq f\leq n$

70. $|V_2|>1 \ \& \ |V_1|<f\leq|V_1|+|V_2| \ \& \ \theta((V_1,V_2,V_3),(A,1,m-1,n,|V|)) \ \&$
$(A',i',j') = F6_3(A,m,n) \supset$
$(\exists X_4,X_5,X_6)(\theta((X_4,X_5,X_6),(A',m,j',i'-1,n)))$

71. $|V_2|>1 \ \& \ |V_1|<f\leq|V_1|+|V_2| \ \& \ \theta((V_1,V_2,V_3),(A,1,m-1,n,|V|)) \ \&$
$(A',i',j') = F6_3(A,m,n) \ \&$
$\theta((X_4,X_5,X_6),(A',m,j',i'-1,n)) \supset \omega_4(V_2,X_4,X_5,X_6)$

and hence $F6_3$ maps $F4_1$.

Justification

72. $V_1 \cup V_2 \cup V_3 = V \ \& \ pdis(V_1,V_2,V_3)$ 18

and the conclusion of 68 follows from this and 16.

For 69:

73.	$\|V_2\|>1$	Hyp
74.	$\|V_1\|<f\leq\|V_1\|+\|V_2\|$	Hyp
75.	$\theta(((V_1,V_2,V_3),(A,1,m-1,n,\|V\|))$	Hyp
76.	$0\leq m-1\leq n\leq\|V\|$	75,5,3
77.	$\delta(A,m,n)$	75,5,3
78.	$V_2 = \{A[u] \mid m\leq u\leq n\}$	75,5,3
79.	$\|V_2\| = n-m+1$	77,78
80.	$m<n$	73,79
81.	$\|V_1\| = m-1$	75,5,3
82.	$m-1<f\leq n$	74,79,81
83.	$m\leq f\leq n$	82

- and the conclusion follows from 76, 77, 80, 83.

For 70 we have the hypotheses 73 - 75, and hence the statements 76 - 82 of the above proof, and also:

84.	$(A',i',j') = F6_3(A,m,n)$	Hyp

85. $\gamma_6(A,A',m,n)$ & $\delta(A',m,n)$ & $\omega_6(A',m,n,i',j')$ 8.9,76,77,80, 83,84
86. $1 \leq m$ & $m-1 \leq j'$ & $j' \leq |V|$ 76,85,11
87. $\delta(A',m,j')$ 85,86,2

Now, let:
88. $X_4 = \{A'[u] | m \leq n \leq j'\}$

then:
89. $\theta(X_4,A',m,j')$ 86,87,88,3

Similarly with:
90. $X_5 = \{A'[u] | j'+1 \leq u \leq i'-1\}$
91. $\theta(X_5,A',j'+1,i'-1)$

and with:
92. $X_6 = \{A'[u] | i' \leq u \leq n\}$
93. $\theta(X_6,A',i',n)$
94. $\theta((X_4,X_5,X_6),(A,m,j',i'-1,n))$ 89,91,93,5

- which proves 70. For 71 we have the hypotheses 73 - 75, 84, and:
95. $\theta((X_4,X_5,X_6),(A,m,j',i'-1,n))$ Hyp

- from which the definitions 88,90,82 follow by 5 and 3.
Then the statements 76-94 are valid, and:
96. $\delta(A',m,n)$ 85
97. $pdis(X_4,X_5,X_6)$ 88,90,92,96
98. $X_4 \cup X_5 \cup X_6 = \{A[u] | m \leq u \leq n\}$ 88,90,92
99. $= V_2$ 98,78
100. $m-1 \leq j' \leq i'-1 \leq n$ 85,8.11
101. $i'-1 \leq n$ 85,8.11
102. $m \leq j'+1$ 85,8.11
103. $m < j'+1 \vee i'-1 < n$ 85,8.11
104. $|X_4| = j'-m+1$ & $|X_5| = i'-j'-1$ & $|X_6| = n-i'+1$ 88,90,92,100
105. $|X_4|>0 \vee |X_6|>0$ 103,104
106. $|X_5| = 0 \supset i'-1 = j'$ 104
107. $\supset i' \leq m$ 106,102
108. $\supset i' < n$ 107,80
109. $\supset |X_6| \neq 0$ 108,104
110. $\supset n \leq j'$ 106,101
111. $\supset m < j'$ 110,80
112. $\supset |X_4| \neq 0$ 111,104
113. $(|X_4| \neq 0 \vee |X_6| \neq 0)$ & $(X_5 | \neq 0 \vee |X_6| \neq 0)$ & $(|X_5| \neq 0 \vee |X_4| \neq 0)$ 105,109,112
114. $m \leq x \leq j'$ & $j'+1 \leq y \leq i'-1 \supset A'[x] \leq. A'[y]$ 85,8.11
116. $X_4 \leq^* X_5$ 114,88,90
117. $m \leq x \leq j'$ & $i' \leq y \leq n \supset A'[x] \leq. A'[y]$ 85,8.11

118. $X_4 \leq^* X_6$ 116,88,92
119. $j'+1 \leq x \leq i'-1$ & $i' \leq y \leq n \supset A'[x] \leq. A'[y]$ 85,8.11
120. $X_5 \leq^* X_6$ 119,90,92
121 $\omega_4(V_2, X_4, X_5, X_6)$ 6.3,97,99,113, 116,118,120

- proving 71.

Assertion 4

122. $(\exists A,m,n,i,j)(\theta((V_1,X_4,X_5,X_6,V_3),(A,1,m-1,j,i-1,n,|V|)))$
123. $\theta((V_1,X_4,X_5,X_6,V_3),(A,1,m-1,j,i-1,n,|V|)) \supset$
$0 \leq m-1 \leq j \leq i-1 \leq n \leq |V|$ & $\delta(A,m,n)$
124. $\theta((V_1,X_4,X_5,X_6,V_3),(A,1,m-1,j,i-1,n,|V|))$ &
$(m',n') = F6_4(m,n,i,j,f) \supset$
$(\exists V_1^1,V_2^1,V_3^1)(\theta((V_1^1,V_2^1,V_3^1),(A,1,m'-1,n',|V|)))$
125. $\theta((V_1,X_4,X_5,X_6,V_3),(A,1,m-1,j,i-1,n,|V|))$ &
$(m',n') = F6_4(m,n,i,j,f)$ &
$\theta((V_1^1,V_2^1,V_3^1),(A,1,m'-1,n',|V|)) \supset$
$[f \leq |V_1|+|X_4| \supset (V_1^1,V_2^1,V_3^1) = (V_1,X_4,X_5 \cup X_6 \cup V_3)]$ &
$[|V_1|+|X_4|+|X_5| < f \supset (V_1^1,V_2^1,V_3^1) = (V_1 \cup X_4 \cup X_5, X_6, V_3)]$ &
$[|V_1|+|X_4| < f \leq |V_1|+|X_4|+|X_5| \supset$
$(V_1^1,V_2^1,V_3^1) = (V_1 \cup X_4, X_5, X_6 \cup V_3)]$

and hence $F6_4$ maps F5.

Justification

126. $X_4 \cup X_5 \cup X_6 = V_2$ & $pdis(X_4,X_5,X_6)$ 20
127. $V_1 \cup V_2 \cup V_3 = V$ & $pdis(V_1,V_2,V_3)$ 18

Now let:
128. $m_1 = |V_1|+1$

and let the first m_1-1 elements of A_1 be those of V_1:
129. $V_1 = \{A_1[u] | 1 \leq u \leq m_1-1\}$ & $\delta(A_1,1,m_1-1)$
130. $0 \leq m_1-1 \leq |V|$ 127,128
131. $\theta(V_1,A_1,1,m_1-1)$ 130,129,3

Let:
132. $j_1 = |X_4|+m_1-1$

and the elements from m_1 to j_1 of A_1 be those of X_4:
133. $X_4 = \{A_1[u] | m_1 \leq u \leq j_1\}$ & $\delta(A_1,m_1,j_1)$
134. $1 \leq m_1$ & $m_1-1 \leq j_1$ & $j_1 \leq |V|$ 126,127,130,132
135. $\theta(X_4,A_1,m_1,j_1)$ 134,133,3

Let:
137. $i_1 = |X_5|+j_1+1$

and the elements from j_1+1 to i_1-1 of A_1 be those of X_5:

138. $X_5 = \{A_1[u] | j_1+1 \leq u \leq i_1-1\} \ \& \ \delta(A_1, j_1+1, i_1-1)$
139. $1 \leq j_1+1 \ \& \ j_1 \leq i_1-1 \ \& \ i_1-1 \leq |V|$ 132,130,137,128, 126,127
140. $\theta(X_5, A_1, j_1+1, i_1-1)$ 138,139,3

Let:

141. $n_1 = |X_6| + i_1 - 1$

and the elements from i_1 to n_1 of A_1 be those of X_6:

142. $X_6 = \{A[u] | i_1 \leq u \leq n_1\} \ \& \ \delta(A_1, i_1, n_1)$
143. $1 \leq i_1 \ \& \ i_1-1 \leq n_1 \ \& \ n_1 \leq |V|$ 139,141,126,127
144. $\theta(X_6, A_1, i_1, n_1)$ 142,143,3

and let the elements from n_1+1 to $|V|$ of A_1 be those of V_3:

145. $V_3 = \{A[u] | n_1+1 \leq u \leq |V|\} \ \& \ \delta(A, n_1+1, |V|)$

(for $|V_3| = |V| - |V_1| - |V_2|$ 127
$= |V| - |V_1| - |X_4| - |X_5| - |X_6|$ 126
$= |V| - n_1$) 141,137,132,128

146. $1 \leq n_1+1 \ \& \ n_1 \leq |V|$ 143
147. $\theta(V_3, A_1, n_1+1, |V|)$ 146,145,3
148. $\theta((V_1, X_4, X_5, X_6, V_3), (A, 1, m_1-1, j_1, i_1-1, n_1, |V|))$

proving 122. For 123:

149. $\theta((V_1, X_4, X_5, X_6, V_3), (A, 1, m-1, j, i-1, n, |V|))$ Hyp
150. $\theta(V_1, A, 1, m-1)$ 149,5
151. $0 \leq m-1$ 150,3
152. $\theta(X_4, A, m, j)$ 149,5
153. $m-1 \leq j$ 152,3
154. $\theta(X_5, A, j+1, i-1)$ 149,5
155. $j \leq i-1$ 154,3
156. $\theta(X_6, A, i, n)$ 149,5
157. $i-1 \leq n$ 156,3
158. $\theta(V_3, A, n-1, |V|)$ 149,5
159. $n \leq |V|$ 158,3
160. $\delta(A, m, j)$ 152,3
161. $\delta(A, j+1, i-1)$ 154,3
162. $\delta(A, i, n)$ 156,3
163. $\delta(A, m, n)$ 160-162,126

- and the conclusion of 123 follows from 151, 153, 155, 157, 159, 163. For 124 we have the hypothesis 149, and hence the statements 150-163, and also:

164. $(m', n') = F6_4(m, n, i, j, f)$ Hyp
165. $0 \leq m-1 \leq j \leq i-1 \leq n \leq |V| \ \& \ \delta(A, m, n)$

- as proved above.

166. $f \leq j \supset m' = m \ \& \ n' = j$ 164,165,8.12

167. $i-1<f \supset m'=i \;\&\; n'=n$ 164,165,8.12
168. $j<f\leq i-1 \supset m'=j+1 \;\&\; n'=i-1$ 164,165,8.12

and we consider the three cases separately.

Case 1

169. $f\leq j$
170. $m'=m \;\&\; n'=j$ 169,166

Put:
171. $V_1^1 = V_1$
172. $\theta(V_1^1,A,1,m'-1)$ 150,171,170

Put:
173. $V_2^1 = X_4$
174. $\theta(V_2^1,A,m',n')$ 152,173,170

Put:
175. $V_3^1 = \{A[u] \mid j+1\leq u\leq |V|\}$
176. $pdis(X_5,X_6,V_3)$ 126,127
177. $\delta(A,j+1,|V|)$ 154,156,158,3, 176
178. $1\leq j+1 \;\&\; j\leq |V|$ 154,152,3
179. $\theta(V_3^1,A,j+1,|V|)$ 178,177,175,3
180. $\theta(V_3^1,A,n'+1,|V|)$ 179,170
181. $\theta((V_1^1,V_2^1,V_3^1),(A,1,m'-1,n',|V|))$ 172,174,180

proving 123 for this case.

Case 2

182. $i-1<f$
183. $m'=i \;\&\; n'>n$ 182,167

Put:
184. $V_1^1 = \{A[u] \mid 1\leq u\leq i-1\}$
185. $pdis(V_1,X_4,X_5)$ 126,127
186. $\delta(A,1,i-1)$ 150,152,154,3
187. $0\leq i-1 \;\&\; i-1\leq |V|$ 156,3,154
188. $\theta(V_1^1,A,1,i-1)$ 187,186,184,3
189. $\theta(V_1^1,A,1,m'-1)$ 188,183

Put:
190. $V_2^1 = X_6$
191. $\theta(V_2^1,A,m',n')$ 156,183

Put:
192. $V_3^1 = V_3$

193. $\theta(V_3^1, A, n'+1, |V|)$
194. $\theta((V_1^1, V_2^1, V_3^1), (A, 1, m'-1, n', |V|))$ 189,191,193,5

proving 123 for this case.

Case 3
195. $j < f \leq i-1$
196. $m' = j+1$ & $n' = i-1$ 195,168

Put:
197. $V_1^1 = \{A[u] \mid 1 \leq u \leq j\}$
198. $pdis(V_1, X_4)$ 126,127
199. $\delta(A, 1, j)$ 150,152,3,198
200. $0 \leq j$ & $j \leq |V|$ 154,3,152
201. $\theta(V_1^1, A, 1, j)$ 200,199,197,3
202. $\theta(V_1^1, A, 1, m'-1)$ 201,196

Put:
203. $V_2^1 = X_5$
204. $\theta(V_2^1, A, m', n')$ 154,196

Put:
205. $V_3^1 = \{A[u] \mid i \leq u \leq |V|\}$
206. $pdis(X_6, V_3)$ 126,127
207. $\delta(A, i, |V|)$ 156,158,3,206
208. $1 \leq i$ & $i-1 \leq |V|$ 156,3,154
209. $\theta(V_3^1, A, i, |V|)$ 208,207,205,3
210. $\theta(V_3^1, A, n'+1, |V|)$ 209,196
211. $\theta((V_1^1, V_2^1, V_3^1), (A, 1, m'-1, n', |V|))$ 202,204,210,5

proving 123 for this case. Now:
212. $f \leq j \vee j < f \leq i-1 \vee i-1 < f$ 155

- hence these three cases exhaust the possibilities, and 123 is proved.

For 124, we have hypotheses 149, 164 and hence the statements 150 - 168. Also:
213. $\theta((V_1^1, V_2^1, V_3^1), (A, 1, m'-1, n', |V|))$ Hyp
214. $\theta(V_1^1, A, 1, m'-1)$ 213,5
215. $\theta(V_2^1, A, m', n')$ 213,5
216. $\theta(V_3^1, A, n'+1, |V|)$ 213,5

and we consider the three terms of the conclusion separately.

Case 1 Assuming:

217. $f \leq |V_1| + |X_4|$
218. $f \leq j$ 217,150,152
219. $m' = m$ & $n' = j$ 166,218
220. $\theta(V_1', A, 1, m-1)$ 214,219
221. $\theta(V_2', A, m, j)$ 215,219
222. $\theta(V_3', A, j+1, |V|)$ 216,219
223. $V_1' = V_1$ 220,150,4
224. $V_2' = X_4$ 221,152,4
225. $pdis(X_5, X_6, V_3)$ 126,127
226. $V_3' = X_5 \cup X_6 \cup V_3$ 154,156,158,225
227. $f \leq |V_1| + |X_4| \supset (V_1', V_2', V_3') = (V_1, X_4, X_5 \cup X_6 \cup V_3)$ 223,224,226

- recalling assumption 217.

Case 2. Assuming:

228. $|V_1| + |X_4| + |X_5| < f$
229. $i-1 \leq f$ 228,150,152,154
230. $m' = i$ & $n' = n$ 229,167
231. $\theta(V_1', A, 1, i-1)$ 214,230
232. $\theta(V_2', A, i, n)$ 215,230
233. $\theta(V_3', A, n+1, |V|)$ 216,230
234. $pdis(V_1, X_4, X_5)$ 126,127
235. $V_1' = V_1 \cup X_4 \cup X_5$ 150,152,154,234 231
236. $V_2' = X_6$ 232,156,4
237. $V_3' = V_3$ 233,158,4
238. $|V_1| + |X_4| + |X_5| < f \supset (V_1', V_2', V_3') = (V_1 \cup X_4 \cup X_5, X_6, V_3)$ 235,236,237

- recalling assumption 228.

Case 3. Assuming:

239. $|V_1| + |X_4| < f \leq |V_1| + |X_4| + |X_5|$
240. $j < f \leq i-1$ 218,229
241. $m' = j+1$ & $n' = i-1$ 240,168
242. $\theta(V_1', A, 1, j)$ 214,241
243. $\theta(V_2', A, j+1, i-1)$ 215,241
244. $\theta(V_3', A, i, |V|)$ 216,241
245. $dis(V_1, X_4)$ 126,127
246. $V_1' = V_1 \cup X_4$ 150,152,245,242
247. $V_2' = X_5$ 243,154
248. $dis(X_6, V_3)$ 126,127
249. $V_3' = X_6 \cup V_3$ 156,158,248,244
250. $|V_1| + |X_4| < f \leq |V_1| + |X_4| + |X_5| \supset$
$(V_1', V_2', V_3') = (V_1 \cup X_4, X_5, X_6 \cup V_3)$ 246,247,249

- recalling assumption 239. Then 125 follows from 227, 238 and 250.

Assertion 5

251. $(\exists A,m,n)(\theta((V_1,V_2,V_3),(A,1,m-1,n,|V|)))$
252. $\theta((V_1,V_2,V_3),(A,1,m-1,n,|V|)) \ \&\ (A',m',n') = F6_2(A,m,n,f) \supset$
$(\exists V_1',V_2',V_3')(\theta((V_1',V_2',V_3'),(A',1,m'-1,n',|V|)))$

- and hence $F6_2$ maps $F3_2$.

Justification

251 is identical to 59, and has been proved above. For 252 we have an induction on:
253. $k = n-m$

as follows:

254. $k \leq 0$	Hyp
255. $\theta((V_1,V_2,V_3),(A,1,m-1,n,\|V\|))$	Hyp
256. $(A',m',n') = F6_2(A,m,n,f)$	Hyp
257. $\neg P6(A,m,n)$	254,253,8
258. $0 \leq m-1 \leq n \leq \|V\|$	255,5,3
259. $\delta(A,m,n)$	255,5,3
260. $F6_2(A,m,n,f) = (A,m,n)$	258,259,257,13
261. $(A',m',n') = (A,m,n)$	256,260
262. $\theta((V_1,V_2,V_3),(A',1,m'-1,n',\|V\|))$	255,261

- and the conclusion follows.

Now assume that the theorem is true for $n_1-m_1<k$, i.e. writing:
263. $k_1 = n_1-m_1$
264. $k_1<k \ \&\ \theta((V_{11},V_{21},V_{31}),(A_1,1,m_1-1,n_1,|V|)) \ \&$
$(A_1',m_1',n_1') = F6_2(A_1,m_1,n_1,f) \supset$
$(\exists V_1',V_2',V_3')(\theta((V_1',V_2',V_3'),(A_1',1,m_1'-1,n_1',|V|)))$

We prove that it is true for $k>0$ as follows:

265. $k>0$	Hyp
266. $\theta((V_1,V_2,V_3),(A,1,m-1,n,\|V\|))$	Hyp
267. $(A',m',n') = F6_2(A,m,n,f)$	Hyp

Since A,m,n map V_1,V_2,V_3 and $F6_2$ maps $F3_2$, by 18 we have:

268. $\beta_1(V,f,V_1,V_2,V_3)$	
269. $\|V_1\|<f\leq\|V_1\|+\|V_2\|$	268,3.2
270. $m<f\leq n$	269,266,5,3
271. $m<n$	265,253
272. $0 \leq m-1 \leq n \leq \|V\|$	266,5,3
273. $\delta(A,m,n)$	266,5,3
274. $(\exists A',i',j')(A',i',j') = F6_3(A,m,n))$	272,273,271, 270,9

Let A_2,i_2,j_2 be such, so that:
275. $(A_2,i_2,j_2) = F6_3(A,m,n)$

276. $\gamma_6(A,A_2,m,n)$ & $\delta(A_2,m,n)$ & $\omega_6(A_2,m,n,i_2,j_2)$ 9

Now we have:

277. $|V_2|>1$ 266,5,3,271

278. $(\exists X_4,X_5,X_6)(\theta((X_4,X_5,X_6),(A_2,m,j_2,i_2-1,n))$ 277,269,266,275 70

Let X_4,X_5,X_6 be such, so that:

279. $\theta((X_4,X_5,X_6),(A_2,m,j_2,i_2-1,n))$

280. $\omega_4(V_2,X_4,X_5,X_6)$ 277,269,266,275 279,71

281. $\theta(V_1,A_2,1,m-1)$ & $\theta(V_3,A_2,n+1,|V|)$ 266,5,3,276,10

282. $\theta((V_1,X_4,X_5,X_6,V_3),(A_2,1,m-1,j_2,i_2-1,n,|V|))$ 281,279,5

283. $0\leq m-1\leq j_2\leq i_2-1\leq n\leq|V|$ & $\delta(A_2,m,n)$ 282,123

284. $(\exists m',n')((m',n')=F6_4(m,n,i_2,j_2,f))$ 283,12

Let m_2,n_2 be such, so that:

285. $(m_2,n_2)=F6_4(m,n,i_2,j_2,f)$

286. $(\exists V_1^1,V_2^1,V_3^1)(\theta((V_1^1,V_2^1,V_3^1),(A_2,1,m_2-1,n_2,|V|)))$ 282,285,124

Let V_{11},V_{21},V_{31} be such, so that:

287. $\theta((V_{11},V_{21},V_{31}),(A_2,1,m_2-1,n_2,|V|))$

288. $(V_{11},V_{21},V_{31})=F5(V_1,X_4,X_5,X_6,V_3,f)$ 282,285,287,13

Now, by 7.2, (V_{11},V_{21},V_{31}) satisfy the conditions of 6.2 on $F4_2(V_1,X_4,X_5,X_6,V_3,f)$ and in particular:

289. $0<|V_{21}|<|V_2|$

290. $n_2-m_2+1<n-m+1$ 289,287,266

291. $k_2<k$ 290,263,253

292. $P6(A,m,n)$ 271,8

293. $F6_2(A,m,n,f)=F6_2(A_2,F6_4(m,n,i_2,j_2,f),f)$ 272,273,292,275 14

294. $=F6_2(A_2,m_2,n_2,f)$ 293,285

295. $(\exists A,m,n)(A,m,n)=F6_2(A_2,m_2,n_2,f)$ 272,273,292,14

Let A_1^1,m_1^1,n_1^1 be such, so that:

296. $(A_1^1,m_1^1,n_1^1)=F6_2(A_2,m_2,n_2,f)$

297. $(\exists V_{11}^1,V_{21}^1,V_{31}^1)(\theta((V_{11}^1,V_{21}^1,V_{31}^1),(A',1,m_1^1-1,n_1^1,|V|)))$ 291,287,286,264

298. $(A',m',n')=(A_1^1,m_1^1,n_1^1)$ 267,294,296

299. $(\exists V_1^1,V_2^1,V_3^1)(\theta((V_1^1,V_2^1,V_3^1),(A',1,m'-1,n',|V|)))$ 297,298

- which proves the theorem in this case. Since it is true for $k\leq 0$ (262) then by induction it is true for all k.

Thus we have shown that any mapping, θ, with the property 3 turns the sets of the previous development into one-dimensional arrays (which contain no duplicate elements, since they are mapped from sets). If the assumptions on $F6_1$, P6, $F6_2$, $F6_3$, $F6_4$ are satisfied, then in the new system these functions of arrays model the functions $F2_1$, P3, $F3_2$, F4, F5 of the sets in such a way that the required properties hold in the new form. We can now continue with the development of $F6_3$ (F4 of section 6), towards a definition involving only operations available in the programming language.

10. Stage 7

In this stage we develop a function equivalent to $F6_3$. This function requires an arbitrary element of the middle set as a basis for comparisons. Since we know that the f th element of the current array is in the middle set, we use A[f] for this purpose, and give it to the function as an explicit argument. This will lead to the use of A[f] as a standard element for the construction of X_4 and X_6, containing elements lower and higher than A[f] respectively.

Assumptions

$F7 : D \times I^2 \times U \rightarrow D \times I^2$

1. $\delta(A,m,n) \;\&\; m<n \;\&\; m\leq x\leq n \;\&\; r=A[x] \;\&\; (A',i',j') = F7(A,m,n,r) \vdash \gamma_6(A,A',m,n) \;\&\; \delta(A',m,n) \;\&\; \omega_6(A',m,n,i',j')$

Assertion

2. $F6_3(A,m,n) = F7(A,m,n,A[f])$ satisfies 9.9.

Justification

The assertion follows from:-

3. $\delta(A,m,n) \;\&\; m<n \;\&\; m\leq f\leq n \;\&\; (A',i',j')=F7(A,m,n,A[f]) \vdash \gamma_6(A,A',m,n) \;\&\; \delta(A',m,n) \;\&\; \omega_6(A',m,n,i',j')$

Proof

immediate with x = f

11. Stage 8

The direction of development is now towards an iterative process for computing the F7 of the previous section, so as in section 3 we produce an inductive predicate β_8, and modify the specification accordingly.

Assumptions

$F8 : D \times I^2 \times U \rightarrow D \times I^2$

1. $\delta(A,m,n) \;\&\; m<n \;\&\; (A',i',j')=F8(A,m,n,r) \vdash$
   $\gamma_6(A,A',m,n) \;\&\; \delta(A',m,n) \;\&\; \beta_8(A',m,n,r,i',j') \;\&\; j'<i'$

where:-

2. $\beta_8(A,m,n,r,i,j) =$
   $(i=m \supset (j+1 \leq x \leq n \supset r <. A[x])) \;\&$
   $(j=n \supset (m \leq x \leq i-1 \supset (A[x] <. r)) \;\&$
   $m \leq i \;\&\; j \leq n \;\&\; i-2 \leq j \;\&$
   $(m \leq x < i \supset A[x] \leq. r) \;\&$
   $(j < x \leq n \supset r \leq. A[x])$

Assertion

3. $F7(A,m,n,r) = F8(A,m,n,r)$
   satisfies 10.1.

Justification

The assertion follows from:-

4. $\delta(A,m,n) \;\&\; m<n \;\&\; m \leq x \leq n \;\&\; r=A[x] \;\&$
   $(A',i',j')=F8(A,m,n,r) \vdash$
   $\gamma_6(A,A',m,n) \;\&\; \delta(A',m,n) \;\&\; \omega_6(A',m,n,i',j')$

Proof

5.	$\delta(A,m,n)$	Hyp
6.	$m < n$	Hyp
7.	$m \leq x \leq n$	Hyp
8.	$r = A[x]$	Hyp
9.	$(A',i',j') = F8(A,m,n,r)$	Hyp
10.	$\gamma_6(A,A',m,n)$	5,6,9,1
11.	$\delta(A',m,n)$	5,6,9,1
12.	$\beta_8(A',m,n,r,i',j')$	5,6,9,1
13.	$j' < i'$	5,6,9,1

suppose:-

14.	$i'-1 < m$	
15.	$i' = m$	14,12,2
16.	$j'+1 \leq x \leq n \supset r <. A[x]$	15,12,2

17.	$i' \leq x \leq n \supset r <. A[x]$	16,13
18.	$m \leq x \leq n \supset r <. A[x]$	17,15

but this contradicts 7,8,
thus:-

19.	$\neg(i'-1 < m)$	

similarly:-

20.	$\neg(n < j'+1)$	

suppose:-

21.	$j'+1 \leq m \ \& \ n \leq i'-1$	
22.	$m \leq i' \ \& \ j' \leq n$	12,2
23.	$i'-2 \leq j'$	12,2
24.	$n \leq m$	23,21

but this contradicts 6,
thus:-

25.	$m < j'+1 \vee i'-1 < n$	
26.	$m \leq x < i' \supset A'[x] \leq. r$	12,2
27.	$j' < x \leq n \supset r \leq. A'[x]$	12,2
28.	$m \leq i'-1 \ \& \ j'+1 \leq n$	19,20
29.	$i'-2 \leq j'$	2,12
30.	$m \leq j'+1 \ \& \ i'-1 \leq n$	28,29
31.	$m \leq x \leq j' \ \& \ j'+1 \leq y \leq i'-1 \supset A'[x] \leq. A'[y]$	13,26,27,30,1.2
32.	$j'+1 \leq x \leq i'-1 \ \& \ i' \leq y \leq n \supset A'[x] \leq. A'[y]$	13,26,27,30,1.2
33.	$m \leq x \leq j' \ \& \ i' \leq y \leq n \supset A'[x] \leq. A'[y]$	13,26,27,1.2
34.	$m-1 \leq j' \leq i'-1 \leq n$	30,13
35.	$\omega_6(A', m, n, i', j')$	34,19,20,25,31, 32,33,9.11b

which concludes the proof. 10,11,35

The justification, as in section 3, consists of showing that the revised specification for the function is as strong as the original.

12. Stage 9

We now consider the initialisation and iteration separately as in section 4. Here, however, the initialisation is explicit, setting i = m, j = n, so that it does not appear as another function. The specification on the function F9 now becomes the preservation of the truth of the inductive predicate β_8.

Assumptions

$F9 : D \times U \times I^2 \rightarrow D \times I^2$

1. $\delta(A,m,n) \;\&\; m<n \;\&\; \beta_8(A,m,n,r,i,j) \;\&\; (A',i',j') = F9(A,r,i,j) \vdash \gamma_6(A,A',m,n) \;\&\; \delta(A',m,n) \;\&\; \beta_8(A',m,n,r,i',j') \;\&\; j'<i'$

Assertion

2. $F8(A,m,n,r) = F9(A,r,m,n)$ satisfies 11.1.

Justification

The assertion follows from:-

3. $\delta(A,m,n) \;\&\; m<n \;\&\; (A',i',j') = F9(A,r,m,n) \vdash \gamma_6(A,A',m,n) \;\&\; \delta(A',m,n) \;\&\; \beta_8(A',m,n,r,i',j') \;\&\; j'<i'$

Proof

4.	$\delta(A,m,n)$	Hyp
5.	$m < n$	Hyp
6.	$(A',i',j') = F9(A,r,m,n)$	Hyp

the following statements are vacuously true:-

7.	$n+1 \leq x \leq n \supset r <. A[x]$	
8.	$m \leq x \leq m-1 \supset A[x] <. r$	
9.	$m \leq m$	
10.	$n \leq n$	
11.	$m-2 \leq n$	5
12.	$m \leq x < m \supset A[x] \leq. r$	
13.	$n < x \leq n \supset r \leq. A[x]$	
14.	$\beta_8(A,m,n,r,m,n)$	7-13,11.2
15.	$\gamma_6(A,A',m,n)$	4,5,14,6,1
16.	$\delta(A',m,n)$	4,5,14,6,1
17.	$\beta_8(A',m,n,r,i',j')$	4,5,14,6,1
18.	$j' < i'$	4,5,14,6,1

which concludes the proof 15,16,17,18

The justification shows that β_8 is true initially, hence if it is preserved by F9, then the additional conditions γ_6 and $j'<i'$ ensure that the conditions on F8 of the previous section are satisfied.

13. Stage 10

Here we develop the iterative computation of F9, using $F10_2$ to define the structure of the algorithm and $F10_1$ to carry the body of the iteration. The remarks at the beginning of section 5 apply here also.

Assumptions

$F10_1 : D \times U \times I^2 \rightarrow D \times I^2$

1. $\delta(A,m,n) \;\&\; \beta_8(A,m,n,r,i,j) \;\&\; i \leq j \;\&\; (A',i',j') = F10_1(A,r,i,j) \vdash \gamma_6(A,A',m,n) \;\&\; \delta(A',m,n) \;\&\; \beta_8(A',m,n,r,i',j') \;\&\; (i<i' \vee j'<j) \;\&\; i \leq i' \;\&\; j' \leq j$

$F10_2 : D \times U \times I^2 \rightarrow D \times I^2$

2. $j<i \vdash F10_2(A,r,i,j) = (A,i,j)$
3. $i \leq j \;\&\; (A',i',j') = F10_1(A,r,i,j) \vdash F10_2(A,r,i,j) = F10_2(A',r,i',j')$

Assertion

4. $F9(A,r,i,j) = F10_2(A,r,i,j)$ satisfies 12.1.

Justification

The assertion follows from:-

5. $\delta(A,m,n) \;\&\; m<n \;\&\; \beta_8(A,m,n,r,i,j) \;\&\; (A',i',j') = F10_2(A,r,i,j) \vdash \gamma_6(A,A',m,n) \;\&\; \delta(A',m,n) \;\&\; \beta_8(A',m,n,r,i',j') \;\&\; j'<i'$

Proof

6.	$\delta(A,m,n)$	Hyp
7.	$m < n$	Hyp
8.	$\beta_8(A,m,n,r,i,j)$	Hyp
9.	$(A',i',j') = F10_2(A,r,i,j)$	Hyp

Proceed by induction on j-i.
Basis, assume :-

10.	$j-i < 0$	
11.	$(A',i',j') = (A,i,j)$	10,9,2
12.	$\gamma_6(A,A',m,n)$	11,9.11a
13.	$\delta(A',m,n)$	6,11
14.	$\beta_8(A',m,n,r,i',j')$	8,11
15.	$j' < i'$	10,11
so 5 is true for $j-i<0$		12-15

Induction, suppose true for $0 \leq j-i < x$, show for $j-i = x$:-

16.	$i \leq j$	
	writing:-	
17.	$(A'',i'',j'') = F10_1(A,r,i,j)$	
18.	$\gamma_6(A,A'',m,n)$	6,8,16,17,1
19.	$\delta(A'',m,n)$	6,8,16,17,1
20.	$\beta_8(A'',m,n,r,i'',j'')$	6,8,16,17,1
21.	$(i<i'' \vee j''<j) \ \& \ i\leq i'' \ \& \ j''\leq j$	6,8,16,17,1
22.	$(A',i',j') = F10_2(A'',r,i'',j'')$	16,9,3,17
	since $j''-i'' < x$, from 21, we get by assumption:-	
23.	$\gamma_6(A,A',m,n)$	19,7,20,22,5
24.	$\delta(A',m,n)$	19,7,20,22,5
25.	$\beta_8(A',m,n,r,i',j')$	19,7,20,22,5
26.	$j' < i'$	19,7,20,22,5

which concludes the induction.

The justification consists of the inductive proof that if β_8 is preserved during the iteration, then the additional condition γ_6 becomes true when finally $j'<i'$. Note that the conditions $i\leq i'$ and $j'\leq j$ ensure that ultimately $j'<i'$, and the iteration terminates.

14. Stage 11

In this final stage, we develop an explicit definition of F11 by cases, using operations available in the programming language, that satisfies the specification of the last section for $F10_1$.

Assumption

F11 : D X U X I^2 → D X I^2

1. $\delta(A,m,n)$ & $\beta_8(A,m,n,r,i,j)$ & $i \leq j$ & $(A',i',j') = F11(A,r,i,j)$ ⊢
   [$(r \leq .A[i]$ & $A[j] \leq .r)$ ⊃ $((x \neq i$ & $x \neq j$ ⊃ $A'[x]=A[x])$ &
   $A'[i]=A[j]$ & $A'[j]=A[i]$ &
   $i'=i+1$ & $j'=j-1$)] &
   [$A[i] <.r$ ⊃ $(A'=A$ & $i'=i+1$ & $j'=j$)] &
   [$r<.A[i]$ ⊃ $(A'=A$ & $i'=i$ & $j'=j-1)$]

Assertion

2. $F10_1(A,r,i,j) = F11(A,r,i,j)$
   satisfies 13.1.

Justification

The assertion follows from:-

3. $\delta(A,m,n)$ & $\beta_8(A,m,n,r,i,j)$ & $i \leq j$ & $(A',i',j') = F11(A,r,i,j)$
   ⊢ $\gamma_6(A,A',m,n)$ & $\delta(A',m,n)$ & $\beta_8(A',m,n,r,i',j')$ &
   $(i<i' \vee j'<j)$ & $i \leq i'$ & $j' \leq j$

Proof

4.	$\delta(A,m,n)$	Hyp
5.	$\beta_8((A,m,n,r,i,j)$	Hyp
6.	$i \leq j$	Hyp
7.	$(A',i',j') = F11(A,r,i,j)$	Hyp
8.	$i=m$ ⊃ $(j+1 \leq x \leq n$ ⊃ $r <.A[x])$	5,11.2
9.	$j=n$ ⊃ $(m \leq x \leq i-1$ ⊃ $A[x]<.r)$	5,11.2
10.	$m \leq i$ & $j \leq n$ & $i-2 \leq j$	5,11.2
11.	$m \leq x < i$ ⊃ $A[x] \leq .r$	5,11.2
12.	$j < x \leq n$ ⊃ $r \leq .A[x]$	5,11.2

Consider the three cases of the definition 1 of F11, first:-

13.	$r \leq .A[i]$ & $A[j] \leq .r$	
14.	$x \neq i$ & $x \neq j$ ⊃ $A'[x]=A[x]$	4,5,6,7,13,1
15.	$A'[i]=A[j]$ & $A'[j]=A[i]$	4,5,6,7,13,1
16.	$i'=i+1$ & $j'=j-1$	4,5,6,7,13,1

the following two statements become (vacuously) true

17.	$i' = m$ ⊃ $(j'+1 \leq x \leq n$ ⊃ $r <.A'[x])$	10,16
18.	$j' = n$ ⊃ $(m \leq x \leq i'-1$ ⊃ $A'[x] <.r)$	10,16

19.	$m \leq i' \ \& \ j' \leq n$	10,16
20.	$i'-2 \leq j'$	6,16
21.	$m \leq x < i' \supset A'[x] \leq . r$	6,11,13,16,14,15
22.	$j' < x \leq n \supset r \leq . A'[x]$	6,12,13,16,14,15
23.	$\beta_8(A',m,n,r,i',j')$	17-22,11.2
24.	$\gamma_6(A,A',m,n)$	9.11a,10,14,15
25.	$\delta(A',m,n)$	4,10,14,15
26.	$i < i' \ \& \ j' < j$	16
which concludes this case.		24,25,23,26

Second case:-

27	$A[i] < . r$	
28.	$A' = A$	4,5,6,7,27,1
29.	$i' = i+1$	4,5,6,7,27,1
30.	$j' = j$	4,5,6,7,27,1

the following statement is (vacuously) true

31.	$i' = m \supset (j'+1 \leq x \leq n \supset r < . A'[x])$	10,29
32.	$j' = n \supset (m \leq x \leq i'-1 \supset A'[x] < . r)$	9,27,28
33.	$m \leq i' \ \& \ j' \leq n$	10,29,30
34.	$i'-2 \leq j'$	6,29,30
35.	$m \leq x < i' \supset A'[x] \leq . r$	11,27,28,29
36.	$j' < x \leq n \supset r \leq . A'[x]$	12,30,28
37.	$\beta_8(A',m,n,r,i',j')$	31-36,11.2
38.	$\gamma_6(A,A',m,n)$	9.11a,28
39.	$\delta(A',m,n)$	4,28
40.	$i < i' \ \& \ j' \leq j$	29,30
which concludes this case.		38,39,37,40

The final case is similar to 27-40 above.

At this point we have arrived at a statement of an algorithm which can be mapped directly into a high-level programming language. In the following two sections we summarise the algorithm as developed, and give, without further justification, the corresponding program in an ALGOL-like language.

15. Summary of Development

In this section we summarise (as in section 8) the development in preparation for translation into a program.

Assumptions

Suppose we have functions:-

$F11 : D \times U \times I^2 \to D \times I^2$

1. $\delta(A,m,n) \;\&\; \beta_8(A,m,n,r,i,j) \;\&\; i \le j \;\&\; (A',i',j') = F11(A,r,i,j) \vdash$
$[(r \le .A[i] \;\&\; A[j] \le .r) \supset ((x \ne i \;\&\; x \ne j \supset A'[x] = A[x]) \;\&\;$
$A'[i] = A[j] \;\&\; A'[j] = A[i] \;\&\;$
$i' = i+1 \;\&\; j' = j-1)] \;\&\;$
$[A[i] <. r \supset (A' = A \;\&\; i' = i+1 \;\&\; j' = j)] \;\&\;$
$[r <. A[i] \supset (A' = A \;\&\; i' = i \;\&\; j' = j-1)]$ 14.1

$F10_2 : D \times U \times I^2 \to D \times I^2$

2. $j < i \vdash F10_2(A,r,i,j) = (A,i,j)$ 13.2

3. $i \le j \;\&\; (A',i',j') = F11(A,r,i,j) \vdash$
$F10_2(A,r,i,j) = F10_2(A',r',i',j')$ 13.3, 14.2

$F6_0 : \beta(U) \to D$

4. $A = F6_0(V) \vdash \theta(V,A,1,|V|)$ 9.6

$F6_1 : D \to D \times I^2$

5. $\vdash F6;(A) = (A,1,|V|))$ 9.7

$P6 : D \times I^2 \to \{T,F\}$

6. $\vdash P6(A,m,n) \equiv m < n$ 9.8

$F6_4 : I^5 \to I^2$

7. $0 \le m-1 \le j \le i-1 \le n \le |V| \;\&\; \delta(A,m,n) \;\&\;$
$(m',n') = F6_4(m,n,i,j,f) \vdash$
$(f \le j \supset m' = m \;\&\; n' = j) \;\&\;$
$(i-1 < f \supset m' = i \;\&\; n' = n) \;\&\;$
$(j < f \le i-1 \supset m' = j+1 \;\&\; n' = i-1)$ 9.12

$F6_2 : D \times I^3 \to D \times I^2$

8. $0 \le m-1 \le n \le |V| \;\&\; m < n \;\&\; m \le f \le n \;\&\; \delta(A,m,n) \;\&\;$
$\neg P6(A,m,n) \vdash F6_2(A,m,n,f) = (A,m,n)$ 9.13

9. $0 \le m-1 \le n \le |V| \;\&\; m < n \;\&\; m \le f \le n \;\&\; \delta(A,m,n) \;\&\;$
$P6(A,m,n) \;\&\; (A',i',j') = F10_2(A,A[f],m,n) \vdash$
$F6_2(A,m,n,f) = F6_2(A',F6_4(m,n,i',j',f),f)$
9.14, 10.2, 11.3, 12.2, 13.4

$F6_5 : D \times I^2 \to \beta(U)^3$

10. $0 \le m-1 \le n \le |V| \;\&\; \delta(A,1,m-1) \;\&\; \delta(A,m,n) \;\&\;$
$\delta(A,n+1,|V|) \;\&\; (V_1',V_2',V_3') = F6_5(A,m,n) \vdash$
$\theta((V_1',V_2',V_3'),(A,1,m-1,n,|V|))$ 9.15

Assertion

11. $FIND(V,f) = F6_5(F6_2(F6_1(F6_0(V)),f))$

Justification

Putting:-
12. $F10_1(A,r,i,j) = F11(A,r,i,j)$

we have:-
13. $F10_1(A,r,i,j)$ satisfies 13.1 — 14.2,1

Putting:-
14. $F9(A,r,i,j) = F10_2(A,r,i,j)$

we have:-
15. $F9(A,r,i,j)$ satisfies 12.1 — 13.4,2,3,12,13

Putting:-
16. $F8(A,m,n,r) = F9(A,r,m,n)$
17. $= F10_2(A,r,m,n)$ — 16,14

we have:-
18. $F8(A,m,n,r)$ satisfies 11.1 — 12.2,15

Putting:-
19. $F7(A,m,n,r) = F8(A,m,n,r)$
20. $= F10_2(A,r,m,n)$ — 19,17

we have:-
21. $F7(A,m,n,r)$ satisfies 10.1 — 11.3,18

Putting:-
22. $F6_3(A,m,n) = F7(A,m,n,A[f])$
23. $= F10_2(A,A[f],m,n)$ — 22,20

we have:-
24. $F6_3(A,m,n)$ satisfies 9.9 — 10.2,21

Now:-
25. $FIND(V,f) = F3_2(F2_1(V),f)$ satisfies 2.1 — 8.14,8.2

Thus the assumptions of section 9 are satisfied (or re-assumed above) as follows. 9.6 is 4, 9.7 is 5, 9.8 is 6, 9.9 is 24, 9.12 is 7, 9.13 is 8, 9.15 is 10. For the remaining assumption 9.14 we have:

26. $0 \le m-1 \le n \le |V|$ & $m > n$ & $m \le f \le n$ & $\delta(A,m,n)$ &
$P6(A,m,n)$ & $(A',i',j') = F6_3(A,m,n) \vdash$
$F6_2(A,m,n,f) = F6_2(A', F6_4(m,n,i',j',f),f)$ 9,23

Thus all the mappings of section 9 are valid, and we may map the right-hand side of 24 as follows:

27.	$V \rightarrow F6_0(V)$	9.6
28.	$F2_1(V) \rightarrow F6_1(F6_0(V))$	27,9.33-35
29.	$F3_2(F2_1(V),f) \rightarrow F6_2(F6_1(F6_0(V)),f)$	28,9.251-252
30.	$\rightarrow F6_5(F6_2(F6_1(F6_0(V)),f))$	29,9.15

and the assertion follows from 30 and 25.

16. The Program

In this section we show a program in an ALGOL-like language, corresponding to the functional expansion of FIND summarised in the previous section. No formal justification of this stage is given. To provide it, formal statements of properties of the particular constructs of the language, as used in the program, would be required. Such properties might for instance be deduced from a formal definition of the language.

Notes on the Statements.

3 element must be a declaration appropriate to the elements of A.
7 set must be a declaration appropriate to the form of V passed to the program.
9-11 are the realization of $F6_1$ according to 9.7.
19-30 are the realization of F11 according to 14.1.
17-31 are the realization of $F10_2$ according to 15.30, 15.31.
13-31 are the realization of $F6_3$ according to 15.20.
31-38 are the realization of $F6_4$ according to 9.12.
12 tests P6 according to 9.8.
12-39 are the realization of $F6_2$ according to 15.28, 15.29.
Hence the program realizes FIND according to 15.8,9,10.

Note that we have not written the input routine, which sets up A from V in whatever form it was passed, nor the output routine to produce the sets V_1, V_2, V_3, in whatever form they are required. However, the formal development process has automatically given a complete formal specification of the interfaces between these routines and the program. Also, depending on the type of the array elements, the operators $\leq.$ and $<.$ in lines 19, 27, 29 may need a sub-program (in or out of line) to realise them.

```
1     procedure FIND(V,f) ;
2     integer f,m,n,i,j;
3     element temp,r;
4     element array A;
5     array procedure INPUT(V);
          comment returns an array A such that θ(V,A,1,|V|);
      ...
6     sets procedure OUTPUT(A,1,m,n,|V|);
          comment returns three sets V1,V2,V3 such that
              θ((V1,V2,V3),(A,1,m,n,|V|));
      ...
7     set V;
8     begin
9     A := INPUT(V);
10    m:= 1; n:=|V|;
12    while m<n do
13         begin
14         r:= A[ f];
15         i:= m; j:=n;
17         while i≤j do
18              begin
19              if r ≤.A[ i] & A[ j] ≤.r then
20                   begin
21                   temp := A[ i];
22                   A[ i] := A[ j];
23                   A[ j] := temp;
24                   i := i + 1;
25                   j := j - 1
26                   end
27              else if A[ i] <.r then i := i+1
29              else if r<.A[ j] then j :=j-1
31              end
32         if f≤j then n := j
33         else if i-1<f then m := i
34         else if j<f≤i-1 then
35              begin
36              m:= j+1;
37              n:= i-1
38              end
39         end;
40         FIND := OUTPUT(A,1,m,n,|V|)
41    end
```

Acknowledgements

The authors would like to acknowledge many useful discussions with D. Chapman on the material presented here.

References

1. E. W. Dijkstra.
"Notes on Structured Programming". Report EWD 249, August 1969.

2. E. W. Dijkstra.
"A Short Introduction to the Art of Programming". Report EWD 316, August 1971.

3. C. A. R. Hoare.
"Proof of a Program: FIND". Comm. ACM, vol. 14, no. 1, January 1971.

4. C. B. Jones.
"Formal Development of Correct Algorithms: an Example Based on Early's Recogniser". ACM Sigplan Conference on "Proofs of Assertions About Programs", January 1972.

5. J. McCarthy.
"Recursive Functions of Symbolic Expressions and Their Computation by Machine". Comm. ACM, vol. 3, no. 4, 1960.

6. R. J. Waldinger.
"Constructing Programs Automatically Using Theorem Proving". Ph.D. Thesis, Carnegie - Mellon University.