

Software Inspections We Can Trust

David Lorge Parnas, P.Eng.

NSERC/Bell Industrial Research Chair in Software Engineering
Director of the Software Engineering Programme
Department Of Computing And Software, Faculty of Engineering,
McMaster University Hamilton ON Canada L8S 4K1

Software is devilishly hard to inspect. Serious errors can hide for years. Consequently, many are hesitant to employ software in safety-critical applications and all companies are finding correcting and improving software to be an increasingly burdensome cost.

This talk describes a procedure for inspecting software that consistently finds subtle errors in software that is believed to be correct. The procedure is based on four key principles:

- All software reviewers **actively** use the code.
- Reviewers **exploit the hierarchical structure of the code** rather than proceeding sequentially through the code.
- Reviewers **focus on small sections of code, producing precise summaries** that are used when inspecting other sections. The summaries provide the “links” between the sections.
- Reviewers **proceed systematically** so that no case, and no section of the program, gets overlooked.

During the procedure, the inspectors produce and review mathematical documentation. The mathematics allows them to check for complete coverage; the notation allows the work to proceed in small systematic steps.

Responsibilities of (Software) Engineers

- To understand the properties of their products thoroughly.
- To follow established rules of good practice when designing and building products.
- To apply theory where it has been demonstrated to lead to better, or safer, products.

Engineering is Not Management

The art of system management is the ability to get things built without knowing exactly what they are.

The engineer must thoroughly understand the properties of the product.

Software projects are hard to manage - especially if they are badly designed, but...

Unless we have good Engineers, the best managers will not be able to successfully manage these projects.

Inspections have to be carefully managed but executed by Engineers.

When is Software Critical?

“Critical” is not necessarily “safety critical”

Other types of critical programs:

- Mass distributed programs in warranty situations
- Critical kernels in many systems
- Financial Systems
- Security (Privacy, Data Protection) programs
- any system where a failure may lead to a lawsuit.

The common property of all of these examples is that the cost of a failure is high.

If you value your reputation, your work may be critical.

The Critical-Software Tripod

- (1) Precise, well organised, mathematical documentation with systematic review
- (2) Extensive Testing
 - Systematic Testing-quick discovery of gross errors
 - Random Testing -discovery of shared oversights and reliability assessment
- (3) Qualified People and Approved Processes

The Three Legs are complementary

The three legs are all needed.

The stool falls over if any leg is forgotten.

The third leg is the shortest.

It's the shortest leg that we should worry about.

Today we discuss only leg (1).

Why Conventional Reviews are Ineffective

- (1) The reviewers are swamped with information.
- (2) Most reviewers are not familiar with the product design goals.
- (3) There are no clear individual responsibilities.
- (4) Reviewers can avoid potential embarrassment by saying nothing.
- (5) The review is conducted as a large meeting where detailed discussions are difficult.
- (6) Presence of managers silences criticism.
- (7) Presence of uninformed reviewers may turn the review into a tutorial.
- (8) Specialists are asked general questions.
- (9) Generalists are expected to know specifics.
- (10) The review procedure reviews code without respect to structure.
(n lines per hour)
- (11) Unstated assumptions are not questioned.

Effective Reviews are Active Reviews

A dilemma:

- Errors in programs and design documents should be found *before* the documents/systems are used.
- Errors in programs and documents are usually found *when* the documents are used.

Another dilemma:

- Everyone's work requires review!
- It's easier to say "OK" than to find subtle errors!
- Reviewer's approval is not reviewed.

One more dilemma:

- No individual can review all aspects of a design.
- When working in a group, people tend to relax in the knowledge that others are also working the problem.

Solutions:

- Make the reviewers use the documents.
- Make the reviewers document their analysis.
- Have specialised reviews. Ask the reviewer about things that they know.
- Make the reviewers provide specifics - not just a bit.

Previous Work on Inspections

Best known approach Fagan - 1976.

Many followers - new book by Gilb.

Explicitly focus on the management aspects.

- Who should be there?
- What are the roles of the participants?
- How long is a meeting?
- How fast do you work?
- Forms for reporting errors?

Read the code in sequence and paraphrase.

Paraphrases are informal.

Most observers find these more effective than conventional reviews or walk-throughs, but...

... can we do better?

Parnas/NRL/AECB/AECL/Ontario Hydro

Focus on the engineering side.

Depend on hierarchical decomposition rather than sequential reading.

Use mathematical notations to provide precise descriptions rather than informal paraphrases.

Produce useful *precise* documentation as a side effect.

Proceed much more quickly if the documentation was produced by the developers.

Insures that cases and variables are not overlooked.

Applies simple mathematics to check for completeness aspects.

Active Review of Design Documents

Base the review process on the nature of the document.

(1) Begin by identifying desired properties.

(2) Prepare questionnaires for the reviewers. Ask them questions that:

- make them use the document.
- make them demonstrate that the desired properties are present.
- ask for sources of information to support the answers to other questions.

For example:

- Ask reviewers to identify the domain of the program
- Ask reviewers to identify “error” cases.
- Ask reviewers to explain why no other error cases are possible.
- Ask reviewers to explain why the behaviour required for each case is the desired behaviour.

For more information read [1].

▪ **McMaster University** ▪
Inspecting Programs

It is the code that “hits the road”.

Getting the requirements right, the structure right, the interfaces right, the documentation right, etc. are all important but *we have to check the code.*

The same review principles apply, viz:

- Make the reviewers use the material they review.
- Make the reviewers answer questions.
- Ask the reviewer about things that they know.
- Make the reviewers provide specifics.

We compare completed programs with previously reviewed specifications.

We ask some reviewers to produce precise descriptions.

We ask other reviewers to show that the descriptions match the specifications.

It is hard work but it produces results.

- We get good documentation for future use.
- We find errors in the best industrial code - programs that were considered correct.

Our Code Inspection Process

- (1) Prepare a precise specification of what the code should do - a program function table.
- (2) Decompose the program into small parts appropriate for the “display approach” [2].
- (3) Produce the specifications required for the “display approach”.
- (4) Compare the “top level” display description with the requirement specification.

Observations:

- You can't inspect without precise requirements.
- Step (2) would already have been done if you use the display method for documentation.
- Step (3) is truly an active design review
- All reviewer work is itself reviewable.
- If you did not already have it, the by-product is thorough documentation.
- It's a bunch of small steps and very systematic.

Descriptions vs. Specifications

An actual description is a statement of some actual attributes of a product, or set of products.

A specification is a statement of all properties required of a product, or a set of products.

In the sequel, “description”, without modifier, means “actual description”.

The following are implications of these definitions:

- A description may include attributes that are not required.
- A specification may include attributes that a (faulty) product does not possess.
- The statement that a product satisfies a given specification may constitute a description.

The third fact results in much confusion. A useful distinction has been lost.

Do We Need *New* Semantics Theories For Programming?

Not for the practical software engineering problems that I see.

I can find 30 year old theory that works for the problems that I will describe today.

Semantic theory has failed to describe real languages, but (in my opinion) the fault lies with the languages.

We do need improvements in:

- the notation used to describe actual programs.
- the ability to describe behaviour in terms of the values of observable variables - nothing else.
- convenient ways to deal with all aspects of termination including non-deterministic non-termination.

What follows is mathematically equivalent to some **very old** ideas, but has some practical advantages.

A Mathematical Interlude - LD-relations.

A *binary relation* R on a given set U is a set of ordered pairs with both elements from U ,
i.e. $R \subseteq U \times U$.

The set U is called the *Universe of R* .

The set of pairs R can be described by its *characteristic predicate*, $R(p,q)$,
i.e. $R = \{(p,q): U \times U \mid R(p,q)\}$.

The *domain* of R is denoted $\text{Dom}(R)$ and is $\{p \mid \exists q [R(p,q)]\}$.

The *range* of R is denoted $\text{Range}(R)$ and is
 $\{q \mid \exists p [R(p,q)]\}$.

Below, “relation” means “binary relation”.

A *limited-domain relation* (LD-relation) on a set, U , is a pair, $L = (R_L, C_L)$
where:

R_L , the *relational component* of L , is a relation on U , i.e. $R_L \subseteq U \times U$, and
 C_L , the *competence set* of L , is a subset of the domain of R_L , i.e. $C_L \subseteq \text{Dom}(R_L)$.

Using LD-Relations as Before/After Behavioural Descriptions (1)

Let P be a program, let S be a set of states, and let $L_P = (R_P, C_P)$ be an LD-relation on S such that

$(x, y) \in R_P$ if and only if $\langle x, \dots, y \rangle$ is a possible terminating execution of P , and

$x \in C_P$ if and only if P is guaranteed to terminate if it is started in state s .¹

L_P is called the *LD-relation of P*

By convention, if C_P is not given, it is,
(by default), $\text{Dom}(R_P)$.

With this convention, our approach is upwards compatible with the “cleanroom” approach for dealing with deterministic programs.

¹ Please note that C_P is not the same as the precondition used in VDM [4]. S_P is the set of states in which the termination of P is certain.

Using LD-Relations as Before/After Behavioural Descriptions (2)

The following follow from the definitions:

- If P starts in x and $x \in C_P$, P always terminates; if $(x, y) \in R_P$, P may terminate in y .
- If P starts in x , and $x \in (\text{Dom}(R_P) - C_P)$, the termination of P is non-deterministic; in this case, if $(x, y) \in R_P$, when P is started in x , it may terminate in y or may not terminate.
- If P starts in x , and $x \notin \text{Dom}(R_P)$, then P will never terminate.

By these conventions we are able to provide complete before/after descriptions of any program but retain a simpler representation to use for those cases that arise most often.

Specifying Programs (1)

Specifications may *allow* behaviour not actually exhibited by a satisfactory program.

We can also use LD-relations as before/after specifications. To understand the meaning of a specification, you must understand what “satisfies” means.

Let $L_P = (R_P, C_P)$ be the description of program P.

Let S , called a *specification*, be a set of LD-relations on the same universe and

$L_S = (R_S, C_S)$ be an element of S .

We say that

(1) P *satisfies an LD-relation L_S , if and only if*
 $C_S \subseteq C_P$ and $R_P \subseteq R_S$, and

(2) P *satisfies a specification, S , if and only if*
 L_P satisfies at least one element of S .

Often, S has only one element. If $S = \{L_S\}$ is a specification, then we can also call L_S a specification.

Specifying Programs (2)

The following follow from the definitions:

- A program will satisfy its own description as well as infinitely many other LD-relations.
- An acceptable program must not terminate when started in states outside $\text{Dom}(R_S)$.
- An acceptable program must terminate when started in states in C_S ($C_S \subseteq \text{Dom}(R_P)$).
- An acceptable program may only terminate in states that are in $\text{Range}(R_S)$.
- A deterministic program can satisfy a specification that would also be satisfied by a non-deterministic program.

Note the following differences between the description and the specification of a program.

- There is only one LD-relation describing a program, but that program will satisfy many distinct specifications described by different LD-relations.
- An acceptable program need not exhibit all of the behaviours allowed by R_S ($R_P \subseteq R_S$).
- An acceptable program may be certain to terminate in states outside C_S . ($C_S \subseteq C_P$).

The intended use of each LD-relation (specification or description) must be stated explicitly!

Tabular Descriptions and Specifications

Specification for a search program

$(\exists i, B[i] = x)$	$(\forall i, ((1 \leq i \leq N) \Rightarrow B[i] \neq x))$
-------------------------	--

j'	B[j'] = x	<u>true</u>	$\wedge NC(x, B)$
present' =	true	false	

Description of a search program

$(\exists i, B[i] = x)$	$(\forall i, ((1 \leq i \leq N) \Rightarrow B[i] \neq x))$
-------------------------	--

j'	$(B[j'] = x) \wedge$ $(\forall i, ((j' < i \leq N)$ $\Rightarrow B[i] \neq x))$	<u>true</u>	$\wedge NC(x, B)$
present' =	true	false	

The above is one of many kinds of tables!

Simple tables like this understate the advantage.

These have proven “practitioner appeal”

Formal methods discussions emphasise program development.

A successful program will have more readers than writers, because it will be maintained for many years.

The needs of reviewers and maintainers, are as important as the needs of program designers.

Programs should be presented in a way suitable for review and maintenance.

Proper decomposition into modules will reduce the complexity and length of programs.

But, some may still be quite long.

We present a documentation method for non-trivial, long, well-structured programs.

The limits of human comprehension

Human beings cannot easily understand long programs.

Studying a long program, we mentally decompose it.

We provisionally, assign a function to each part.

We try to convince ourselves that, if each part implements its assigned function, the whole program is correct.

We then try to confirm our starting hypothesis, anditerate until exhausted!

Reviewer should not have to guess a program's structure.

Program should be presented as a collection of small parts.

Function of each part should be precisely stated.

It should be possible to review those small parts separately.

Reviewer's responsibility is checking small fragments.

The concept of displays

Designers to present a program as a set of displays.

Well-structured program: short text invoking other programs.

All programs can be short;

A *display* presents a program so that its correctness can be examined in isolation from other displays.

A display consists of three parts:

- (1) A description of what the program should do.
- (2) the program itself.
- (3) descriptions of subprograms invoked by this program.

A set of displays will be considered *complete* if, for each description of a non-standard subprogram found in part (3), there exists a display in which this specification forms part (1).

Completeness, in this sense, can easily be checked mechanically.

Verification of the correctness of a set of displays is reduced to a set of smaller tasks

Why use The Functional Approach

The display method is independent of the specification technique.

The display method is independent of programming language.

It works best with the functional approach.

[e.g. H.D. Mills, N.G. de Bruijn, Majster-Cederbaum,].

Functional Approaches “scale up” because there are no special primitive programs.

It can be applied even if the names represent huge programs.

Isn't Stepwise refinement enough?

Stepwise refinement leads to long programs [Wirth example].

Stepwise refinement leads to repetitive programs.

Displays with functional specifications avoid these pitfalls.

NEVER write a long program!

Hierarchical control structure in programs

Program: text describing sequence of state transitions in a computer.

“Structured Programming” constructs have three very useful properties:

- (1) programs constructed using them can be decomposed into a hierarchy of parts (with lower level parts completely contained in an upper level part) using simple parsers; those parsers need not even distinguish one identifier from another,
- (2) the semantics of the total program can be determined from the semantics of its parts, using simple operations (cf. e.g. [14, 15]).
- (3) semantics can be determined in a simple order: inner parts first.

The above properties make it easier to study a long structured program can be understood.

The Display Method is intended to be used for programs that have these properties.

Use of data abstractions

The best structured program will be difficult to explain and understand if it is presented in terms of complex data structures.

Data structures should be hidden by the introduction of *abstract data types*

Precise program documentation is not possible unless the abstract data type interfaces are precisely documented.

Our examples have been selected so that they can be understood without an understanding of module specifications.

(**integer** array H[1:N];

(**integer** c; **integer** n; n \leftarrow 1;

it (n \leq N \rightarrow

(


(**integer** u; **integer** l; **boolean** p; l \leftarrow 1; c \leftarrow 0;


it (u \leftarrow l + n - 1;


(u \leq N \rightarrow (

(**integer** i; i \leftarrow 0; p \leftarrow **true**;

it (i < $\lfloor (u - l + 1) \div 2 \rfloor \rightarrow$


(A[l+i] = A[u-i] \rightarrow (i \leftarrow i + 1; 


| A[l+i] \neq A[u-i] \rightarrow (p \leftarrow **false**; 

| $\lfloor (u - l + 1) \div 2 \rfloor \leq i \rightarrow$ 

ti)

;

(\neg p \rightarrow **skip** | p \rightarrow c \leftarrow c + 1; l \leftarrow l + 1; 

| u > N \rightarrow 

ti)

;

H[n] \leftarrow c; n \leftarrow n + 1; 

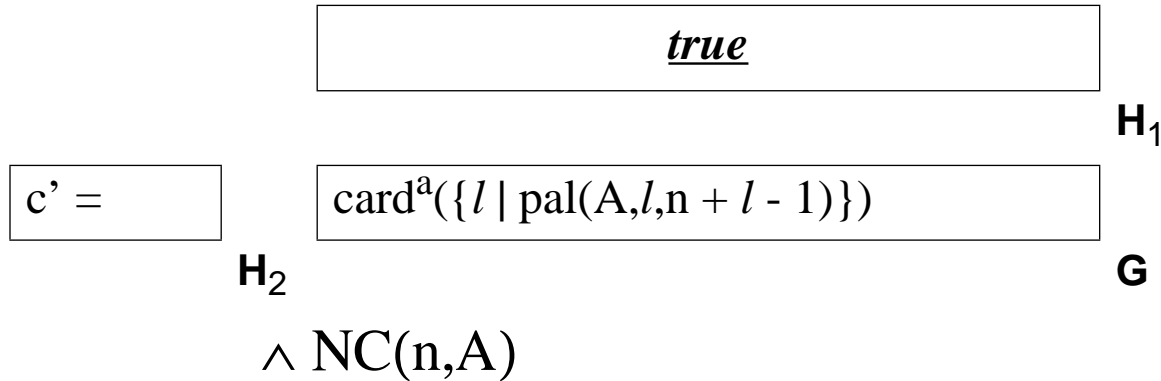
| n > N \rightarrow 

ti)

)

▪ **McMaster University** ▪
Display: An Example

Problem: $ctpal \equiv$



a. $\text{card}(x)$, where x is a set, is the number of elements in x .

Solution: $ctpal \equiv$

(integer u, l ; **boolean** p ; $l \leftarrow 1$; $c \leftarrow 0$;
it ($u \leftarrow l + n - 1$;
($u \leq N \rightarrow (\text{pal}u; (\neg p \rightarrow \text{skip} \mid p \rightarrow c \leftarrow c + 1)$;
 $l \leftarrow l + 1$;))
 $\mid u > N \rightarrow \bullet$))
ti)

$\text{pal}u \equiv: \text{NC}(l, u, A) \wedge (p' = \text{pal}(A, l, u))$

where

$\text{pal}(A, b, c) \equiv ((1 \leq b \leq c \leq N) \wedge$
 $(\forall i, 0 \leq i < \lfloor (c - b + 1) \div 2 \rfloor \Rightarrow A[b + i] = A[c - i]))$

Displays: An Explanation

The top part of each display is the specification for the program in the middle.

The program in the middle is kept small by removing sections, creating a display for them, and including their specification in the bottom part.

The bottom part contains a specification of these invoked programs.

To check a display determine the description of the program in the middle, and see if it satisfies the specification at the top. In doing this, use the specifications of the invoked programs, not their text.

To check a set of displays, make sure that every specification at the bottom of one display is at the top of another. The exceptions:

- standard programs
- primitive programs

Completeness can be checked mechanically.

Tabular Description of Sample Code

Table 1

	' OKTT = .FALSE.	(' OKTT = .TRUE.) AND NOT !NoSensTrip!	(' OKTT = .TRUE.) AND . !NoSensTrip!
B(' PTB , DOW1 ')	B(' PTB , DOW1 .OR. '#TMASK(' PTB)#)	Table 4	B(' PTB , DOW1 .OR. '#TMASK(' PTB)#)
B('#CN#, DOW2 ')	B('#CN#, DOW2 ')	Table 4	B('#CN#, DOW2 ')
B('#CND#, DOW2 ')	B('#CND#, DOW2 ')	Table 4	B('#CND#, DOW2 ')
EX '	' EX .OR. ' MASK	' EX .OR. ' MASK	' EX .OR. ' MASK
HI1 '	' HI1	'//HTL(5)// - ' HYS	'//HTL(5)// - ' HYS
HI2 '	' HI2	'//HTL(5)//	'//THL(5)//
LO1 '	' LO1	'//LTL(5)//	'//LTL(5)//
LO2 '	' LO2	'//LTL(5)// = ' HYS	'//LTL(5)// + ' HYS
MC '	' MC	Table 4	0
PC '	' PC	Table 4	0
B(j, STBV '), j = ' STB + j-1, i in {1...5}	B(j,' STBV)	Table 3	Table 3
B(j, STBV), NOT (j in {' STB + i-1}, i in {1...5})	B(j,(' STBV AND. ' UM))	B(j,(' STW .AND. ' UM))	
B(' STB + i-1, STW '), i in {1...5}	B(' STB + i-1, (STW .OR. ' UM))	Table 3	Table 3
B(j, STW '), NOT (j in {' STB + i-1},	B(i,(' STW .OR. ' UM))	B(i, STW)	B(i, STW)
B(' TIB , TIW ')	B(' TIB ,(' TIW .OR. '#TMASK(' TIB)#)	B(' TIB ,(' TIW .AND. '#FMASK(' TIB)#)	B(' TIB ,(' TIW .AND. '#FMASK(' TIB)#)
HIF(1...5) '	' HIF(1...5)	Table 2	Table 2
I '	' I	6	6
LOF(1...5) '	' LOF(1...5)	Table 2	Table 2

Table 2

	!AbvHiHys(i)!	!InHiHys(i)!	!InNorm(i)!	!InLoHys(i)!	!BlwLoHys(i)!
HIF(i) '	.FALSE.	' HIF(i)	.TRUE.	.TRUE.	.TRUE.
LOF(i) '	.TRUE.	.TRUE.	.TRUE.	' LOF(i)	.FALSE.

Table 3

	NOT !SensTrip(i)!	!SensTrip(i)!
B(j, STBV ')	B(j,(' STW .OR. '#TMASK(j)# .AND. ' UM))	B(j,(' STW .AND. '#FMASK(j)# .AND. ' UM))
B(' STB + i-1, STW ')	B(' STB + i-1,(' STW .OR. '#TMASK(' STB + i-1)#))	B(' STB + i-1,(' STW .AND. '#FMASK(' STB + i-1)#))

Table 4

Modes:

$$A^* = [('||MC|| \quad '|DEL|) \quad \text{OR} \quad ('||MC|| < 0) \quad \text{OR} \\ ('||PC|| + 1 \quad '|PCL|) \quad \text{OR} \quad ('||PC|| + 1 < 0)]$$

A

NOT *A*

PC '	' PCL	' PC + 1
MC '	' DEL	' MC
B(' PTB , DOW1 ')	B(' PTB ,(' DOW1 .AND. '#FMASK(' PTB #))	B(' PTB , DOW1
B('#CN#, DOW2 ')	B('#CN#,(' DOW2 .AND. '#FMASK('#CN#)#))	B('#CN#, DOW2
B('#CND#, DOW2 ')	B('#CND#,(' DOW2 .AND. '#FMASK('#CND#)#))	B('#CND#, DOW2

Structure and Inspection

Well-structured programs are easier to decompose. They can be decomposed by purely syntactic means.

Well-structured programs are much easier to inspect.

Inspection encourages good structuring.

Inspection suggests structural improvements.

Inspected programs are easier to maintain.

Modified programs need not be completely re-inspected. The parts that must be inspected again can be easily identified.

The cost of future maintenance is greatly reduced.

The definition of “well-structured” should not be based on the absence or presence of certain control structures. It has to do with the ease of decomposition. [2]

Our Initial Experience: Darlington Nuclear Power Generating Station¹

Three control systems in Canadian reactors:

- one normal control system
- two independent shutdown systems

Safety analysis *assumes* control system will fail. Only shutdown systems are considered safety-critical.

Previous shutdown systems were analogue and relay systems.

At Darlington they are software controlled.

Each Software System has a simple task.

Their designs are “diverse”.

The systems are more complex than their predecessors with the result that AECB² could not be confident of their trustworthiness.

How can we increase that level of confidence?

¹ Discussed in more detail in [4] and [3].

² Atomic Energy Control Board of Canada

Why We Could Not Use English

The following type of sentence was found in the requirements document.

“Shut off the pumps if the water level is above 100 meters for 4 seconds”

What does this simple sentence mean?

Three Reasonable Interpretations:

“Shut off the pumps if the mean water level over the past 4 seconds was above 100 meters”.

$$\left[\left(\int_{T-4}^T WL(t) dt \right) \div 4 > 100 \right]$$

“Shut off the pumps if the median water level over the past 4 seconds was above 100 meters”.

$$\left(\text{MAX}_{[t-4,t]} (WL(t)) + \text{MIN}_{[t-4,t]} (WL(t)) \right) \div 2 > 100$$

“Shut off the pumps if the “rms” water level over the past 4 seconds was above 100 meters”.

$$\sqrt{\left(\int_{T-4}^T WL^2(t) dt \right) \div 4} > 100$$

A Fourth (Unreasonable) Interpretation:

“Shut off pumps if the minimum water level over the past 4 seconds was above 100 meters”.

$$\text{MIN}_{[T-4, T]} [\text{WL}(t)] > 100$$

This is the most literal interpretation!

It is a disaster waiting to happen!

- If you use natural languages, there are thousands of such phrases waiting to “bug” you.

The Inspection Process at Darlington

Four teams:

- (1) Application Experts
- (2) Programming Experts
- (3) Verifiers
- (4) Auditors

Roles of the teams:

- (1) Produces requirements tables.
- (2) Produce Program Function Tables (Displays).
- (3) Show (1) = (2) and that (2) are correct.
- (4) Audit the “proofs”.

Subsequent Experience

In classes on this method, we have applied this to numerous small industrial programs that were believed to be correct.

In most cases, we found unexpected errors.

In some cases, the participants could not state the requirements.

In other cases, the program could not be decomposed (machine code w/o documentation).

I believe that one program was correct.

In all cases, we could improve the program.

We have found errors in textbook programs, library programs, and well-used and tested programs.

No process is perfect, but this one engenders confidence. It produces code that people trust.

What Makes Things Hard?

Variables with no names.

Variables with long names or characterising expressions.

Quantification over indices rather than elements.

Programs that are not understood.

Programs that are badly modularised.

Self-referencing data structures

These can all be fixed!

Essential Point: Divide and Conquer

The initial decomposition is essential. Attempts to simply scrutinise the program fail.

Trying to read the program the way a computer would is much less effective. Logically connected parts may be far apart.

The use of tables is essential. It breaks things down into simple cases so that

- We can be sure that all cases are covered.
- Each case is straightforward

We consider all variables, but one at a time.

We consider all cases, one at a time.

We can take “breaks”, go home and sleep, even take holidays, without losing our place.

Using displays and tabular summaries is far more work than Fagan’s English paraphrasing, but it imposes a discipline that helps.

The Other Essential Point: Precise, Abstract Descriptions

Having lots of little parts is not enough.

We have to be sure that the parts fit together.

We have to be able to do that without page-flipping.

Each part's behaviour must be precisely summarised without giving intermediate states.

We must be sure that the description at the bottom of one display will be identical with that at the top of another display.

These global checks can, and have been, mechanised.

- Precise descriptions are painstaking work, but if quality is important, they are essential.

It's not always easy!

The most critical step, besides decomposition, is finding a good representation for the state space.

It is not always worthwhile.

There are informal variations.

It is a capability that your organisation should have.

Displays

A *display* is a document that consists of the following three parts:

- P1: a specification for the program presented in this display,
- P2: the program itself, in which names of other programs may appear; we will call these named programs *subprograms* and say that they are *invoked* by this program,
- P3: specifications of all non-standard subprograms invoked in P2.

A *standard* subprogram is the one that does not require a specification.

If an invoked subprogram is not standard, its specification appears as P1 in another display.

A name in P2 may represent either a procedure call or a macro.

To avoid repetition of information on more than one display, we write it in a *lexicon*.

Completeness and Correctness

A display is said to be *correct* if program P2 satisfies specification P1 whenever the subprograms invoked in P2 satisfy the corresponding specifications in P3.

A *set of displays* (for a given program) *is complete*, if for each specification of a non-standard subprogram found in P3, of a display, there is a display where that specification is P1.

A *program* (presented as a set of displays) *is correct* if this set of displays is complete and each of the displays from this set is correct.

If R is a relation, then:

- “ R ” denotes the set of ordered pairs that constitutes this relation,
- “ $R(x,y)$ ” denotes the characteristic predicate of the set R .

Let P be described by an LD-relation $L = (R, C)$.

Let and let v_1, \dots, v_k be program variables in P which form its data structure, $v = (v_1, \dots, v_k)$. Then:

- “ v_i ” (to be read “ v_i *before*”) denotes the value of the programming variable v_i before an execution of P ,
- “ v_i' ” (to be read “ v_i *after*”) denotes the value of the variable v_i after a terminating execution of P .

Each pair in R will be of the form (v, v') .

We often write “ $R(.)$ ” as an abbreviation of $R((a, b, c, \dots), (a', b', c', \dots))$.

$$NC(v_1, \dots, v_k) \Leftrightarrow (v_1' = v_1) \wedge \dots \wedge (v_k' = v_k)$$

Parameters and side-effects

The specification of the procedure invocation will be written in terms of *actual* parameters.

In the declaration of this procedure *formal* parameters will be used.

Both, the specifications of subprograms appearing in the declaration, and statements in the declaration body must be written in terms of the formal parameters of the procedure (and its other local or non-local objects).

For sake of simplicity we will forbid any form of aliasing, e.g.:

- If more than one parameter is called by variable, then the actual parameters must be different variables.

If there are side-effects, then a variable external to the procedure body may not be passed as a parameter called by variable.

DISPLAY 1

Specification

Find(x, A, j, present)		
$R_0(.) = ((1 \leq n) \wedge \forall i [(1 \leq i < n) \Rightarrow ('A[i] \leq 'A[i+1])]) \Rightarrow$		
	$\exists i [(1 \leq i \leq n) \wedge ('A[i] = 'x)] =$	
	<i>true</i>	<i>false</i>
j'	'A[j]' = 'x	<i>true</i>
present' =	true	false
		$\wedge NC(x, A)$



Program

Procedure declaration:

```

procedure Find(e : integer; V : vector; var index : integer; var found : Boolean);
var low, high : integer;
begin
    Initialization; Body
end {Find}
    
```


DISPLAY 1 (Continued)

Program (Repeated)

Procedure declaration:

```

procedure Find(e : integer; V : vector; var index : integer; var found : Boolean);
var low, high : integer;
begin
  Initialization; Body
end {Find}
    
```



Specifications of Subprograms

Initialization	external variables: e, V, index, found, low, high
$R_1(.) = (low' = 1) \wedge (high' = n) \wedge (found' = false) \wedge (index' = 1) \wedge NC(e, V)$	

(on Display 4)

Body	external variables: e, V, index, found, low, high	
$R_2(.) = ((low' \leq high') \wedge (found' = false) \wedge \forall i [(low' \leq i < high') \Rightarrow (V[i] \leq V[i+1])]) \Rightarrow$		
$\exists i [(low' \leq i \leq high') \wedge (V[i] = e)] =$		
	<i>true</i>	<i>false</i>
index'	V[index'] = e	<i>true</i>
found' =	true	<i>false</i>
low'	<i>true</i>	<i>true</i>
high'	<i>true</i>	<i>true</i>
		$\wedge NC(e, V)$

(on Display 2)

END OF DISPLAY 1

DISPLAY 2

Specification

Body	external variables: e, V, index, found, low, high		<i>(from Display 1)</i>
$R_2(.) =$ $((\text{'low'} \leq \text{'high'}) \wedge (\text{'found'} = \text{false}) \wedge \forall i [(\text{'low'} \leq i < \text{'high'}) \Rightarrow (\forall [i] \leq \text{'V}[i+1])]) \Rightarrow$			
$\exists i [(\text{'low'} \leq i \leq \text{'high'}) \wedge (\text{'V}[i] = \text{'e'})]$ $=$			
	<i>true</i>	<i>false</i>	
index'	'V[index]' = 'e	<i>true</i>	
found' =	true	false	
low'	<i>true</i>	<i>true</i>	
high'	<i>true</i>	<i>true</i>	$\wedge \text{NC}(\text{e}, \text{V})$



DISPLAY 2 (Continued)

Program (Repeated)

New variable (to be declared in the embedding block): var med : integer;

Program statements:

```
{Body}
while not found and (low ≤ high) do begin
  med := (low + high) div 2;
  Test
end
```



Specifications of Subprograms

Test	external variables: e, V, index, found, low, high, med			(on Display 3)
$R_3(.) = ('low \leq 'med \leq 'high) \Rightarrow$				
	'V['med]			
	< 'e	= 'e	> 'e	
index'	<i>true</i>	index' = 'med	<i>true</i>	
found' =	'found	true	'found	
low' =	'med + 1	'low	'low	
high' =	'high	'high	'med - 1	$\wedge NC(e, V, med)$

END OF DISPLAY 2

DISPLAY 3

Specification

Test	external variables: e, V, index, found, low, high, med			(from Display 2)
$R_3(.) = ('low \leq 'med \leq 'high) \Rightarrow$				
	V['med]			
	< 'e	= 'e	> 'e	
index'	<i>true</i>	index' = 'med	<i>true</i>	
found' =	'found	true	'found	
low' =	'med + 1	'low	'low	
high' =	'high	'high	'med - 1	$\wedge NC(e, V, med)$

.....
Program

```
{Test}
if V[med] < e then
  low := med + 1
else
  if V[med] > e then
    high := med - 1
  else begin
    index := med;
    found := true
  end
end
```

.....
Specifications of Subprograms

Empty

END OF DISPLAY 3

DISPLAY 4

Specification

Initialization	external variables: e, V, index, found, low, high	<i>(from Display 1)</i>
$R_1(.) = (low' = 1) \wedge (high' = n) \wedge (found' = false) \wedge (index' = 1) \wedge NC(e, V)$		

.....
Program

{Initialization}
low := 1;
high := n;
found := false;
index := 1

.....
Specifications of Subprograms

Empty

END OF DISPLAY 4

LEXICON

A. Pascal external definitions and declarations

```
const n = n; {literal integer is to be written here}  
type vector = array[1..n] of integer;  
var x, j : integer; A : vector; present : Boolean;
```

INDEX

Name	Used in
A	D0, D1 ₁ , L _A
Body	D1 _{2,3} , D2 _{1,2}
e	D1 _{2,3} , D2 _{1,3} , D3, D4 ₁
Find	D1 _{1,2}
found	D1 _{2,3} , D2, D3, D4
high	D1 _{2,3} , D2, D3, D4
index	D1 _{2,3} , D2 _{1,3} , D3, D4
Initialization	D1 _{2,3} , D4
j	D0, D1 ₁ , L _A
low	D1 _{2,3} , D2, D3, D4
med	D2 _{2,3} , D3
n	D0, D1 _{1,3} , D4, L _A
present	D0, D1 ₁ , L _A
Test	D2 _{2,3} , D3
V	D1 _{2,3} , D2 _{1,3} , D3, D4 ₁
vector	D0, D1 ₂ , L _A
x	D0, D1 ₁ , L _A

Conclusions

Programs must be understood in small chunks

Programs should be presented in small chunks

NEVER read (or write) a long program.

Precise specifications/descriptions are essential

Size of specification not based on program size.

Without precise descriptions of program structure, even great programmers will err.

Correctness can be checked “by head”

Completeness, consistency, can be checked by machine.

Tools advantageous in daily use.

Review: What must you do

- (1) Begin with a specification of what you want the critical program to do.
- (2) Decompose the program:
 - Introduce modules/data abstractions/objects wherever possible and provide abstract specifications for them
 - Use hierarchical decomposition as demonstrated earlier.
- (3) Produce a set of displays based on the decomposition.
- (4) Make sure that the displays are complete and consistent
 - Every specification at the bottom of a page must appear at the top of another.
 - There can be only one implementation display for each program.
- (5) Verify/Inspect each display. Use tabular structure to decompose the inspection process.
- (6) When errors in specifications are found, mark all displays that include those specifications as requiring a repeat inspection.

Some Suggested Reading

- (1) Parnas, D. L., Weiss, D. M., “Active Design Reviews: Principles and Practices”, *Proceedings of the 8th International Conference on Software Engineering*, London, August 1985.
Also in *Journal of Systems and Software*, December 1987.
- (2) Parnas, D. L., Madey, J., Iglewski, M.,
“Precise Documentation of Well-Structured Programs”,
IEEE Transactions on Software Engineering, Vol. 20, No. 12,
December 1994, pp. 948 - 976.
- (3) Parnas, D. L. “Inspection of Safety Critical Software using Function Tables”, Proceedings of IFIP World Congress 1994, Volume III, August 1994, pp. 270 - 277.
- (4) Parnas, D. L., Asmis, G.J.K., Madey, J., “Assessment of Safety-Critical Software in Nuclear Power Plants”, *Nuclear Safety*, vol. 32, no. 2, April-June 1991, pp. 189-198.