Reverse Engineering from Assembler to Formal Specifications via Program Transformations

M. P. Ward
Software Technology Research Lab
De Montfort University
The Gateway,
Leicester LE1 9BH, UK
Martin.Ward@durham.ac.uk

Abstract

The FermaT transformation system, based on research carried out over the last sixteen years at Durham University, De Montfort University and Software Migrations Ltd., is an industrial-strength formal transformation engine with many applications in program comprehension and language migration. This paper is a case study which uses automated plus manually-directed transformations and abstractions to convert an IBM 370 Assembler code program into a very high-level abstract specification.

1 Introduction

Keywords: Assembler, Migration, Comprehension, Formal Methods, Abstraction, WSL, Wide Spectrum Language, Program Transformation, Legacy Systems, Restructuring.

2 Introduction

There is a vast collection of operational software systems which are vitally important to their users, yet are becoming increasingly difficult to maintain, enhance and keep up to date with rapidly changing requirements. For many of these so called *legacy systems* the option of throwing the system away and re-writing it from scratch is not economically viable. Methods are therefore urgently required which enable these systems to evolve in a controlled manner. In particular, legacy assembler systems have high maintenance costs, and migrating such systems to a different environment (eg. a client-server architecture) is much more difficult than for high-level language systems. The FermaT transformation system uses formal proven program transformations, which preserve or refine the semantics of a program while changing its form. These transformations are applied to restructure and simplify the legacy systems and to extract higher-level representations.

By using an appropriate sequence of transformations, the extracted representation is guaranteed to be equivalent to the original code logic. The method is based on a formal wide spectrum language, called WSL, with accompanying formal method. Over the last sixteen years we have developed a large catalogue of proven transformations, together with mechanically verifiable applicability conditions. These have been applied to many software development, reverse engineering and maintenance problems.

3 Theoretical Foundation

The theoretical work on which FermaT is based originated not in software maintenance, but in research on the development of a language in which proofs of equivalence for program transformations could be achieved as easily as possible for a wide range of constructs.

WSL is the "Wide Spectrum Language" used in our program transformation work, which includes low-level programming constructs and high-level abstract specifications within a single language. This has the advantage that one does not need to differentiate between programming and specification languages: the entire transformational development of a program from abstract specification to detailed implementation can be carried out in a single language. Conversely,

the entire reverse-engineering process, from a transliteration of the source program to a high-level specification, can also be carried out in the same language. During either of these processes, different parts of the program may be expressed at different levels of abstraction. So a wide-spectrum language forms an ideal tool for developing methods for formal program development and also for formal reverse engineering (for which we have coined the term *inverse engineering*).

A *program transformation* is an operation which modifies a program into a different form which has the same external behaviour (i.e. it is equivalent under a precisely defined denotational semantics). Since both programs and specifications are part of the same language, transformations can be used to demonstrate that a given program is a correct implementation of a given specification.

A *refinement* is an operation which modifies a program to make its behaviour more defined and/or more deterministic. A typical implementation of a nondeterministic specification will be a *refinement* rather than a strict equivalence. The opposite of refinement is *abstraction*: we say that a specification is an abstraction of a program which implements it. See [5,6] and [1] for a description of refinement.

The syntax and semantics of WSL are described in [8,9,12] so will not be discussed in detail here. Most of the constructs in WSL, for example **if** statements, **while** loops, procedures and functions, are common to many programming languages. However there are some features relating to the "specification level" of the language which are unusual. Expressions and conditions (formulae) in WSL are taken directly from first order logic: in fact, an infinitary first order logic is used (see [4] for details), which allows countably infinite disjunctions and conjunctions. This use of first order logic means that statements in WSL can include existential and universal quantification over infinite sets, and similar (non-executable) operations. Two list operators are also used in specifications: for a unary function f and list $L = \langle a_1, \ldots, a_n \rangle$ the map operator $*$ is defined:

$$f * L =_{\mathrm{DF}} \langle f(a_1), f(a_2), \ldots, f(a_n) \rangle$$

For a binary operator g and non-empty list L the reduce operator $/$ is defined:

$$\begin{aligned} g/L &=_{\mathrm{DF}} a_1 \qquad \text{if } n = 1 \\ &=_{\mathrm{DF}} g(a_1, g/\langle a_2, \ldots, a_n \rangle) \quad \text{if } \ell(L) > 1 \end{aligned}$$

For example, if f is a function which returns integers, and L is a non-empty list of suitable arguments for f, then $+/f * L$ is the result of applying f to every element of L and adding up the results. We also use $\ell(L)$ to denote the length of list L and $L[i\,..\,j]$ to denote the sublist $\langle a_i, \ldots, a_j \rangle$.

Over the last sixteen years we have been developing the WSL language, in parallel with the development of a transformation theory and proof methods. Over this time the language has developed from a simple and tractable kernel language [9] to a complete and powerful programming language. At the "low-level" end of the language there exist automatic translators from IBM Assembler into WSL, and from a subset of WSL into C. At the "high-level" end it is possible to write abstract specifications, similar to **Z** and VDM.

In [10,13] program transformations are used to derive a variety of efficient algorithms from abstract specifications. In [10,12,13] the same transformations are used in the reverse direction: using transformations to derive a concise abstract representation of the specification for several challenging programs.

In [11] we describe a case study using FermaT to migrate an assembler program to modular and maintainable C code, using purely automatic transformations with no manual intervention. As far as we know, none of the other researchers in program transformations (for example, [2,7]) have attempted to apply their methods to assembler code. The nearest research is Cristina Cifuentes work on decompilation and binary translation [Cifuentes CSMR00].

In this paper we go even further in the reverse engineering process. Starting with the same assembler program from [11] we use formal transformations to abstract an equivalent high-level specification of the program.

4 Example Transformations in FermaT

In this section we describe a small number of the transformations implemented in FermaT which are used in the case study. If $\mathbf{S}_1$ and $\mathbf{S}_2$ are any WSL statements and Δ is any countable set of formulae with no free variables, then we write $\Delta \vdash \mathbf{S}_1 \leq \mathbf{S}_2$ to denote that $\mathbf{S}_2$ is a refinement of $\mathbf{S}_1$ whenever all the formulae on Δ are true. If $\Delta \vdash \mathbf{S}_1 \leq \mathbf{S}_2$ and $\Delta \vdash \mathbf{S}_2 \leq \mathbf{S}_1$ then we write $\Delta \vdash \mathbf{S}_1 \approx \mathbf{S}_2$ and say that $\mathbf{S}_1$ and $\mathbf{S}_2$ are *equivalent*. If $\mathbf{S}_2$ is generated from $\mathbf{S}_1$ by a program transformation, then $\Delta \vdash \mathbf{S}_1 \approx \mathbf{S}_2$, where Δ is the set of applicability conditions for the transformation.

4.1 Expand Forwards

If $\mathbf{B}$ is any condition and $\mathbf{S}_1$, $\mathbf{S}_2$ and $\mathbf{S}_3$ are any statements then:

$$\Delta \vdash \textbf{if B then } \mathbf{S}_1 \textbf{ else } \mathbf{S}_2 \textbf{ fi}; \mathbf{S}_3 \approx \textbf{if B then } \mathbf{S}_1; \mathbf{S}_3 \textbf{ else } \mathbf{S}_2; \mathbf{S}_3 \textbf{ fi}$$

4.2 Loops

As well as the usual **for** and **while** loops, there is a notation for unbounded loops. Statements of the form **do S od**, where **S** is a statement, are "infinite" or "unbounded" loops which can only be terminated by the execution of a statement of the form **exit**(n) which causes the program to exit the n enclosing loops. We use **exit** as an abbreviation for **exit**(1). To simplify the language we disallow **exit**s which leave a block or a loop other than an unbounded loop. We also insist that n be an integer, *not* a variable or expression—this ensures that we can always determine the target of the **exit**.

Definition 4.1 *Global Substitution*
If $\mathbf{P}(\mathbf{S}, p)$ is a predicate on a statement $\mathbf{S}$ and position p within $\mathbf{S}$, and $\mathbf{S}'(\mathbf{S}, p)$ is a function which returns a statement for any given statement $\mathbf{S}$ and p, then the effect of replacing or appending to the statement at position p in $\mathbf{S}$ with $\mathbf{S}'(\mathbf{S}, p)$ for every p such that $\mathbf{P}(\mathbf{S}, p)$ holds is denoted:

$$\mathbf{S}\,[\,\mathbf{S}'(\mathbf{S}, p) \,/\, p \mid \mathbf{P}(\mathbf{S}, p)\,]$$

If the statement at position p in $\mathbf{S}$ is an **exit** statement, then it is replaced by $\mathbf{S}'(\mathbf{S}, p)$. Otherwise, $\mathbf{S}'(\mathbf{S}, p)$ is appended in sequence after the statement at position p.

Within a global substitution we use $\delta(\mathbf{S}, p)$ to denote the *depth* of a component of a statement. This is the number of enclosing **do** ... **od** loops surrounding the component. We use $\tau(\mathbf{S}, p)$ to denote the terminal value of a statement. This is the number of enclosing loops around $\mathbf{S}$ which might be terminated by execution of the statement at position p in $\mathbf{S}$. If the statement at position p in $\mathbf{S}$ does not terminate $\mathbf{S}$ then $\tau(\mathbf{S}, p) = -1$. For example, any **exit**(n) has terminal value n. If $\mathbf{S}$ contains an **exit**(n) within m nested loops (where $m \leqslant n$) then the terminal value of $\mathbf{S}$ itself, denoted $\tau(\mathbf{S}, \langle\rangle)$, will be at least $n - m$. A statement $\mathbf{S}$ with terminal value zero cannot terminate any enclosing loops, so the next thing to be executed after $\mathbf{S}$ will be the next statement in the sequence containing $\mathbf{S}$ (if there is one). Such a statement is called a *proper sequence*. If $\mathbf{S}$ is a proper sequence, then:

$$\Delta \vdash \textbf{do if B then exit fi}; \mathbf{S} \textbf{ od} \approx \textbf{while } \neg\mathbf{B} \textbf{ do } \mathbf{S} \textbf{ od}$$

In the following transformations, the global substitutions are all applied to the *simple terminal statements* of $\mathbf{S}$. These are the statements which are neither a sequence, a conditional, or a **do** ... **od** loop and which will terminate $\mathbf{S}$ if they are executed. For example, in:

if B then $x := 1;\ y := 2$ **else exit fi**

the terminal statements are $y := 2$ and **exit**. If the statement is enclosed in a **do** ... **od** loop, only the **exit** will be a terminal statement.

We usually omit the parameters from δ and τ in a global substitution when these are obvious from the context.

Definition 4.2 *Incrementation*
The incrementation of $\mathbf{S}$ by n (where n is any non-negative integer) is defined as the incrementation of all simple terminal statements in $\mathbf{S}$. An **exit** is incremented by incrementing its parameter, while any other simple statement is incremented by appending an **exit**:

$$\mathbf{S} + n \;=_{\mathrm{DF}}\; \mathbf{S}\,[\,\textbf{exit}(n + \delta) \,/\, p \mid \tau \geqslant 0\,]$$

For example:

$$\begin{aligned}&\textbf{if B then } x := 1;\ y := 2 \textbf{ else exit fi} + 2\\ &= \textbf{if B then } x := 1;\ y := 2;\ \textbf{exit}(2) \textbf{ else exit}(3) \textbf{ fi}\end{aligned}$$

while:

$$\begin{aligned}&\textbf{do if B then } x := 1;\ y := 2 \textbf{ else exit fi od} + 2\\ &= \textbf{do if B then } x := 1;\ y := 2 \textbf{ else exit}(3) \textbf{ fi od}\end{aligned}$$

Definition 4.3 *Partial Incrementation*
The notation $\mathbf{S} + (n, m)$ where $m \geqslant 0$ denotes incrementation of the terminal statements in $\mathbf{S}$ with terminal value m or greater:

$$\mathbf{S} + (n, m) \;=_{\mathrm{DF}}\; \mathbf{S}\,[\,\textbf{exit}(n + \delta) \,/\, p \mid \tau \geqslant m\,]$$

Note that **do S od** $+ (n, m) =$ **do S** $+ (n, m + 1)$ **od**.

4.3 Absorption

For any statements $\mathbf{S}_1$ and $\mathbf{S}_2$:

$$\Delta \vdash \mathbf{S}_1;\ \mathbf{S}_2 \approx \mathbf{S}_1\,[\,\mathbf{S}_2 + \delta \,/\, p \mid \tau = 0\,]$$

For example:

$$\textbf{do if B then } x := 1;\ y := 2 \textbf{ else exit fi od};\ z := 1$$
$$\textbf{do if B then } x := 1;\ y := 2 \textbf{ else } z := 1;\ \textbf{exit fi od}$$

This transformation can be applied in reverse to "take out" code from a loop.

4.4 False Loop

We can insert a loop around any statement, by incrementing it first:

$$\Delta \vdash \mathbf{S} \ \approx\ \textbf{do } \mathbf{S} + 1 \textbf{ od}$$

(This is a "false loop" because the body of the loop can only be executed once).

4.5 Loop Doubling

Any loop can be converted to a double loop by the last transformation, or by incrementing the body of the loop:

$$\begin{aligned}\Delta \vdash \textbf{do } \mathbf{S} \textbf{ od} \ &\approx\ \textbf{do do } \mathbf{S} \textbf{ od} + 1 \textbf{ od}\\ &\approx\ \textbf{do do } \mathbf{S} + 1 \textbf{ od od}\end{aligned}$$

More generally, we can arbitrarily decide whether or not to increment each terminal statement in $\mathbf{S}$ with terminal value zero:

$$\begin{aligned}&\Delta \vdash \textbf{do } \mathbf{S} \textbf{ od} \ \approx\\ &\textbf{do do } \mathbf{S}\,[\,\textbf{exit}(\delta+1)/p\\ &\qquad |\,\tau > 0 \ \vee\ \tau = 0 \ \wedge\ \Psi(\mathbf{S}, p)\,]\ \textbf{od od}\end{aligned}$$

Where Ψ is *any* condition on $\mathbf{S}$ and p.

This can be combined with the inverse of absorption to "isolate" part of a loop body. For example:

$$\begin{aligned}&\Delta \vdash \textbf{do } \mathbf{S};\ \textbf{if B then } \mathbf{S}_1 \textbf{ else } \mathbf{S}_2 \textbf{ fi od}\\ &\ \approx \textbf{do do } \mathbf{S} + (1,1);\\ &\qquad \textbf{if B then exit else } \mathbf{S}_2 + (1,1) \textbf{ fi od};\\ &\quad \mathbf{S}_1 \textbf{ od}\end{aligned}$$

4.6 Loop Inversion

If $\mathbf{S}_1$ is a proper sequence then:

$$\Delta \vdash \textbf{do } \mathbf{S}_1;\ \mathbf{S}_2 \textbf{ od} \ \approx\ \mathbf{S}_1;\ \textbf{do } \mathbf{S}_2;\ \mathbf{S}_1 \textbf{ od}$$

More generally, for *any* statements $\mathbf{S}_1$ and $\mathbf{S}_2$:

$$\Delta \vdash \textbf{do } \mathbf{S}_1;\ \mathbf{S}_2 \textbf{ od} \ \approx\ \textbf{do } \mathbf{S}_1;\ \textbf{do } \mathbf{S}_2;\ \mathbf{S}_1 \textbf{ od} + 1 \textbf{ od}$$

4.7 Loop Unrolling

We can unroll the first step of a loop:

$$\begin{aligned}\Delta \vdash \textbf{do } \mathbf{S} \textbf{ od} \ \approx\ \mathbf{S}[&\textbf{do } \mathbf{S} \textbf{ od} + \delta + 1 / p \mid \tau = 0\,]\\ &[\,\textbf{exit}(\tau + \delta - 1) / p \mid \tau \geqslant 1\,]\end{aligned}$$

where the RHS contains two successive global substitutions on $\mathbf{S}$.

More generally, we can insert a copy of the whole loop, with certain terminal statements of the loop body incremented, after certain terminal statements in the loop body. Let $\mathbf{S}'$ be formed from $\mathbf{S}$ by incrementing selected terminal statements with terminal value zero:

$$\mathbf{S}' = \mathbf{S}\,[\,\textbf{exit}(\delta+1)/p \mid \tau = 0 \ \wedge\ \Phi(\mathbf{S}, p)\,]$$

where Φ is any condition (see Section 4.5). Then:

$$\begin{aligned}&\Delta \vdash \textbf{do } \mathbf{S} \textbf{ od}\\ &\ \approx\ \textbf{do } \mathbf{S}\ \big[\textbf{do } \mathbf{S}' \textbf{ od} + \delta + 1 / p \,\big|\, \tau = 0 \ \wedge\ \Psi(\mathbf{S}, p)\,\big]\\ &\qquad [\,\textbf{exit}(\tau + \delta - 1) / p \mid \tau \geqslant 1\,]\ \textbf{od}\end{aligned}$$

where Ψ is any condition.

5 Modelling Assembler in WSL

Constructing a useful scientific model necessarily involves throwing away some information: in other words, to be useful a model *must* be inaccurate, or at least idealised, to a certain extent. For example "ideal gases", "incompressible fluids" and "billiard ball molecules" are all useful models which gain their utility by abstracting away some details of the real world. In the case of modelling a programming language, such as Assembler, it is theoretically possible to have a perfect model of the language which correctly captures the behaviour of all assembler programs. Certain features of Assembler, such as branching to register addresses, self-modifying code and so on, would imply that such a model would have to record the entire state of the machine, including all registers, memory, disk space, and external devices, and "interpret" this state as each instruction is executed. (Consider the effect of loading some data from a disk file into memory, performing arithmetic at arbitrary places in the data, and then branching to the start of the data block!) Unfortunately, such a model is useless for reverse engineering or migration purposes.

What we need is a practical model for assembler programs which is suitable for reverse engineering, and is accurate enough to deal with all the programming constructs which are likely to be encountered.

5.1 Assembler to WSL Translation

The aim of the assembler to WSL translator is to generate WSL code which models as accurately as possible the behaviour of the original assembler module, without worrying too much about the size, efficiency or complexity of the resulting code. Typically, the raw WSL translation of an assembler module will be three to five times bigger than the source file and have a very high McCabe cyclomatic complexity (typically in the hundreds, often in the thousands). This is, in part, because every "branch to register" instruction branches to the dispatch routine, which in turn contains branches to every possible return point. In addition, every instruction which sets the "condition code" flags will is translated into WSL code which assigns an appropriate value to a special variable cc (to emulate the condition code): whether or not the condition code is subsequently tested. See [11] for further details of the assembler to WSL translation process and the various features of commercial assembler code which it has to deal with.

However, the FermaT transformation engine includes some very powerful transformations for simplifying WSL code, removing redundancies, tracking dispatch codes, and so on. In most cases FermaT can automatically unscramble the tangle of "branch and save" and "branch to register" code to extract self-contained, single-entry single-exit procedures and so eliminate the dispatch procedure. In addition, FermaT can nearly always eliminate the cc variable by constructing appropriate conditional statements.

6 The Sample Program

Our sample program is from "A Guided Tour of Program Design Methodologies", by G. D. Bergland [3] who in turn took it from a story called "Getting it Wrong" that has been related by Michael Jackson on numerous occasions:

```
proc Management_Report ≡
  var SW1 := 0, SW2 := 0 :
    Produce_Heading;
    read(stuff);
    while NOT eof(stuff) do
      if First_Record_In_Group
        then if SW1 = 1
                then Process_End_Of_Previous_Group
             fi;
             SW1 := 1;
             Process_Start_Of_New_Group;
             Process_Record;
             SW2 := 1
        else
          Process_Record; SW2 := 1
      fi;
      read(stuff)
    od;
    if SW2 = 1 then Process_End_Of_Last_Group
    fi;
    Produce_Summary
  end.
```

The program is a simple report generator which reads a sorted transaction file: each transaction contains the name of an item and the amount received or distributed from the warehouse. The program generates a report showing the net change in inventory for each item in the transaction file.

Our resident assembler guru was given the above pseudocode and asked to write an assembler implementation which uses as many "features" of assembler as possible. The result is given in Section 11 (I should like to point out on his behalf that this is *not* his normal coding style!) The program includes self-modifying code: the "first time through switch" `SW1` is implemented by modifying the branch labelled `LAAA` to a `NOP` in the instruction labelled `LAB`, and an EXecute statement has been used to get a variable length move.

7 Automatic Program Transformation

The first stage in the transformation process is Data Translation. This transformation uses the restructured data file to change the data representation in the program. Initially all data is accessed directly from memory (represented as the byte array a) by adding the base register to the displacement to get an address. The restructured data file gives the layout of all data in memory, so by making some reasonable assumptions about non-overlapping DSECTS etc., FermaT is able to transform the program into an equivalent program where the data is accessed directly through variables and structures. For example, consider the "raw WSL" statement:

```
!P mvc(a[db(writem, r3), 3 + 1]
        var a[db(wlast, r3), 3 + 1]);
```

Here, the !P indicates an external procedure call to the mvc procedure which implements the MVC (move characters) instruction. This moves the given number of characters from the given source address to

the given destination address. The function db(x, y) simply returns $x + y$, the displacement plus the base register, so the source address is writem + r3 and the destination address is wlast + r3. After data translation, the same names are used as the actual variables and the base registers are eliminated.

This statement is automatically transformed into the simple assignment:

```
wlast := wrec.writem;
```

In the case of our simple program, there is only one structure to uncover: the wrec print record which contains fields writem, wrtype and wrqty plus some unnamed fillers.

The next stage is control flow restructuring: eliminating non-essential labels and branches, introducing loops. This is carried out in a series of passes through the program, at each iteration the program is searched for points where a simplifying transformation (such as loop insertion or branch merging) can be applied. The iteration is continued until no further improvement can be achieved.

The raw WSL is written as an *action system*, a collection of parameterless procedures (actions) where execution of any actuin will always lead to either calling another action, or calling the special action Z which terminates the whole action system. An action system itself is a simple statement, so action systems can be nested inside each other, but a sub-action system cannot call actions in the main system.

The system then analyses the remaining actions to determine which actions may form the body of a simple procedure. To do this it uses both control flow and data flow analysis. If it determines that a collection of actions form a procedure, then these actions are extracted out as a sub-action system in the body of the procedure.

After control flow restructuring we have data flow analysis: in particular an extended form of constant propagation which can propagate return addresses through procedure calls. If a dispatch call is encountered with a known destination value, then it can be unfolded and simplified. The same transformation also deals with conditional assignments to the condition code (cc) in order to remove references to cc where possible.

FermaT was able to extract a collection of actions to form the endgroup procedure, so that the code:

```
r10 := 112; call endgroup
```

becomes:

```
r10 := 112; endgroup(); call dispatch
```

FermaT determines that the value in r10 will be copied into destination by the body of endgroup. Within dispatch the value in destination is compared against the offsets of all the possible return points. Offset 112 is associated with the label lab, so this **call** dispatch can be replaced by **call** lab.

The control flow and data flow restructuring transformations are iterated until no further improvement is possible. Figure 1 lists the metrics for the raw WSL translation and after automatic restructuring and simplifying transformations have been applied. This order of magnitude improvement in most of the metrics is typical for all sizes of assembler module. See [11] for more details of this part of the transformation process.

Metric	Raw WSL	Structured WSL
Statements	561	106
Expressions	1,589	210
McCabe	184	17
Control/Data Flow	520	156
Branch–Loop	145	17
Structural	6,685	751

Figure 1: Metrics Before and After Transformation

```
begin
  f_laaa := 1;
  !P open(ddin_ddname, input var os);
  !P open(rdsout_ddname, output var os);
  wprt[1..17] := "MANAGEMENT REPORT";
  write1(); write1();
  wprt[1..20] := "ITEM NET CHANGE";
  write1(); write1();
  xsw1 := 0;
  do r0 := 0; r1 := 0; r15 := 0;
     !P get(ddin_ddname var os, r0, r1, r15, wrec);
     if !XC end_of_file(ddin_ddname)
       then exit(1) fi;
     if wrec.writem ≠ wlast
       then if f_laaa ≠ 1
                then endgroup() fi;
            f_laaa := 0;
            wlast := wrec.writem;
            wnet := !XF zap("hex 0x0C") fi;
     worka := !XF pack(wrec.wrqty, 2);
     if wrec.wrtype ≠ "R"
       then wnet := !XF sp(wnet, worka)
        else wnet := !XF ap(wnet, worka) fi;
     xsw1 := "hex 0xFF" od;
```

```
  if xsw1 = "hex 0xFF" then endgroup() fi;
  wprt[1..17] := "NUMBER CHANGED = ";
  !P ed(wchange[1..10] var workb);
  r4 := !XF address_of(workb); r1 := 9;
  do if a[r4, 1] ≠ " " then exit(1) fi;
      r4 := r4 + 1;
      r1 := r1 − 1;
      if r1 = 0 then exit(1) fi od;
  a[!XF address_of(wprt) + 17, r1 + 1]
    := a[r4, r1 + 1];
  write1();
  !P close(ddin_ddname var os);
  !P close(rdsout_ddname var os)
where
proc endgroup() ≡
  wprt[1..4] := wlast;
  wsign := "+";
  if wnet < "hex 0x0C" then wsign := "-" fi;
  wprt[8..17] := "hex 0x40206B2020206B202120";
  !P edmk(wnet[1..10] var wprt[8..17], r1);
  r1 := r1 − 1;
  a[r1, 1] := wsign;
  write1(); write1();
  wchange := !XF ap(wchange, "hex 0x1C") end,
proc write1() ≡
  !P put(rdsout_ddname, wprt var os);
  wprt := wspaces end
end
```

8 Abstracting a Specification

This is about as far as the FermaT system can get by purely automatic transformation applications with no human intervention. The next step in the abstraction process is to change the data representation so that files become lists. We unfold the write1 procedure and replace zap, ap and sp calls by their actual operations. We abstract away from the layout of the output file by creating a list of the data elements that appear on each line of output and appending this list to the output array:

```
begin
  i := 0; f_laaa := 1;
  output := ⟨⟨"MANAGEMENT REPORT"⟩,
            ⟨"ITEM       NET CHANGE"⟩⟩;
  xsw1 := 0;
  do i := i + 1; wrec := input[i];
      if i ⩾ n then exit(1) fi;
      if wrec.writem ≠ wlast
        then if f_laaa ≠ 1
                then endgroup() fi;
             f_laaa := 0;
             wlast := wrec.writem;
             wnet := 0 fi;
        if wrec.wrtype ≠ "R"
          then wnet := wnet − wrec.wrqty
           else wnet := wnet + wrec.wrqty fi;
        xsw1 := "hex 0xFF" od;
  if xsw1 = "hex 0xFF" then endgroup() fi;
  output :=output ++
            ⟨⟨"NUMBER CHANGED = ", wchange⟩⟩;
where
proc endgroup() ≡
  output := output ++ ⟨⟨wlast, wnet⟩⟩;
  wchange := wchange + 1 end
end
```

We can get rid of the switches xsw1 and f_laaa by unrolling the first step of the **do** ... **od** loop and simplifying. We then use *loop inversion* to move some statements to the top of the loop:

```
i := i + 1; wrec := input[i];
if i ⩾ n
  then skip
   else wlast := wrec.writem;
        wnet := 0;
        do if wrec.wrtype ≠ "R"
              then wnet := wnet − wrec.wrqty
               else wnet := wnet + wrec.wrqty fi;
           i := i + 1; wrec := input[i];
           if wrec.writem ≠ wlast ∨ i ⩾ n
             then endgroup();
                  if i ⩾ n
                    then exit(1)
                     else wlast := wrec.writem;
                          wnet := 0 fi fi od fi;
```

We want to roll the two statements LAST := wrec.writem; wnet := 0 into the top of the loop, so convert the loop to a double-nested loop (*loop doubling*) and take the statements out of the inner loop (*take out of loop*). Then apply *loop inversion*. We can then take the statements starting with endgroup() out of the inner loop also:

```
i := i + 1; wrec := input[i];
if i ⩾ n
  then skip
   else do wlast := wrec.writem;
           wnet := 0;
           do if wrec.wrtype ≠ "R"
                 then wnet := wnet − wrec.wrqty
                  else wnet := wnet + wrec.wrqty fi;
              i := i + 1; wrec := input[i];
```

```
        if wrec.writem ≠ wlast ∨ i ⩾ n
          then exit(1) fi od;
      endgroup();
      if i ⩾ n exit(1) fi od fi;
```

Finally, the outer **if** statement can be removed by converting the outer loop to a **while** loop (this is the *floop to while* transformation):

```
i := i + 1; wrec := input[i];
while i < n do
  wlast := wrec.writem;
  wnet := 0;
  do if wrec.wrtype ≠ "R"
        then wnet := wnet − wrec.wrqty
         else wnet := wnet + wrec.wrqty fi;
     i := i + 1; wrec := input[i];
     if wrec.writem ≠ wlast ∨ i ⩾ n
        then exit(1) fi od;
  endgroup() od;
```

Note that, after the initialisation code, the invariant wrec = input[i] is always true, and for $i > 1$, wlast = input[$i-1$].writem is also true, as is the invariant wchange = ℓ(output) -2. So we can remove these three variables from the program.

The program now consists of two simple nested loops, the outer **while** loop iterates over the groups of records and ends with a call to endgroup(), while the inner **do** ... **od** loop iterates over the records in the group.

This suggests that we restructure the data to more closely match the control structure of the program by converting the input array to a list of lists where each sublist consists of a single group of data elements, so that the outer loop processes sublists one at a time and the inner loop processes elements of each sublist. The key to the data restructuring is to split the input sequence into sections such that the outer loop processes one segment per iteration. This is easily achieved with a function split(p, B) which splits p into non-empty sections with the section breaks occurring between those pairs of elements of p where B is false. (See [12] for a formal definition of split). In our case, the terminating condition on the inner loop provides the predicate on which to split:

```
funct same_item(x, y) ≡
  x.writem = y.writem.
```

Then the new variable q is introduced with the assignment: q := split(input, same_item). We index the q list with two variables k_1 and k_2 so that $q[k_1][k_2]$ = input[i]. To do this we preserve the invariant:

$$i = +/(\ell * q[1\,..\,k_1 - 1]) + k$$

which, together with the invariant input = $+\!\!+/q$ gives the required relationship. Adding these ghost variables to the program we get:

```
q := split(input, same_item);
i := 1; k1 := 1; k2 := 1;
while i < ℓ(input) do
  wnet := 0;
  do if input[i].wrtype ≠ "R"
        then wnet := wnet − input[i].wrqty
         else wnet := wnet + input[i].wrqty fi;
     i := i + 1;
     k2 := k2 + 1;
     if k2 > ℓ(q[k1]) then k1 := k1 + 1; k2 := 1 fi;
     if input[i].writem ≠ input[i − 1].writem
        ∨ i ⩾ ℓ(input) then exit(1) fi od;
     endgroup() od;
```

We can now replace references to the concrete variables input and i by references to the new variables q, k_1 and k_2. The key point is that $i < \ell$(input) if and only if $k_1 < \ell(q)$ and

$$\text{input}[i].\text{writem} \neq \text{input}[i-1].\text{writem}$$

is true when we have just moved into a new section of the input: in other words, precisely when $k_2 = 1$. So we can remove the concrete variables from the program:

```
q := split(input, same_item);
k1 := 1; k2 := 1;
while k1 < ℓ(q) do
  wnet := 0;
  do if q[k1][k2].wrtype ≠ "R"
        then wnet := wnet − q[k1][k2].wrqty
         else wnet := wnet + q[k1][k2].wrqty fi;
     k2 := k2 + 1;
     if k2 > ℓ(q[k1]) then k1 := k1 + 1; k2 := 1 fi;
     if k2 = 1 then exit(1) fi od;
  endgroup() od;
```

Now the inner loop reduces to a simple **for** loop:

```
q := split(input, same_item);
k1 := 1;
while k1 < ℓ(q) do
  wnet := 0;
  for k2 := 1 to ℓ(q[k1]) step 1 do
     if q[k1][k2].wrtype ≠ "R"
        then wnet := wnet − q[k1][k2].wrqty
         else wnet := wnet + q[k1][k2].wrqty fi;
     k1 := k1 + 1;
     endgroup() od;
```

We can express the change to wnet as a function of the structure:

funct change(s) $\equiv$
  if s.wrtype $\neq$ "R" **then** $-s$.wrqty **else** s.wrqty **fi.**

It is clear that the inner loop is computing the sum of the change outputs for all the structures in the sub list $q[k_1]$, so we can collapse the inner loop to a reduce of a map operation:

$q :=$ split(input, same_item);
$k_1 := 1$;
while $k_1 < \ell(q)$ **do**
  wnet := +/change * $q[k_1]$;
  $k_1 := k_1 + 1$;
  endgroup() **od**;

The endgroup procedure simply appends an element to the output list:

$q :=$ split(input, same_item);
$k_1 := 1$;
while $k_1 < \ell(q)$ **do**
  wnet := +/change * $q[k_1]$;
  output := output $+\!\!+$ $\langle\langle q[k_1][1], \text{wnet}\rangle\rangle$;
  $k_1 := k_1 + 1$;
  endgroup() **od**;

so we can collapse the outer loop to a map operation. See Section 12 for the final specification.

This extracted specification looks very different to the original assembler (see Section 11) but both programs are semantically equivalent and generate identical output files (when the output from the specification is formatted to match the assembler).

9 Conclusion

This paper describes a particularly challenging reverse engineering task: using formal program transformations to extract a high-level abstract specification from an IBM 370 assembler program. The original assembler program contains several "layers" of complexity including self-modifying code, a flag used to direct control flow, a convoluted control flow structure and so on. Fortunately the powerful automatic transformations implemented in FermaT allow us to remove the first few layers of complexity before we even have to look at the program. Moving to higher levels of abstraction requires a certain amount of human intervention: particularly to select appropriate abstract data structures. However, this intervention requires only localised analysis of the program. The higher-level control flow transformations such as loop unrolling, loop rolling, taking code out of loops etc., are all implemented in the FermaT system and any global analysis required by these transformations is handled automatically.

10 References

[1] R. J. R. Back, *Correctness Preserving Program Refinements*, Mathematical Centre Tracts #131, Mathematisch Centrum, Amsterdam, 1980.

[2] F. L. Bauer, B. Moller, H. Partsch & P. Pepper, "Formal Construction by Transformation—Computer Aided Intuition Guided Programming," *IEEE Trans. Software Eng.* 15 (Feb., 1989).

[3] G. D. Bergland, "A Guided Tour of Program Design Methodologies," *Computer* 14 (Oct., 1981), 18–37.

[4] C. R. Karp, *Languages with Expressions of Infinite Length*, North-Holland, Amsterdam, 1964.

[5] C. C. Morgan, *Programming from Specifications*, Prentice-Hall, Englewood Cliffs, NJ, 1994, Second Edition.

[6] C. C. Morgan, K. Robinson & Paul Gardiner, "On the Refinement Calculus," Oxford University, Technical Monograph PRG-70, Oct., 1988.

[7] H. A. Partsch, *Specification and Transformation of Programs*, Springer-Verlag, New York–Heidelberg–Berlin, 1990.

[8] H. A. Priestley & M. Ward, "A Multipurpose Backtracking Algorithm," *J. Symb. Comput.* 18 (1994), 1–40, ⟨http://www.dur.ac.uk/~dcs0mpw/martin/papers/backtr-t.ps.gz⟩.

[9] M. Ward, "Proving Program Refinements and Transformations," Oxford University, DPhil Thesis, 1989.

[10] M. Ward, "Program Analysis by Formal Transformation," *Comput. J.* 39 (1996), ⟨http://www.dur.ac.uk/~dcs0mpw/martin/papers/topsort-t.ps.gz⟩.

[11] M. Ward, "Assembler to C Migration using the FermaT Transformation System," *International Conference on Software Maintenance, 30th Aug–3rd Sept 1999, Oxford, England* (1999).

[12] M. Ward, "Abstracting a Specification from Code," *J. Software Maintenance: Research and Practice* 5 (June, 1993), 101–122, ⟨http://www.dur.ac.uk/~dcs0mpw/martin/papers/prog-spec.ps.gz⟩.

[13] M. Ward, "Derivation of Data Intensive Algorithms by Formal Transformation," *IEEE Trans. Software Eng.* 22 (Sept., 1996), 665–686, ⟨http://www.dur.ac.uk/~dcs0mpw/martin/papers/sw-alg.ps.gz⟩.

11 The Assembler Source

```
****************************************
*  TST004A0  SAMPLE PROGRAM (MCDONALDS) *
****************************************
*
         REGEQU
*
*        PRINT NOGEN
TST004A0 CSECT
         STM   R14,R12,12(R13)
         LR    R3,R15
         USING TST004A0,R3
         ST    R13,WSAVE+4
         LA    R14,WSAVE
         ST    R14,8(R13)
         LA    R13,WSAVE
*
         OPEN  (DDIN,(INPUT))
         OPEN  (RDSOUT,(OUTPUT))
*
         MVC   WPRT(17),=CL17'MANAGEMENT REPORT'
         BAL   R10,WRITE1
         BAL   R10,WRITE1
         MVC   WPRT(20),=CL20'ITEM      NET CHANGE'
         BAL   R10,WRITE1
         BAL   R10,WRITE1
*
         MVI   XSW1,0
LAA      EQU   *
         GET   DDIN,WREC
         CLC   WRITEM,WLAST
         BE    LAC
LAAA     B     LAB
         BAL   R10,ENDGROUP
LAB      MVI   LAAA+1,0
         MVC   WLAST,WRITEM
         ZAP   WNET,=P'0'
         BAL   R10,PROCGRP
         MVI   XSW1,X'FF'
         B     LAA
LAC      BAL   R10,PROCGRP
         MVI   XSW1,X'FF'
         B     LAA
*
LAD      CLI   XSW1,X'FF'
         BNE   LADA
         BAL   R10,ENDGROUP
LADA     EQU   *
         MVC   WPRT(17),=CL17'NUMBER CHANGED = '
         ED    WORKB,WCHANGE
         LA    R4,WORKB
         LA    R1,9
LADB     CLI   0(R4),C' '
         BNE   LADC
         LA    R4,1(R4)
         BCT   R1,LADB
LADC     EX    R1,WMVC1
*WMVC1   MVC   WPRT+17(1),0(R4)
         BAL   R10,WRITE1
*
         CLOSE DDIN
         CLOSE RDSOUT
*
         L     R13,WSAVE+4
         LM    R14,R12,12(R13)
         SLR   R15,R15
         BR    R14
*
PROCGRP  EQU   *
         ST    R10,WST10A
         PACK  WORKA,WRQTY
         CLI   WRTYPE,C'R'
         BNE   LBA
         AP    WNET,WORKA
         B     LBB
LBA      SP    WNET,WORKA
LBB      L     R10,WST10A
         BR    R10
*
ENDGROUP EQU   *
         ST    R10,WST10A
         MVC   WPRT(4),WLAST
         MVI   WSIGN,C'+'
         CP    WNET,=P'0'
         BNL   LCA
         MVI   WSIGN,C'-'
LCA      EQU   *
         MVC   WPRT+7(10),=X'40206B2020206B202120'
         EDMK  WPRT+7(10),WNET
         BCTR  R1,0
         MVC   0(1,R1),WSIGN
         BAL   R10,WRITE1
         BAL   R10,WRITE1
         AP    WCHANGE,=P'1'
         L     R10,WST10A
         BR    R10
*
WRITE1   EQU   *
         PUT   RDSOUT,WPRT
         MVC   WPRT,WSPACES
         BR    R10
*
WMVC1    MVC   WPRT+17(1),0(R4)
*
WSAVE    DC    18F'0'
WST10A   DS    F
WREC     DS    0CL80
WRITEM   DS    CL4
         DS    CL1
WRTYPE   DS    CL1
         DS    CL1
WRQTY    DS    CL3
         DS    CL70
WPRT     DC    CL80' '
WSPACES  DC    CL80' '
WLAST    DC    CL4'****'
WCHANGE  DC    PL4'0'
WNET     DC    PL4'0'
WORKA    DC    PL2'0'
WORKB    DC    XL10'40206B2020206B202120'
WSIGN    DC    CL1' '
XSW1     DC    X'00'
*
         LTORG
*
DDIN     DCB   DDNAME=DDIN,
               DSORG=PS,
               EODAD=LAD,
               MACRF=GM
RDSOUT   DCB   DDNAME=RDSOUT,
               DSORG=PS,
               MACRF=PM
*
         END
```

12 The WSL Specification

begin
  $q :=$ split(input, same_item);
  output :=header $\#$ process $*\ q$
    $\#\ \langle\langle$"NUMBER CHANGED = ", $\ell(q)\rangle\rangle$
where
funct same_item$(x, y)\ \equiv\ x$.writem $= y$.writem.
funct process$(L)\ \equiv\ \langle L[1], +/$change $*\ L\rangle$.
funct change$(s)\ \equiv$
  if s.wrtype $\neq$ "R" **then** $-s$.wrqty **else** s.wrqty **fi**.
end