DECUS
PROGRAM LIBRARY

DECUS NO.	5/8-18C
TITLE	DISASSEMBLER WITH SYMBOLS
AUTHOR	Eberhard Werner
COMPANY	University of California, San Diego Marine Physical Laboratory of the Scripps Institution of Oceanography, San Diego, California
DATE	October 16, 1967
SOURCE LANGUAGE	PAL

DISASSEMBLER WITH SYMBOLS

DECUS Program Library Write-up

DECUS No. 5/8-18C

ABSTRACT

Disassembler accepts a binary tape of standard format and produces a listing of the tape in PAL-III mnemonics and a cross reference table of all addresses referenced by any memory reference instruction. A symbol table may be entered to produce a listing similar to a PAL-III Pass 3 listing. A patch to produce only a cross reference table is included.

REQUIREMENTS

The program is loaded into locations 20-1773 and uses 1774-7577 for scratch storage for the symbol table and cross reference table.

Input is on the high-speed reader. Output is either on ASR-33 or on high-speed punch (selectable by switch setting). The type 182 EAE is used.

USAGE

Disassembler is available in standard binary loader format.

Bit 0 of the switch register OFF indicates output on the ASR-33. Bit 0 ON indicates output on high-speed punch. Bit 11 ON indicates presence of floating-point system instructions.

(A) Start program at 200.
(B) Computer halts at 201.
(C) Load symbol table tape in high-speed reader.
(D) Press "CONTINUE". Computer will read tape and halt at 1522.
(E) Load binary program tape in high-speed reader.
(F) Set bit 0 of switch register for desired output device. Set bit 11 of switch register if floating point instructions occur in the program.

(G) Press "CONTINUE". Program will read binary tape and output listing and cross reference table. Program then proceeds to step (B) above and entire procedure may be repeated. To disassemble a second program using the same symbol table, place binary tape in reader and start at 1530. Control bits of the SR must be set before START is pressed.

Note: Step (C) is optional and may be skipped. Step (D), however, may not be skipped.

If a character is missed by the reader, the program will be out of step with the binary tape (i.e., the last six bits of an instruction will be taken as the first six bits of the next instruction and the first six bits will be taken as the last six bits of the previous instruction). When the program reads a character with a channel seven or eight punch as the

second character of a two-character word, the message "READER ERROR" is typed out and the computer halts.

If the scratch storage for the cross reference table is exceeded the message "CROSS REF TABLE FULL" is typed.

Field settings on the binary tape will be treated as if the end of the tape has been reached.

Recovery from reader error is to restart the program, or press "CONTINUE" to synchronize program with tape. The latter, however, will produce erroneous references in the cross reference table, and, of course, a portion of the listing is in error.

When the cross reference table is full, no more entries will be made. Only recovery possible is to segment the binary tape and run the program through several cycles.

If a tape without field settings can be made, this should be used. Otherwise each segment must be treated as an independent program.

RESTRICTIONS

(None)

DESCRIPTION

Disassembler is a general utility program. It will provide a symbolic listing from a binary tape. PAL-III mnemonic and effective address, if any, are typed out. If a symbol table is provided, the effective address is replaced by the symbol. A reference table of all direct references is printed. See example below for detailed description of program features.

The program is used in cases where a binary program tape but no symbolic listing is available. This generally occurs when a program is obtained from an outside source without any documentation. The tape is run through the program, then the user assigns symbols to certain memory locations and types a symbol table. The symbol table and binary tape are then run through the disassembler program for a symbolic listing. A second case is where a program has had extensive changes made by changing the contents of program locations by use of ODT or the switches. A disassembler listing will provide documentation of modifications and a reference for future modifications or for changing the program source tape.

Example:

Below are shown a short program as listed by PAL-III Pass 3 and two versions produced from the binary tape by Disassembler. The symbol table was entered in the second version.

(A) PAL-III Pass 3 Output

```
                    /Disassembler Test Program
Ø2ØØ   6Ø46                 TLS
Ø2Ø1   6Ø41   BEGIN,        TSF
```

```
Ø2Ø2   52Ø1                JMP .-1
Ø2Ø3   1221                TAD A
Ø2Ø4   7Ø41                CIA
Ø2Ø5   7415                ASR
Ø2Ø6   ØØØ5                5
Ø2Ø7   75Ø1                MQA
Ø21Ø   3223                DCA B+1
Ø211   44Ø7                FPNT
Ø212   5222                FGET B
Ø213   3225                FMPY C
Ø214   ØØØ3                FSIN
Ø215   623Ø                FPUT D
Ø216   ØØØØ                FEXT
Ø217   76Ø2                HLT CLA
Ø22Ø   52Ø1                JMP BEGIN
Ø221   7776        A,      -2
Ø222   6Ø4Ø        B,      6Ø4Ø
Ø223   2ØØØ                2ØØØ
Ø224   ØØØØ                ØØØØ
Ø225   ØØ1Ø        C,      ØØ1Ø
Ø226   2ØØØ                2ØØØ
Ø227   ØØØØ                ØØØØ
Ø23Ø   ØØØØ        D,      Ø
Ø231   ØØØØ                Ø
Ø232   ØØØØ                Ø

A      Ø221
B      Ø222
BEGIN  Ø2Ø1
C      Ø225
D      Ø23Ø
```

(B) Disassembler output: No symbol table tape was read by the program.

```
*Ø2ØØ
ØØØØ   6Ø46    TCF TPC
Ø2Ø1   6Ø41    TSF
Ø2Ø2   52Ø1    JMP .-1          Note (1)
Ø2Ø3   1221    TAD Ø221
Ø2Ø4   7Ø41    CMA IAC
Ø2Ø5   7415    ASR              Note (3)
Ø2Ø6   ØØØ5    ØØØ5             Note (3)
Ø2Ø7   75Ø1    MQA
Ø21Ø   3223    DCA Ø223
Ø211   44Ø7    FPNT             Note (5)
Ø212   5222    FGET Ø222
Ø213   3225    FMPY Ø225
Ø214   ØØØ3    SUBR ØØØ3        Note (6)
Ø215   623Ø    FPUT Ø23Ø
Ø216   ØØØØ    FEXT
Ø217   76Ø2    CLA HLT
```

```
Ø22Ø   52Ø1   JMP Ø2Ø1
Ø221   7776   CLA SPA SNA SZL OSR HLT          Note (7)
Ø222   6Ø4Ø   6Ø4Ø
Ø223   2ØØØ   2ØØØ            Note (8)
Ø224   ØØØØ   Ø
Ø225   ØØ1Ø   AND ØØ1Ø         Note (9)
Ø226   2ØØØ   2ØØØ            Note (8)
Ø227   ØØØØ   Ø
Ø23Ø   ØØØØ   Ø
Ø231   ØØØØ   Ø
Ø232   ØØØØ   Ø
Ø233   22Ø4   ISZ Ø2Ø4         Note (10)
```

New Page

CROSS REF TABLE

```
ØØ1Ø   Ø225          Note (11)
Ø2Ø1   Ø22Ø          Note (12)
Ø2Ø4   Ø233
Ø221   Ø2Ø3
Ø222   Ø212
Ø223   Ø21Ø
Ø225   Ø213
Ø23Ø   Ø215
```

(C) Disassembler output. The symbol table tape as produced by PAL-III was read by the program. Notice the similarity of this listing to (A).

```
*Ø2ØØ
Ø2ØØ   6Ø46          TCF TPC
Ø2Ø1   6Ø41   BEGIN,  TSF
Ø2Ø2   52Ø1          JMP BEGIN          Note (1)
Ø2Ø3   1221          TAD A              Note (2)
Ø2Ø4   7Ø41          CMA IAC
Ø2Ø5   7415          ASR                Note (3)
Ø2Ø6   ØØØ5          ØØØ5               Note (3)
Ø2Ø7   75Ø1          MQA
Ø21Ø   3223          DCA Ø223           Note (4)
Ø211   44Ø7          FPNT               Note (5)
Ø212   5222          FGET B
Ø213   3225          FMPY C
Ø214   ØØØ3          SUBR ØØØ3          Note (6)
Ø215   623Ø          FPUT D
Ø216   ØØØØ          FEXT
Ø217   76Ø2          CLA HLT
Ø22Ø   52Ø1          JMP BEGIN
Ø221   7776   A,     CLA SPA SNA SZL OSR HLT        Note (7)
Ø222   6Ø4Ø   B,     6Ø4Ø
Ø223   2ØØØ          2ØØØ               Note (8)
Ø224   ØØØØ          Ø
```

```
Ø225   ØØ1Ø   C,      AND ØØ1Ø      Note (9)
Ø226   2ØØØ           2ØØØ          Note (8)
Ø227   ØØØØ           Ø
Ø23Ø   ØØØØ   D,       Ø
Ø231   ØØØØ            Ø
Ø232   ØØØØ            Ø
Ø233   22Ø4            ISZ Ø2Ø4      Note (10)
```

New Page

CROSS REF TABLE

```
ØØ1Ø                Ø225              Note (11)
Ø2Ø1   BEGIN        Ø2Ø2  Ø22Ø        Note (12)
Ø2Ø4                Ø233
Ø221   A,           Ø2Ø3
Ø222   B,           Ø212
Ø223                Ø21Ø
Ø225   C,           Ø213
Ø23Ø   D,           Ø215
```

NOTES

(1) This instruction uses relative addressing in (B) but symbolic addressing in (C) since a symbol appears for location 200 in the symbol table.

(2) The symbol "A" was in the symbol table and so appears here replacing the octal address.

(3) "ASR" is a two word EAE instruction so the second word appears as an octal representation.

(4) The address here was "B + 1". However, the address does not appear in the symbol table and so has been left as an octal representation. It would have been possible to enter "B + 1 " as a symbol with the appropriate address.

(5) Switch 11 was ON so a "JMS I 7" is interpreted as entry to the floating point system.

(6) Floating point subroutines are noted as "SUBR XXXX" where XXXX is the number of the subroutine in octal.

(7) This is a constant (-2). However, it produces a legal combination of group 2 microinstructions and has therefore been decoded as such.

(8) Although 2000 may be decoded to "ISZ 0 ", all references to address 0 are considered illegal.

(9) This is part of the constant. However, it is also a legal instruction.

(10) The checksum is also decoded.

(11) The cross reference table will contain some spurious reference produced by decoding constants.

(12) If an address is decoded as relative addressing (e.g., ".-1"), the reference is not entered in the cross reference table. Note that 0202 is entered for "BEGIN" in (C) but not for 201 in (B).

METHODS

The first phase of the program is to read a symbol table. Accepted characters are carriage return and all characters between 240 and 336. All other characters are ignored. Channel eight punches need not be present. The symbol table is stored starting immediately after the program, four words per symbol, as an address followed by six characters of the symbol.

The second phase is to decode the binary tape. Two characters are read and assembled as a 13 bit word and tested for program counter reset and if so, the proper routine is entered. Program counter resets cause a new page and typing of "*XXXX, where XXXX is the reset figure. For instructions, a search is made through the symbol table, if any, for a symbol with a corresponding address. If one is found it is typed. Instructions are then subdivided into memory reference, floating point or non-floating point, group one, group two, or EAE operate instruction, or IOT instruction. Each group is processed by a different routine. Tests are made for illegal combinations in operate instructions and, if illegal, are typed out as a four digit octal number. Otherwise they are decoded and typed out as the proper mnemonics. IOT instructions for devices 0-4 only are decoded. Memory reference instructions are decoded into a mnemonic, "I" if indirect, and an address. All references to address "0" are considered illegal. Then if a symbol table has been entered, a search is made for a corresponding address and the symbol is typed. If no corresponding address exists, the absolute value of the difference of the address and the current location counter is taken and if less than 7, the form .±k, where k is the above difference, is typed in place of the address. Otherwise the effective address is typed. Finally an entry is made in the reference table in all cases except .±k address.

The third phase of the program is typing out of the reference table. A new page is started and the message "CROSS REFERENCE TABLE" typed. Then a search is made through all entries of the table for reference to all addresses starting with 0001 and these are typed out as a table. Symbols, if any, are typed for each address. When this is finished the computer halts ready to accept another symbol table.

FORMAT

The symbol table must consist of symbol followed by space or carriage return followed by address followed by space or carriage return for each symbol.

The binary tape should be in standard BIN format. If in RIM format, location 330 should be changed to "NOP" to avoid starting a new page for each location.

The output listing will be almost identical to PAL-III Pass 3 listing, typed 50 lines to an 11 inch page.

The reference table is typed as a reference address followed by eight references per line, with the reference address typed only once for each address. If a symbol table has been entered, the symbols or eight spaces are inserted immediately following the address referenced.

New pages will be started whenever a program relocation statement occurs and at the beginning of the reference table unless there is only one line on the page, and whenever a page contains 50 lines.

EXECUTION TIME

Execution time is limited by the teletype or punch speed with an average of 20 characters per line, except while the reference table is being output. At times the reference table search will take longer than typing a character. The loop takes 11n machine cycles per reference, where n is the number of references between successive references to the address being searched for. This time is highly variable depending on the number of references.

POSSIBLE MODIFICATIONS

Production of a Symbolic Tape For Input to PAL-III

If location 242 is changed to JMP.+4(5246), and location 1600 is changed to CLA HLT (7602), a tape may be produced which can be used as input to PAL-III to reproduce the program just disassembled. In practice this is used to produce a symbolic tape if major modifications have been made by use of ODT and/or switches. The tape may then be further modified with symbolic editor (use tab of 8 instead of 10).

To operate make the above changes and run the program in the normal manner. When it halts at 1601, manually enter a dollar sign and carriage return-line feed. The resulting paper tape is ready to run into PAL-III.

Production of Cross Reference Table Only

A patch is on the binary tape immediately following the main program. If this patch is loaded after the main program only the cross reference table will be produced. Operation of the program is in the normal manner except that if there is a cross reference table overflow, the portion in storage will be typed out and the disassembly continues from there. Message type-out is "CROSS REF TABLE FULL XXXX", where XXXX is the current address of the instruction being disassembled.

PAL-III Pass 3 listing of patch follows on the next page.

```
                                /PATCH FOR DISASSEMBLER
                                /CROSS REFERENCE TABLE ONLY
                                *162
Ø162    7ØØØ                    NOP
                                *215
Ø215    7ØØØ                    NOP
                                *242
Ø242    5247                    JMP .+5
Ø243    1266                    TAD C2ØØ
Ø244    3646                    DCA I C1642
Ø245    5161                    JMP RETURN
Ø246    1642    C1642,          1642
                                *256
Ø256    5161                    JMP RETURN
                                *265
Ø265    5161                    JMP RETURN
Ø266    Ø2ØØ    C2ØØ,           2ØØ
                                *33Ø
Ø33Ø    5335                    JMP .+5
                                *4Ø5
Ø4Ø5    5217                    JMP 417
                                *432
Ø432    5161                    JMP RETURN
Ø433    71ØØ                    CLL
Ø434    53Ø7                    JMP OVRFL
                                *1336
1336    1143                    TAD PC
1337    4Ø2Ø                    JMP OCTYP
134Ø    1143                    TAD PC
1341    3356                    DCA XTYP-1
1342    1346                    TAD .+4
1343    3755                    DCA I I1642
1344    5745                    JMP I .+1
1345    16ØØ                    16ØØ
1346    1347                    .+1
1347    1141                    TAD AXREF
135Ø    3Ø16                    DCA 16
1351    1356                    TAD XTYP-1
1352    3143                    DCA PC
1353    5754                    JMP I .+1
1354    Ø243                    243
1355    1642    I1642,          1642

C1642   Ø246
C2ØØ    Ø266
I1642   1355
```