MISOSYS

DISASSEMBLER

Version II

MISOSYS Disassembler - Disk Version II

General:

The MISOSYS Disassembler is a machine language disassembler that functions with the Radio Shack TRS-80 microcomputer to produce an assembler source code from Z-80 machine language resident in memory. This disassembler operates in two passes in order to incorporate symbolic labels in the source output. The symbolic labels are generated for address and 16-bit numeric references within the start-to-end user disassembly request. References preceding the START address are output as equates (EQU) which can be optionally suppressed.

You are assumed to be familiar with Z-80 assembler mnemonics as specified in the RADIO SHACK EDITOR ASSEMBLER USER INSTRUCTION MANUAL #26-2002. Another good reference manual utilizing the standard ZILOG mnemonics is the Z-80 MICROCOMPUTER HANDBOOK by William J. Barden, Jr. (A Howard W. Sams & Co. publication available in most computer stores). Also, be aware of TRS-80 ASSEMBLY LANGUAGE PROGRAMMING also by William Barden, Jr., available at Radio Shack and other computer or program stores. Many other texts can be located which provide various insights into Z-80 assembly language programming. Do not overlook articles on assembler routines appearing in the magazine and journal media.

You should also understand that data elements and ASCII character strings within the range of disassembly will be intepreted as Z-80 machine instructions. These interpretations, in general, may require corrections to disassembled source after loading into the EDITOR ASSEMBLER.

This version provides a disk file output in two formats. One format is compatible with the Radio Shack Editor Assembler as modified by DISK*MOD (a MISOSYS product) or the Apparat EDTASM version. The other format is compatible with MAC-80, a Microsoft macro-assembler.

Finally, the MISOSYS Disassembler includes two commands to aid you in loading SYSTEM program tapes and locating where in memory the programs load. This provides quite an easy method to determine the START and ENDing locations for the disassembly process.

MISOSYS Disassembler - Disk Version II

Load Instructions:

The MISOSYS Disassembler - Disk Version II is a machine language program supplied on a quality cassette. The program can be loaded using Disk BASIC's SYSTEM command. You can also use CMDFILE or TAPEDISK to transfer the program to a disk file. The cassette contains three (3) versions of the Disassembler with a file name of "DSMBLR" configured as follows:

Program 1 - Loads from 5FFFH (24575D) to 75EFH (30191D), with an ENTRY POINT at 5FFFH.

Program 2 - Loads from 9FFFH (40959D) to B5EFH (46575D), with an ENTRY POINT at 9FFFH.

Program 3 - Loads from DFFFH (57343D) to F5EFH (62959D), with an ENTRY POINT at DFFFH.

> BACKUP PARAMATERS ARE PROVIDED FOR YOUR OWN PERSONAL USE IN MAINTAINING SAFE COPIES OF YOUR MISOSYS DISASSEMBLER. YOU SHOULD NOT PROVIDE COPIES TO OTHERS.

The memory region immediately preceding the program is used as a stack area and a disk output buffer. The memory region immediately following the program is used for storage of the program's variables and the symbolic label address buffer.

Transferring the Cassette Program to Disk:

All versions of the Disassembler can be transferred to disk as a "/CMD" file by using the TRSDOS "TAPEDISK" utility or other command file utility such as CMDFILE. The TAPEDISK steps are reproduced here for your convenience.

```
DOS READY
TAPEDISK <ENTER>
?C
?F DSMBLR2/CMD:0 5FFF 75DD 5FFF  (16 k version)
(the disk file will be created)
?E
DOS READY
```

Please note that if you are using a single drive system, you still must specify drive 0 in the filespec. Also, 32k or 48k parameters may be substituted in the above "F" command depending on which version you want to transfer.

Control Function Command Summary:

D - Return control to DOS at X'402D'

C - Clear the symbol table buffer

E - Switch the state of the EQUATE flag

S - Load a SYSTEM program & display load points

T - Determine load points of a SYSTEM program

ENTER - Exit from Control Function

Output Command Summary:

S - Output to Screen (Video Display)

T - output to Tape Cassette

P - Output to Line Printer

D - Output to Disk File - EDTASM format

M - Output to Disk File - MAC-80 format

R - Output review (continuous scroll until paused)

Special Control Functions:

CLEAR - Logical interrupt for a prompt

BREAK - Interrupt of command request entries

SHIFT @ - Pause during continuous scroll.

Control Function Details:

D - Command

This command is used to return control to the DOS command interpreter. A jump to address 402DH is performed. the "DOS READY" message will be displayed.

C - Command

Since this is a two-pass disassembler, the first pass builds a table used for the generation of the symbolic labels. The first pass is performed only when the symbol table buffer region is "cleared". By issuing the "C" command the buffer is cleared and the following message is displayed:

Symbol table cleared

E - Command

It is common practice to define program constants and address references to other programs at the front end of a source program by means of equate statements (with the assembler pseudo-op, EQU). When the target program contains address references that precede the start-of-disassembly, these references will be output as EQU statements. You may choose to suppress the generation of equates in the disassembler's output by using this command. Equate generation will be either on or off. A flag control is used to indicate the ON or OFF mode. You reverse the flag's status each time you enter the "E".

S - Command

This command operates similar to BASIC's "SYSTEM" command. It will load a SYSTEM program into memory. However, in contrast to the nonexistant information supplied by the SYSTEM command, the "S" command will identify the program's FILENAME, its STARTing address, its ENDing address, and its TRANSFER address (the location that control will be transfered to after loading a SYSTEM program via the SYSTEM command and issuing the "/" <ENTER>). The program's FILENAME will be displayed as it is read from the tape. The address information will be displayed in the message:

START=xxxx, END=yyyy, TRANSFER=zzzz

where xxxx, yyyy, and zzzz are displayed in hexadecimal. Also, if the program loads without a checksum error, the START and END variables will be retained for automatic use in the disassembly.

T - Command

The "Test" command operates just like the "S" control command. However, since you may want to discover the address load information without physically loading the program, this command will do just that. The information is identified but the program is not loaded into memory. the START and END variables are

updated.

Disassembly Address Prompts:

Whenever you exit the Control Function prompts, you will be prompted to enter the storage locations of the program you want to disassemble. The addresses are entered in hexadecimal. Full line input control keys (backspace, line delete, etc.) are supported as in BASIC or DOS command input. In addition, you may enter the value without leading zeroes (0000 as 0, 06CC as 6CC, etc.). These prompts appear as follows:

START ADDRESS - Enter the memory address at which the disas- sembly should begin. This will be the first memory location that will be disassembled. If the "S" control command was used to load a SYSTEM program, this value would be automatically set to the program's START address.

END ADDRESS - The memory address at which disassembly should cease (Note that disassembly will run from START up to but not including END so END should be one memory position beyond where you want to stop the disassembly). Similar to START, this vari- able will be set to one greater than the "END" address if the program to disassemble was loaded with the "S" control command.

RELOC ADDRESS - If you had to move the program that you are disassembling (termed the target program) to an address area different from where it originally loaded because it woud have overlayed (loaded into the same region as) the Disassembler, the original START address should be entered here. For example, if the target program originally loaded from 5000H through 5500H and you moved it to load at 7000H to 7500H, then use START=7000, END=7500H, RELOC=5000H. This feature is useful to recover proper address references to code that may have been relocated to a higher or lower address in order to eliminate conflict with the load point of the Disassembler. Three different Disassemblers are provided to further ease conflicts with target programs under disassembly.

Address entries are retained by the program until changed by entering new values. Therefore, subsequent disassemblies using previously entered address information can be performed just by depressing the <ENTER> key. Also, responses to three address prompts may be entered on one line by separating each with a comma. For example:

Start Address = >150,400,150

will input starting address of X'150', ending address of X'400', and relocation address of X'150' (a relocation address of X'150' would also be used by omitting the relocation entry and depressing <ENTER> in response to the "Reloc address" query).

The SYMBOL table is regenerated only when the table is cleared using the control function, "C". Thus, shifting from one disassembly output command to another generates output rapidly. In addition, the Symbol table is not cleared when the Disassembler first loads. This provides a fast "review" capability since the first pass used to generate the symbol table, is bypassed.

Command Details:

The output device to receive the disassembly is determined in response to the prompt:

Output: Review, Screen, Printer, Tape, Disk
(R,S,P,T,D/M)? >

Select one of the devices by entering its respective letter.

S Command - Screen (Video Monitor) output:

The screen output is directed to the CRT. Output is scrolled for 16 lines, then paused. The next 16 lines commence scrolling upon depression of any keyboard key except <CLEAR> and <BREAK>. Depressing <CLEAR> will interrupt output and return you to the prompting message.

The output consists of the following references:

1. Effective memory address of the instruction.

2. Contents of memory starting from the instruction's physical memory location for as many bytes as the instruction's length. Output is in hexadecimal.

3. Sequential line number, in decimal, starting from 00001 and incremented by one (1).

4. A SYMBOLIC LABEL, where referenced as a 16-bit or relative value by the program to be disassembled, consisting of the ad- dress referenced preceded by the letter "Z".

5. Disassembled instruction using Radio Shack (same as

ZILOG) mnemonics. The tab character between the OP code and the OPERAND is expanded for screen display.

6. Character output (in ASCII) of the instruction's hexadecimal values. Bit 7 is stripped from each byte prior to display in order to better identify character strings that utilize bit 7 for "begin-string" or "end-string" detection. Non-printable characters are converted to a period.

T - Tape Output:

This command will create a source cassette tape suitable for loading into the Radio Shack Editor Assembler using its' "L" command (using a version that still permits cassette tape input). After entering the Tape command, you will be prompted to prepare the cassette for writing with the message:

Ready cassette

Depression of the <ENTER> key will cause the disassembly to start. The output consists of:

1. The 5-digit ASCII line number,

2. The SYMBOLIC LABEL (or tab if a label is not required),

3. The disassembled instruction. The tab character between the OP code and the OPERAND is not expanded.

The tape is created in blocks consisting of 256 lines of output per block. File names are assigned sequentially. The first is "BLOCKA", the second is "BLOCKB", etc., incrementing the sixth character by one letter for each block. A five (5) second blank segment is written between each block to provide a manual search capability. An asterisk (*) blinks in the upper right hand corner of the screen (3C3FH) for every two lines of output. The starting address of the block will be output to the screen. Depressing the <CLEAR> key will interrupt the tape output only during the period of asterisk blinking.

P - Printer Output:

This command will provide the same output as the "S" command except that the output is directed to the LINE PRINTER. The output is printed 50 lines per page. Each page is numbered sequentially starting from one (1) and incremented by one (1). A heading which labels each column is provided on each page. The MISOSYS Disassembler fully supports the Centronic 779 Line

Printer as used by Radio Shack. Any other printer compatible to the Centronic 779, should also function.

RS232 serially driven printers may function only after ensuring that the driver routine maintains the line counter at address 4029H (16425D). The line counter is automatically incremented by the printer driver routine in ROM whenever a carriage return (0DH or 13D) is sent to the printer. Disassemble the ROM region from 58DH through 5D8H to examine the line printer driver routine. You must also patch your Printer driver routine into the standard Printer Data Control Block at 4026H & 4027H.

When the printer command is entered, the program will request you to enter a title and position the printer to receive. The prompt:

"Ready printer and enter title"

will be output. You may enter a title of up to twelve (12) characters which will be placed in the heading on each page of printed output. After depressing <ENTER> following the title, the disassembly will automatically start. By depressing the <CLEAR> key at any time during the printing, the output will be interrupted and you will return to the prompt message.

It has been ascertained that some printers (including the Centronic 779) print 67 lines prior to the form feed when reacting with the BASIC ROM printer driver routine. This is apparently due to some ROMs initializing the number of lines per page (4028H or 16424D) to a value of 43H (67D). If this is the case with your printer, perform the following operation when in BASIC:

POKE 16424,66 (4028H,42H)

This will condition the driver routine properly for your printer to print 66 lines per page (standard 11 inch pages). The RAM location (printer device control block) contains the number of lines per page which is initialized by BASIC to 67; 67 is the proper number (?) for only some printers.

D - Disk Output (EDTASM compatible):

This command provides the capability of generating a source disk file which can be loaded into the Radio Shack Editor Assembler as modified by DISK*MOD, a MISOSYS product, or the Apparat EDTASM version. You will be prompted for the filespec with the prompt:

Filespec?

After entering the desired filespec, the source file will be created. If the specified file already exists, it will be replaced with the disassembled source and the message:

Replaced!

will be displayed. If the file is non-existant, then a new file will be created and the message:

New File!

will be displayed.

Note that a disassembly will produce only one output file. It is entirely possible that a disassembly will create a file larger than will load into your EDTASM depending on your system's memory configuration. A range of 800 to 1000 lines of code can be loaded into each 10,000 bytes of memory. A disassembly output first to the screen will provide the information necessary to decide if disassembly segmentation is needed. If segmentation is required, clear the symbol table then disassemble the entire program. This will generate the entire symbol table needed for label construction. Next, disassemble pieces of the program by altering the START and END addresses so that each piece, or segment, does not exceed your Editor Assembler's text buffer region. You may suppress the EQUATE generation on all files except the first depending on your preference.

M - Disk Output (Microsoft MAC-80 compatible)

This output command creates a source disk file in a manner similar to the "D" command. However, by using the "M" command, no file header will be written and each label will be followed by a colon (:), conforming to MAC-80 format.

Developing a Source tape:

The best way to employ the power of the MISOSYS Disassembler in order to create a "SOURCE" program, the following steps should be performed:

1. Determine the boundaries of the machine language program. This can be accomplished by loading the SYSTEM tape into memory with the "S" control command. Since it is possible that the target program may load into the same region as the Disassembler, you will find that a better procedure is to use the "T"

control command first. The START and END values will automatically be initialized to those determined from the program tape itself. If you are disassembling your ROM, consult the memory map in your Level II manual.

2. Disassemble to the screen or printer to detect regions that may have been character strings or data. If you do not have a printer, make note of these regions on scratch paper.

3. Follow up with a "T" command disassembly to generate the SOURCE tape or use the "D" command to write a source disk file.

4. Load the SOURCE tape or disk file into the Editor Assembler using its' "L" command.

5. Using the ASCII equivalents from a printed listing, ascertain any character strings and convert them to "DEFM" instuctions. If you do not have a printer, note logical ASCII sections as identified from a Screen output.

6. Make an attempt to scrutinize the listing for code sequences that make little sense. As you become more experienced with Z-80 assembler code, this will become an easier task. Illogical sequences are probably data areas. These "data areas" would best be cleaned up by converting them to "DEFB" or "DEFW" instructions.

Comments concerning this program may be directed to MISOSYS at the following address:

MISOSYS
5904 Edgehill Drive
Alexandria, Va. 22303
703-960-2998

* * * N O T I C E * * *

* * * L I M I T E D W A R R E N T Y * * *

MISOSYS shall have no liability or responsibility to the purchaser or any other person, company, or entity with respect to any liability, loss, or damage caused or alleged to have been caused by this product, including but not limited to any interruption of service, loss of business and anticipatory profits, or consequential damages resulting from the operation or use of this program.

Should this program recording or recording media prove to be defective in manufacture, labeling, or packaging, MISOSYS will replace the program upon return of the program package to MISOSYS within 90 days of the date of purchase. Except for this replacement policy, the sale or subsequent use of this program material is without warrenty or liability.

* * * W A R N I N G * * *