Z-80 DisAssembler©

INTRODUCTION

The Z-80 DisAssembler is a programming aid for the documentation of hand-coded machine language programs. As such, it can also be a useful learning tool for someone who is upgrading from an 8080 based system to a Z-80 based system.

The Z-80 DisAssembler is somewhat more than just a typical disassembler. It has a number of capabilities which should be useful in the documentation of programs. It will operate in either the split-octal mode or the hexadecimal mode. Output is generated for either video-monitor based systems or printer based systems. It will read in and decode a cassette tape with unknown contents and, finally, accept an appropriate offset address for use in the decoding process to facilitate reading the output.

The commands for the Z-80 DisAssembler fall into three categories or groups: DECODER options which control the type of output, DISPLAY options which control the number base of the output and SET-UP options which are used in the preparation process prior to disassembling..

When the DisAssembler program begins execution the following "shopping-list" should appear on the output device:

```
   * SELECT  OPTION *
 << DECODER  OPTIONS >>
A = ASCII CHARACTER
D = DUMP 8 BYTES/LINE
S = SYMBOLIC INSTRUCTIONS
 << DISPLAY  OPTIONS >>
O = OCTAL MODE
H = HEXADECIMAL MODE
  << SET-UP OPTIONS >>
R = READ PROGRAM TAPE
F = SET RELATIVE OFFSET
V = TV-MONITOR OUTPUT ONLY
P = TV-MONITOR AND PRINTER
? = PRINT COMMAND LIST

COMMAND=
```

The "shopping-list" will be output only once automatically, to obtain another copy simply key a question mark.

NOTE: All inputs to the Z-80 DisAssembler are terminated with a carriage-return (Ø15 or 215 Octal; ØD or 8D Hexadecimal).

DECODER OPTIONS

The Z-80 DisAssembler has three different decoder options to provide as much flexibility as possible to the user. In all three options, whenever a memory address is displayed, it is shown according to the current setting of the display option (e.g., split-octal or hexadecimal). Likewise, since addresses must first be entered specifying which areas of memory are to be decoded, the input addresses must be entered according to the current display option.

Whenever the user selects one of the DECODER options, the DisAssembler will request a series (up to 16) of starting and ending address values. The user then enters pairs of starting and ending addresses in the appropriate notational form depending upon the DISPLAY option in force. The input is checked to determine that the keyed digits are valid for the current DISPLAY option and that the ending address is greater than the starting address. It is possible to overlap areas to be displayed. The DisAssembler will continue to request STADDR and NDADDR pairs until 16 pairs have been entered at which point it goes into automatic execution. Should the user wish to enter less than 16 pairs, a response of C/R (Carriage-Return) to a STADDR request will initialize the execution.

Samples of address pair entry are shown with each of the DECODER option descriptions.

A - ASCII Character:

The ability to see the contents of memory, other than as a straight jump or symbolic disassembly, is often useful. The A-ASCII Character option produces a formatted listing of the ASCII character contents of memory. This is helpful in determing the contents of memory when they are to be printable characters.

The Digital Group (DGI) TV character generator ROM will generate a "printable" character for 127 of the 128 ASCII character values. However, some of these values have other meanings such as line-feed,carriage-return, delete, etc. To facilitate an analyses of the contents of memory in ASCII, these special characters and the "spare" character will be designated as a two-character printout in lower-case for those bytes where the 2^7 bit is zero and upper-case when it is one. These characters would appear as follows:

	2^7=Ø		2^7=1	
CHARACTER	OCT/HX	GRAPHIC	OCT/HX	GRAPHIC
LINE FEED	Ø14/ØC	lf	214/8C	LF
CARR RETN	Ø15/ØD	cr	215/8D	CR
BACK ARROW	Ø33/1B	ba	233/9B	BA
SPACE	Ø4Ø/2Ø	sp	24Ø/AØ	SP
DELETE	177/7F	dl	377/FF	DL

All other characters are printed to the TV-monitor as their appropriate graphics preceeded by a space when 2^7=Ø or preceeded by a dash (-) when 2^7=1:

CHARACTER	2^7=Ø OCT/HX	GRAPHIC	2^7=1 OCT/HX	GRAPHIC
A	1Ø1/41	A	3Ø1/C1	-A
a	141/61	a	341/E1	-a
-	Ø55/2D	-	255/AD	--

Hardcopy printer-driver routines perform a close substitution when the device does not have the appropriate graphic in its character set such as lower-case alphabetics on a TTY. Typically, an ASCII display of the "Shopping List" area of the DisAssembler would appear as follows on an ASCII TTY ASR-33:

```
COMMAND=C
COMMAND=A
STADDR=030300
NDADDR=031157
STADDR=
030300 -. SP SP SP -* SP -S -E
030310 -L -E -C -T SP SP -O -P
030320 -T -I -O -N SP -* CR SP
030330 -< -< SP -D -E -C -O -D
030340 -E -R SP SP -O -P -T -I
030350 -O -N -S SP -> -> CR -A
030360 SP -= SP -A -S -C -I -I
030370 SP -C -H -A -R -A -C -T
031000 -E -R CR -D SP -= SP -D
031010 -U -M -P SP -8 SP -B -Y
031020 -T -E -S -/ -L -I -N -E
031030 CR -S SP -= SP -S -Y -M
031040 -B -O -L -I -C SP -I -N
031050 -S -T -R -U -C -T -I -O
031060 -N -S CR SP -< -< SP -D
031070 -I -S -P -L -A -Y SP SP
031100 -O -P -T -I -O -N -S SP
031110 -> -> CR -O SP -= SP -O
031120 -C -T -A -L SP -M -O -D
031130 -E CR -H SP -= SP -H -E
031140 -X -A -D -E -C -I -M -A
031150 -L SP -M -O -D -E CR
```

```
COMMAND=H
COMMAND=A
STADDR=18C0
NDADDR=196F
STADDR=
18C0 -. SP SP SP -* SP -S -E
18C8 -L -E -C -T SP SP -O -P
18D0 -T -I -O -N SP -* CR SP
18D8 -< -< SP -D -E -C -O -D
18E0 -E -R SP SP -O -P -T -I
18E8 -O -N -S SP -> -> CR -A
18F0 SP -= SP -A -S -C -I -I
18F8 SP -C -H -A -R -A -C -T
1900 -E -R CR -D SP -= SP -D
1908 -U -M -P SP -8 SP -B -Y
1910 -T -E -S -/ -L -I -N -E
1918 CR -S SP -= SP -S -Y -M
1920 -B -O -L -I -C SP -I -N
1928 -S -T -R -U -C -T -I -O
1930 -N -S CR SP -< -< SP -D
1938 -I -S -P -L -A -Y SP SP
1940 -O -P -T -I -O -N -S SP
1948 -> -> CR -O SP -= SP -O
1950 -C -T -A -L SP -M -O -D
1958 -E CR -H SP -= SP -H -E
1960 -X -A -D -E -C -I -M -A
1968 -L SP -M -O -D -E CR
```

D - Dump 8 Bytes/Line:

The DUMP decoder option provides the capability to examine the contents of memory in its raw form. DUMP will display in either split-octal or hexadecimal notation (depending upon the current setting the of DISPLAY option) the contents of selected memory areas.

Unlike the other DECODER options, DUMP's output varies depending upon whether the DisAssembler is driving the TV-Monitor-only or whether a hard copy is being produced. In the TV-Monitor-only mode, the address of the first byte in a DUMPed octad appears on one line and the DUMPed values on the next. In the hard-copy mode, the address and the data are all on one line on the hardcopy device.

A sample of a DUMP of the same area of memory as displayed by the ASCII DECODER is as follows:

```
COMMAND=O
COMMAND=D
STADDR=030300
NDADDR=031157
STADDR=
030300   256 240 240 240 252 240 323 305
030310   314 305 303 324 240 240 317 320
030320   324 311 317 316 240 252 215 240
030330   274 274 240 304 305 303 317 304
030340   305 322 240 240 317 320 324 311
030350   317 316 323 240 276 276 215 301
030360   240 275 240 301 323 303 311 311
030370   240 303 310 301 322 301 303 324
031000   305 322 215 304 240 275 240 304
031010   325 315 320 240 270 240 302 331
031020   324 305 323 257 314 311 316 305
031030   215 323 240 275 240 323 331 315
031040   302 317 314 311 303 240 311 316
031050   323 324 322 325 303 324 311 317
031060   316 323 215 240 274 274 240 304
031070   311 323 320 314 301 331 240 240
031100   317 320 324 311 317 316 323 240
031110   276 276 215 317 240 275 240 317
031120   303 324 301 314 240 315 317 304
031130   305 215 310 240 275 240 310 305
031140   330 301 304 305 303 311 315 301
031150   314 240 315 317 304 305 215 000
```

```
COMMAND=H
COMMAND=D
STADDR=18C0
NDADDR=196F
STADDR=
18C0   AE A0 A0 A0 AA A0 D3 C5
18C8   CC C5 C3 D4 A0 A0 CF D0
18D0   D4 C9 CF CE A0 AA 8D A0
18D8   BC BC A0 C4 C5 C3 CF C4
18E0   C5 D2 A0 A0 CF D0 D4 C9
18E8   CF CE D3 A0 BE BE 8D C1
18F0   A0 BD A0 C1 D3 C3 C9 C9
18F8   A0 C3 C8 C1 D2 C1 C3 D4
1900   C5 D2 8D C4 A0 BD A0 C4
1908   D5 CD D0 A0 B8 A0 C2 D9
1910   D4 C5 D3 AF CC C9 CE C5
1918   8D D3 A0 BD A0 D3 D9 CD
1920   C2 CF CC C9 C3 A0 C9 CE
1928   D3 D4 D2 D5 C3 D4 C9 CF
1930   CE D3 8D A0 BC BC A0 C4
1938   C9 D3 D0 CC C1 D9 A0 A0
1940   CF D0 D4 C9 CF CE D3 A0
1948   BE BE 8D CF A0 BD A0 CF
1950   C3 D4 C1 CC A0 CD CF C4
1958   C5 8D C8 A0 BD A0 C8 C5
1960   D8 C1 C4 C5 C3 C9 CD C1
1968   CC A0 CD CF C4 C5 8D 00
```

S - Symbolic Instruction:

Generally, the most useful documentation aid for the hand coder is a SYMBOLIC INSTRUCTION DisAssembler. The DGSS Z-80 DisAssembler SYMBOLIC INSTRUCTION option decodes the contents of memory into a close replica of what the input to the Z-80 Assembler would be...assuming, of course, the the Assembler input specifies hard-addresses rather than symbolic-addresses...and, assuming that the proper address alignment is given.

Care must be used in specifying STADDR values to insure that the input address is the address of the first byte of a valid instruction. It is imperative to remember that in the Z-80, all 256 possible byte values are valid first bytes for instructions and will be decoded as such. For example, the following is a decoding of the same shopping list print area as is shown in both the ASCII and DUMP mode:

```
COMMAND=O
COMMAND=S
STADDR=030300
NDADDR=030377
STADDR=
030300 256          XOR  (HL)
030301 240          AND  B
030302 240          AND  B
030303 240          AND  B
030304 252          XOR  D
030305 240          AND  B
030306 323 305      OUT  305
030310 314 305 303  CALL Z,303305
030313 324 240 240  CALL NC,240240
030316 317          RST  08
030317 320          RET  NC
030320 324 311 317  CALL NC,317311
030323 316 240      ADC  240
030325 252          XOR  D
030326 215          ADC  L
030327 240          AND  B
030330 274          CP   H
030331 274          CP   H
030332 240          AND  B
030333 304 305 303  CALL NZ,303305
030336 317          RST  08
030337 304 305 322  CALL NZ,322305
030342 240          AND  B
030343 240          AND  B
030344 317          RST  08
030345 320          RET  NC
030346 324 311 317  CALL NC,317311
030351 316 323      ADC  323
030353 240          AND  B
030354 276          CP   (HL)
030355 276          CP   (HL)
030356 215          ADC  L
030357 301          POP  BC
```

```
COMMAND=H
COMMAND=S
STADDR=18C0
NDADDR=18FF
STADDR=
18C0 AE          XOR  (HL)
18C1 A0          AND  B
18C2 A0          AND  B
18C3 A0          AND  B
18C4 AA          XOR  D
18C5 A0          AND  B
18C6 D3 C5       OUT  C5
18C8 CC C5 C3    CALL Z,C3C5
18CB D4 A0 A0    CALL NC,A0A0
18CE CF          RST  08
18CF D0          RET  NC
18D0 D4 C9 CF    CALL NC,CFC9
18D3 CE A0       ADC  A0
18D5 AA          XOR  D
18D6 8D          ADC  L
18D7 A0          AND  B
18D8 BC          CP   H
18D9 BC          CP   H
18DA A0          AND  B
18DB C4 C5 C3    CALL NZ,C3C5
18DE CF          RST  08
18DF C4 C5 D2    CALL NZ,D2C5
18E2 A0          AND  B
18E3 A0          AND  B
18E4 CF          RST  08
18E5 D0          RET  NC
18E6 D4 C9 CF    CALL NC,CFC9
18E9 CE D3       ADC  D3
18EB A0          AND  B
18EC BE          CP   (HL)
18ED BE          CP   (HL)
18EE 8D          ADC  L
18EF C1          POP  BC
```

Obviously, unless the computer has a very large memory, the examples sited on the preceding page are not in an instruction area of memory. Actually, a batch of pseudo-source code, like the preceding example, is a good clue that there are some ASCII character constants (with 2^7=1) present while an apparently random group of LD r,r type commands with the B, C and D registers as destinations indicate the presence of strings of ASCII character values with 2^7=Ø.

Providing that the user knows what is being decoded, there is usually no problem except where data is mixed with instructions. Although Z-80 instructions vary in length from one to four bytes long, a majority of the instructions in a given program tend to be one or two bytes long and, therefore, even when the DECODER gets out of synchronization with the program it will usually realign itself with a few bytes.

The following are examples of decoded SYMBOLIC INSTRUCTIONS. It is the section of the DisAssembler which analyzes the command which the user enters:

```
COMMAND=D
COMMAND=S
STADDR=012100
NDADDR=012130
STADDR=
012100 072 310 010 LD   A,(010310)
012103 006 012     LD   B,012
012105 041 030 032 LD   HL,032030
012110 276         CP   (HL)
012111 050 010     JR   Z,010       *012123*
012113 043         INC  HL
012114 043         INC  HL
012115 043         INC  HL
012116 020 370     DJNZ 370       *012110*
012120 303 046 012 JP   012046
012123 043         INC  HL
012124 136         LD   E,(HL)
012125 043         INC  HL
012126 126         LD   D,(HL)
012127 353         EX   DE,(HL)
012130 351         JP   (HL)

COMMAND=H
COMMAND=S
STADDR=0A40
NDADDR=0A58
STADDR=
0A40 3A C8 08 LD   A,(08C8)
0A43 06 0A    LD   B,0A
0A45 21 18 1A LD   HL,1A18
0A48 BE       CP   (HL)
0A49 28 08    JR   Z,08       *0A53*
0A4B 23       INC  HL
0A4C 23       INC  HL
0A4D 23       INC  HL
0A4E 10 F8    DJNZ F8       *0A48*
0A50 C3 26 0A JP   0A26
0A53 23       INC  HL
0A54 5E       LD   E,(HL)
0A55 23       INC  HL
0A56 56       LD   D,(HL)
0A57 EB       EX   DE,(HL)
0A58 E9       JP   (HL)
```

DISPLAY OPTIONS

There are two DISPLAY OPTIONS provided by the Z-80 DisAssembler: OCTAL (meaning split-octal) and HEXADECIMAL. There is no readily apparent effect in selecting one of these options becuase there is a call for another command immediately. However, the chosen option does cause a flag to be set which controls the format of all DUMPed characters.

DUMPed Mode characters include address components in all decode options, instruction op-codes, operands and components in the SYMBOLIC INSTRUCTION decode option and, of course, the contents of memory in the DUMP option.

The DISPLAY options are:

Ø = OCTAL MODE

H = HEXADECIMAL MODE

THE SET-UP OPTIONS

There are four SET-UP OPTIONS and a special command in the SET-UP OPTIONS list. The purpose of the SET-UP OPTIONS is to enable the user to manipulate the operation of the DisAssembler. With the exception of the SET RELATIVE OFFSET command, the commands are fairly self-explanatory as demonstrated in the following example:

R = READ PROGRAM TAPE

This command is used to read in an audio cassette containing recorded data for subsequent disassembly. The DisAssembler reads the data into memory beginning at Ø34/ØØØ Octal or 1CØØ Hexadecimal. When the user keys in R(C/R) as his command, the Dis Assembler responds as shown in the example below:

```
COMMAND=R
START CASSETTE THEN (RETURN)
STADDR=001000
COMMAND=D
STADDR=001000
NDADDR=001007
STADDR=
001000  123 123 303 000 000 303 000 000
```

When the START CASSETTE THEN (RETURN) message appears, start the cassette. As soon as the tone stabilizes, hit RETURN. The program will read in the data up to the next leader tone and then return control to the user by printing out STADDR=. The user should respond by entering the true starting address of the data which was read in relative to itself. In other words, if the cassette which read in is a normal bootstrap load cassette program, respond ØØ1 ØØØ. The Dis Assembler automatically computes all of the required offsets to allow the user to specify starting and ending addresses relative to the data rather than to the system.

F = SET RELATIVE OFFSET

In order to DisAssemble data with the correct real addresses, it is necessary to inform the DisAssembler of the real addresses of the data to be DisAssembled. This address is always given relative to the DisAssembler read-in area at Ø34 ØØØ Octal or 1CØØ Hexadecimal. Thus, to disassemble the DisAssembler itself in situ without reading it into the read-in area, set the relative offset to Ø34 ØØØ or 1CØØ.

The example shown below corresponds to the example shown in the READ PROGRAM TAPE option. In this case, the offset has been set to 034/000. Notice that the area dumped contains the same data as shown in the READ PROGRAM TAPE example.

```
COMMAND=O
COMMAND=F
STADDR=034000
COMMAND=D
STADDR=034000
NDADDR=034007
STADDR=
034000  123 123 303 000 000 303 000 000
COMMAND=V
```

V = TV-MONITOR OUTPUT ONLY

The TV-MONITOR OUTPUT ONLY option shuts off all output to the printer and, therefore, speeds up the display considerably. In addition, it alters slightly the output of the DUMP function in the OCTAL MODE in order to cause the eight data bytes to be shown on one line. The V option overrides the selected option at operating-system-option-selection time. The sample shown below was printed by starting the DisAssembler with option 8 while the internal mode of the Dis-Assembler was V:

```
COMMAND=O
COMMAND=D
STADDR=030300
NDADDR=031147
STADDR=
030300
256 240 240 240 252 240 323 305
030310
314 305 303 324 240 240 317 320
030320
324 311 317 316 240 252 215 240
030330
274 274 240 304 305 303 317 304
030340
305 322 240 240 317 320 324 311
030350
317 316 323 240 276 276 215 301
030360
240 275 240 301 323 303 311 311
030370
```

P = TV-MONITOR AND PRINTER

The TV-MONITOR AND PRINTER option sets a flag for the DUMP-OCTAL function which causes the data to be printed out on one line. Primarily, it enables the printer-control-logic in the output program. The P option overrides the operating system selected option.

Many users will not have a printer of any kind and, therefore, will wonder how this option can be used for them? The best advice which can be given is to try the P option...especially the Baudot version as this option slows down the output to a good reading speed.

? = PRINT COMMAND LIST

If you have left your instructions in the other room and cannot remember what the commands are, type ? for the list. If you can't even remember this, type anything and the DisAssembler will tell you what to do.