ISTITUTO NAZIONALE DI FISICA NUCLEARE
Laboratori Nazionali di Frascati

LNF-81/31(NT)
3 Giugno 1981

L. Trasatti:

A DISASSEMBLER FOR TEXAS 9900 MICROCOMPUTERS

Servizio Documentazione
dei Laboratori Nazionali di Frascati
Cas. Postale 13 - Frascati (Roma)

INFN - Laboratori Nazionali di Frascati
Servizio Documentazione

LNF-81/31(NT)
3 Giugno 1981

L. Trasatti:

A DISASSEMBLER FOR TEXAS 9900 MICROCOMPUTERS.

Interpretation and modification of programs bought directly on firmware (EPROM) is an extremely frustating job due to the difficulty of interpreting object code. In the process of trying to understand better the TM990 POWER BASIC interpreter, this limitation suggested to write a program to restitute assembly language code from object code as it appears in memory.

The program has been written using the TM990 POWER BASIC itself, on a microcomputer built of a 990/100 CPU board, a 990/210 memory expansion board and a 990/302 Software Development board.

The program reads the object code to be disassembled directly from a portion of memory specified at run time and directs the output list to a printer or VDU terminal.

The output format consists of 4 fields:

1 : The disassembled code in TM990 Assembler standard code, with the exception of the jump statements, which are printed in the form:

JMP Lmmmm, (=nn)

where mmmm is the memory location to which a jump occurs, and nn is the number to be added to the program counter divided by two.

2 : The memory address of the first word of the instruction.

3 : The object code for the disassembled instruction (one or more words).

4 : The ASCII equivalent (if it exists) for each byte of the object code.

The program has succesfully been used to disassemble the Basic Interpreter.

No optimization has been attempted as far as speed is concerned, since anyway the limiting factor for such a program is the speed of the terminal. Instead, clear and understandable code has been a design goal.

A listing of the program follows as well as an example of output.

I wish to thank dr. M. Ferrer for continuing help and incoiragement.

```
LIS
 10  REM NEW 0C000H
 20  REM DISASSEMBLER
 30  REM
 35  DIM OP[1],AS[1]
 40  INPUT "MEM START",M,"      MEM STOP",ME
 100  IF M>ME THEN STOP
 105  PRINT  TAB (6)
 110  A=MEM[M]
 120  A1=MEM[M+1]
 125  M0=M
 126  ABI=0
 128  IF BIT[A,25]=1 THEN ABI=1:: BIT[A,25]=0
 130  AA=A1+A*16*16
 135  IF ABI=1 THEN BIT[A,25]=1:: GOTO 9000
 140  IF A<2 THEN GOTO 2000
 150  GOTO 3000
 1000  REM
 1010  REM  PRINT SUBROUTINES
 1020  REM
 1030  R=AA-(AOP*16)
 1040  IF R<10 THEN PRINT $OP[0]; TAB (12);#"R9"R;
 1050    ELSE PRINT $OP[0]; TAB (12);#"R99"R;
 1060  RETURN
 1100  PRINT  TAB (36);#,M0;"    ";#;A;#;A1;
 1110  RETURN
 1200  PRINT "  ";#;MEM[M];#;MEM[M+1];
 1210  RETURN
 1300  REM IOP1
 1310  REM
 1320  M=M+2
 1330  PRINT ">";#;MEM[M];#;MEM[M+1];
 1340  RETURN
 1400  REM
 1410  REM REG TYPE
 1420  REM
 1430  PRINT  TAB (12)
 1440  IF T=0 THEN GOTO 1600
 1450  IF T=2 THEN GOTO 1500
 1460  PRINT "*";
 1470  GOTO 1600
 1500  M=M+2
 1510  IOP=MEM[M]
 1520  IOQ=MEM[M+1]
 1530  PRINT "@>";#;IOP;#;IOQ;
 1540  IF R=0 THEN RETURN
 1550  IF R<10 THEN PRINT "(R";#"9"R;")";
 1560    ELSE PRINT "(R";#"99"R;")";
 1570  RETURN
 1600  IF R<10 THEN PRINT "R";#"9"R;
 1610    ELSE PRINT "R";#"99"R;
 1620  IF T=3 THEN PRINT "+";
 1630  RETURN
```

```
1700  MA=A
1710  MB=A1
1720  IF MA<020H OR MA>05DH THEN MA=02EH
1730  IF MB<020H OR MB>05DH THEN MB=02EH
1740  $AS[0]=%MA%MB%0
1750  RETURN
1800  MA=MEM[M]
1810  MB=MEM[M+1]
1820  IF MA<020H OR MA>05DH THEN MA=02EH
1830  IF MB<020H OR MB>05DH THEN MB=02EH
1840  $AS[0]=$AS[0]+%MA%MB%0
1850  RETURN
1900  PRINT  TAB (62);$AS[0];
1910  RETURN
2000  REM
2010  REM    DATA
2020  REM
2030  PRINT "DATA  >";$;A;$;A1;
2040  GOSUB 1100
2050  GOSUB 1700
2060  GOSUB 1900
2070  M=M+2
2080  PRINT
2090  GOTO 100
3000  REM
3010  REM FORMAT 8
3020  REM
3030  AOP=INP[AA/32]*2
3040  IF AOP>030H THEN GOTO 4000
3050  IF AOP=02AH THEN $OP[0]="STWP  ":: GOTO 3500
3060  IF AOP=02CH THEN $OP[0]="STST  ":: GOTO 3500
3070  IF AOP=022H THEN $OP[0]="AI    ":: GOTO 3900
3080  IF AOP=024H THEN $OP[0]="ANDI  ":: GOTO 3900
3090  IF AOP=026H THEN $OP[0]="ORI   ":: GOTO 3900
3100  IF AOP=028H THEN $OP[0]="CI    ":: GOTO 3900
3110  IF AOP=020H THEN $OP[0]="LI    ":: GOTO 3900
3120  IF AOP=02EH THEN $OP[0]="LWPI  ":: GOTO 3900
3130  IF AOP=030H THEN $OP[0]="LIMI  ":: GOTO 3900
3140  GOTO 2000
3500  GOSUB 1000
3510  GOSUB 1100
3520  GOSUB 1700
3530  GOSUB 1900
3540  M=M+2
3550  PRINT
3560  GOTO 100
3900  GOSUB 1000
3910  PRINT ",";
3920  GOSUB 1300
3930  GOSUB 1100
3940  GOSUB 1200
3950  GOSUB 1700
3960  GOSUB 1800
3970  GOSUB 1900
3980  PRINT
```

```
3990  M=M+2
3995  GOTO 100
4000  REM
4010  REM FORMAT 7
4020  REM
4030  IF A>=04H THEN GOTO 5000
4040  IF (AA-INP[AA/32]*32)<>0 THEN GOTO 2000
4050  IF AA=0340H THEN PRINT "IDLE";:: GOTO 4300
4060  IF AA=0360H THEN PRINT "RSET";:: GOTO 4300
4070  IF AA=0300H THEN PRINT "RTWP";:: GOTO 4300
4080  IF AA=03A0H THEN PRINT "CKON";:: GOTO 4300
4090  IF AA=03C0H THEN PRINT "CKOF";:: GOTO 4300
4100  IF AA=03E0H THEN PRINT "LREX";:: GOTO 4300
4200  GOTO 2000
4300  GOSUB 1100
4310  GOSUB 1700
4320  GOSUB 1900
4330  PRINT
4340  M=M+2
4350  GOTO 100
5000  REM
5010  REM FORMAT 6
5020  REM
5030  AOP=INP[AA/64]*64
5040  IF AOP>0740H THEN GOTO 6000
5050  TR=AA-AOP
5060  T=INP[TR/16]
5070  R=TR-T*16
5100  IF AOP=0400H THEN PRINT "BLWP ";:: GOTO 5300
5110  IF AOP=0440H THEN PRINT "B ";:: GOTO 5300
5120  IF AOP=0480H THEN PRINT "X ";:: GOTO 5300
5130  IF AOP=04C0H THEN PRINT "CLR ";:: GOTO 5300
5140  IF AOP=0500H THEN PRINT "NEG ";:: GOTO 5300
5150  IF AOP=0540H THEN PRINT "INV ";:: GOTO 5300
5160  IF AOP=0580H THEN PRINT "INC ";:: GOTO 5300
5170  IF AOP=05C0H THEN PRINT "INCT ";:: GOTO 5300
5180  IF AOP=0600H THEN PRINT "DEC ";:: GOTO 5300
5190  IF AOP=0640H THEN PRINT "DECT ";:: GOTO 5300
5200  IF AOP=0680H THEN PRINT "BL ";:: GOTO 5300
5210  IF AOP=06C0H THEN PRINT "SWPB ";:: GOTO 5300
5220  IF AOP=0700H THEN PRINT "SETO ";:: GOTO 5300
5230  IF AOP=0740H THEN PRINT "ABS ";:: GOTO 5300
5240  GOTO 2000
5300  GOSUB 1400
5310  GOSUB 1100
5320  GOSUB 1700
5330  IF T=2 THEN GOSUB 1200:: GOSUB 1800
5340  GOSUB 1900
5350  M=M+2
5360  PRINT
5370  GOTO 100
6000  REM
```

```
6010  REM FORMAT 5
6020  REM
6030  AOP=INP[AA/256]
6040  IF AOP>0BH THEN GOTO 7000
6050  CR=AA-AOP*256
6060  C=INP[CR/16]
6070  R=CR-C*16
6080  IF AOP=08H THEN $OP[0]="SRA":: GOTO 6200
6090  IF AOP=09H THEN $OP[0]="SRL":: GOTO 6200
6100  IF AOP=0AH THEN $OP[0]="SLA":: GOTO 6200
6110  IF AOP=0BH THEN $OP[0]="SRC":: GOTO 6200
6120  GOTO 2000
6200  GOSUB 1040
6210  PRINT ",";C;
6220  GOSUB 1100
6230  GOSUB 1700
6240  GOSUB 1900
6250  PRINT
6260  M=M+2
6270  GOTO 100
7000  REM
7010  REM FORMAT 2
7020  REM
7030  AOP=INP[AA/256]
7040  IF AOP>=020H THEN GOTO 8000
7050  D=AA-AOP*256
7052  IF D>07FH THEN D=D-256
7060  IF AOP=010H THEN PRINT "JMP ";:: GOTO 7300
7070  IF AOP=011H THEN PRINT "JLT ";:: GOTO 7300
7080  IF AOP=012H THEN PRINT "JLE ";:: GOTO 7300
7090  IF AOP=013H THEN PRINT "JEQ ";:: GOTO 7300
7100  IF AOP=014H THEN PRINT "JHE ";:: GOTO 7300
7110  IF AOP=015H THEN PRINT "JGT ";:: GOTO 7300
7120  IF AOP=016H THEN PRINT "JNE ";:: GOTO 7300
7130  IF AOP=017H THEN PRINT "JNC ";:: GOTO 7300
7140  IF AOP=018H THEN PRINT "JOC ";:: GOTO 7300
7150  IF AOP=019H THEN PRINT "JNO ";:: GOTO 7300
7160  IF AOP=01AH THEN PRINT "JL ";:: GOTO 7300
7170  IF AOP=01BH THEN PRINT "JH ";:: GOTO 7300
7180  IF AOP=01CH THEN PRINT "JOP ";:: GOTO 7300
7190  IF AOP=01DH THEN PRINT "SBO ";:: GOTO 7400
7200  IF AOP=01EH THEN PRINT "SBZ ";:: GOTO 7400
7210  IF AOP=01FH THEN PRINT "TB  ";:: GOTO 7400
7220  GOTO 2000
7300  DJ=M+2+D*2
7310  PRINT  TAB (12);"L";4,DJ;"(=";D;")";
7320  GOTO 7410
7400  PRINT " ";D;
7410  GOSUB 1100
7420  GOSUB 1700
7430  GOSUB 1900
7440  M=M+2
7450  PRINT
```

```
7460  GOTO 100
8000  REM
8010  REM FORMAT 3/9/4
8020  REM
8030  AOP=INP[AA/1024]
8040  IF AOP*4>03CH THEN GOTO 9000
8050  DTR=AA-AOP*1024
8060  DT=INP[DTR/16]
8070  R=DTR-DT*16
8080  D=INP[DT/4]
8090  T=DT-D*4
8100  AOP=AOP*4
8110  IF AOP=020H THEN PRINT "COC ";:: GOTO 8300
8120  IF AOP=024H THEN PRINT "CZC ";:: GOTO 8300
8130  IF AOP=028H THEN PRINT "XOR ";:: GOTO 8300
8140  IF AOP=02CH THEN PRINT "XOP ";:: GOTO 8400
8150  IF AOP=030H THEN PRINT "LDCR ";:: GOTO 8400
8160  IF AOP=034H THEN PRINT "STCR ";:: GOTO 8400
8170  IF AOP=038H THEN PRINT "MPY ";:: GOTO 8300
8180  IF AOP=03CH THEN PRINT "DIV ";:: GOTO 8300
8190  GOTO 2000
8300  GOSUB 1400
8310  IF D<10 THEN PRINT ",";#"R9";D;
8315    ELSE PRINT ",";#"R99";D;
8320  GOSUB 1100
8330  GOSUB 1700
8340  IF T=2 THEN GOSUB 1200:: GOSUB 1800
8350  GOSUB 1900
8360  M=M+2
8370  PRINT
8380  GOTO 100
8400  GOSUB 1400
8410  PRINT ",";D;
8420  GOTO 1320
9000  REM
9010  REM FORMAT 1
9020  REM
9030  AOP=INP[AA/4096]
9040  TRA=AA-AOP*4096
9050  TRB=INP[TRA/16]
9060  R=TRA-TRB*16
9070  TRC=INP[TRB/4]
9080  T=TRB-TRC*4
9090  T1=INP[TRC/16]
9100  R1=TRC-T1*16
9105  IF ABI=1 THEN AOP=AOP+08H
9110  IF AOP=04H THEN PRINT "SZC";:: GOTO 9300
9120  IF AOP=05H THEN PRINT "SZCB";:: GOTO 9300
9130  IF AOP=06H THEN PRINT "S";:: GOTO 9300
9140  IF AOP=07H THEN PRINT "SB";:: GOTO 9300
9150  IF AOP=08H THEN PRINT "C";:: GOTO 9300
```

```
9160  IF AOP=09H THEN PRINT "CB";:: GOTO 9300
9170  IF AOP=0AH THEN PRINT "A";:: GOTO 9300
9180  IF AOP=0BH THEN PRINT "AB";:: GOTO 9300
9190  IF AOP=0CH THEN PRINT "MOV";:: GOTO 9300
9200  IF AOP=0DH THEN PRINT "MOVB";:: GOTO 9300
9210  IF AOP=0EH THEN PRINT "SOC";:: GOTO 9300
9220  IF AOP=0FH THEN PRINT "SOCB";:: GOTO 9300
9230  GOTO 2000
9300  GOSUB 1400
9310  PRINT ",";
9315  GOSUB 1700
9320  IF T=2 THEN GOTO 9400
9330  T=T1
9340  R=R1
9350  GOSUB 1400
9360  GOSUB 1100
9370  IF T=2 THEN GOSUB 1200:' GOSUB 1800
9375  GOSUB 1900
9380  M=M+2
9390  PRINT
9395  GOTO 100
9400  I1=IOP
9405  I2=IOQ
9410  T=T1
9420  R=R1
9430  GOSUB 1400
9435  GOSUB 1800
9440  GOSUB 1100
9450  PRINT "  ";#;I1;#;I2;
9460  GOTO 9370
```

```
RUN
MEM START? 3C0H     MEM STOP? 400H
       SZCB  R13,*R1                    03C0    544D                TM
       MPY   *R9+,R4                    03C2    3939                99
       LDCR  @>4241, 0                  03C4    3020  4241          0 BA
       SZCB  R9,R13                     03C8    5349                SI
       SZC   @>5245,R12                 03CA    4320  5245          C RE
       SZCB  @>442E,*R8                 03CE    5620  442E          V D.
       LDCR  @>3130(R14), 4             03D2    312E  3130          1.10
       SLA   R13, 0                     03D6    0A0D                ..
       XOR   *R2,R9                     03D8    2A52                *R
       SZC   R1,*R5                     03DA    4541                EA
       SZC   *R9,*R1                    03DC    4459                DY
       SLA   R13, 0                     03DE    0A0D                ..
       DATA  >0062                      03E0    0062                ..
       MOV   @>FFFE(R14),R1             03E2    C06E  FFFE          ....
       ANDI  R1,>003F                   03E6    0241  003F          .A.?
       MOV   R1,@>0038(R9)              03EA    CA41  0038          .A.8
       CLR   @>003E(R9)                 03EE    04E9  003E          ...>
       C     @>00A6,@>3000              03F2    8820  00A6  3000    . 0.0.
       JNE   L0400(= 3)                 03F8    1603                ..
       BL    @>301A                     03FA    06A0  301A          ..0.
       JMP   L0410(= 8)                 03FE    1008                ..
       BL    @>2CE6                     0400    06A0  2CE6          ....

STOP AT 100
```