How to Read Out the Internal Memory Code of a 80C51 Microcontroller Family

Overview

A single chip microcontroller is a controller with a ROM memory storing the program code of the specific application. The program is masked during the processing of the integrated circuit. The great advantage is that no I/O ressource is consumed to interface the external code memory. I/O line possibilities consequently are increased.
In order to test or to check this internal ROM , some solutions can be implemented.

This application note describes a solution to dump the internal ROM and is based on a specific TEST MODE (**TEST MODE VER**) used to test the microcontroller in production .
In this note a member of MHS's 80C51 family will be named 80Cxxx .

TEST MODE VER to dump the ROM

The TEST MODE VER can be used by setting some 80Cxxx inputs shown in figure 1 . The PORTs P1 and P2 receive respectively the low address lines and the high address lines . The code program in that condition is read from P0 . The lines of PORT0 is open drain and must be tied with 10kohm pull-up resistors .

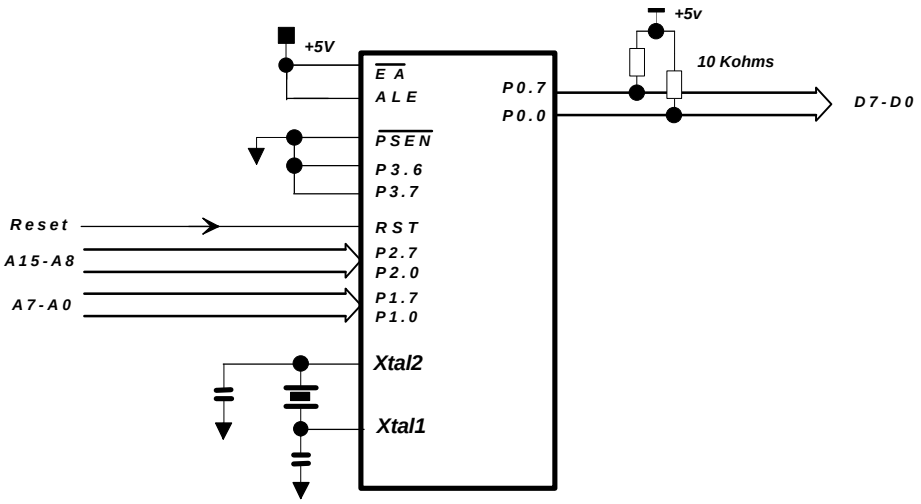

Figure 1. Configuration for the TEST MODE VER

To activate and to dump the ROM a specific timing must be applied, it is shown in figure 2.
Before generating the first **Read** cycle a delay at least equal to 24 clock periods has to be waited. This time is needed to reset correctly the 80Cxxx . At this time the first address is read by the 80Cxxx from the PORT 1 and 2. To read the first data it is necessary to wait again 12 clock periods. This is due to the internal synchronisation and the internal ROM access time. So the data only appears 36 clock periods after the reset is applied .

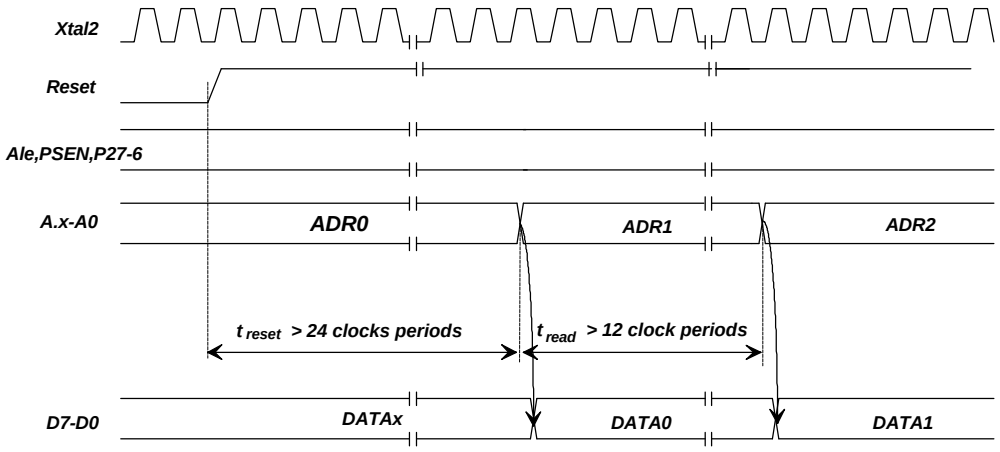

Figure 2.Timings to dump the ROM

Example Dump ROM Application

Figure 3 shows the schematic of this typical application using MHS piggy-back. The main idea is to control the 80Cxxx by another one in order to generate all the signals we need and to output the dumped data on a serial line or to trace the dumped data on PORT0 with a logical analyser.

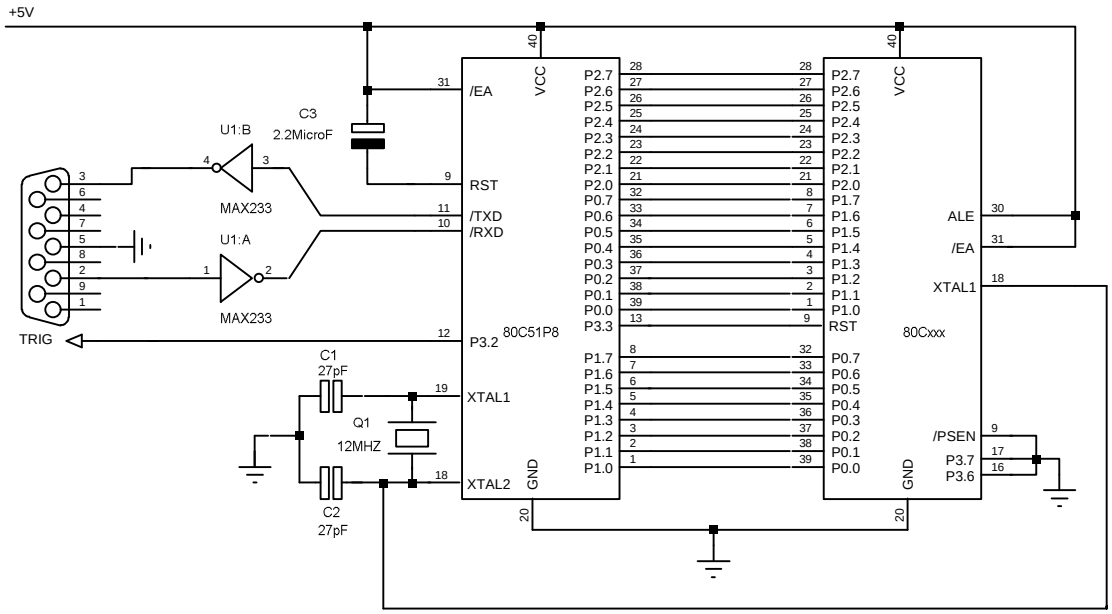

Figure 3. Typical application

Flow chart of the program

Figure 4 shows the flow chart of the program .The program starts with the serial line configuration (2400bds, 8-bit of data) and the set-up of target 80Cxxx for the DUMP operation. Then read operation of the ROM is performed and the read data is transmitted on the serial line. In the same time, the TRIG signal is active low to synchronize an external logical analyser .

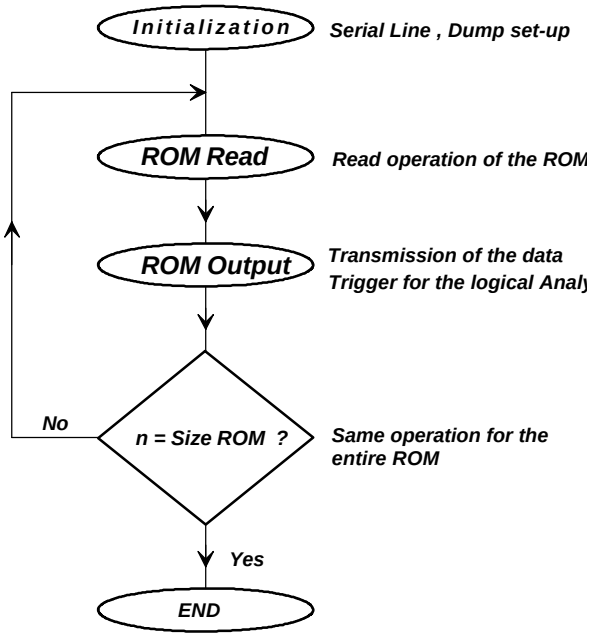

Figure 4. Flow chart for the dump ROM program

Subroutine of the Initialization Sequence

```
;===                                          initialization
==============================
;  Speed = 2400bds , Format = 8 bits
;=========================================
=
;----- Set-up the Baud Rate Generator -------------------------
  SetB   ROM_RST                  ; Target under Reset
  MOV TMOD,#Baud_Rate_Timer  ; TIMER1 = 20H
  MOV TH1,#Speed                  ; Speed = 0F3H
  Setb TR1
;------ Set-up the UART ----------------------------------------
  MOV SCON,#FORMAT      ; FORMAT =42H
;=== ROM Dump operation Set-Up  ================
;              Size_Rom      =      4095      bytes             ,
;-------------------------------------------------------------------
  MOV DPL,#00                  ; starts with first address
```

Subroutine of the dump ROM operation

```
;=== ROM Read Operation ======================
Dump operation:
  MOV P0,DPL                    ; Address of the Read
  MOV P2,DPH
  CLR  Trig                     ; Analyser TRiggering
  MOV A,P1
  Call Serial_trans             ; Serial transmission
  SETB Trig
  INC DPTR                      ; Next address
  MOV A,#Size_ROM_Low
  CJNE A,DPL,Dum_operation
  MOV A,#Size_ROM_High
  CJNE A,DPH,Dump_operation
  JMP $

Serial_trans :
  JNB TI,Serial_trans
  CLR TI
  MOV SBUF,A
  RET
```

Timings analysis

Two parameters are critical in the dump ROM application (figure 2) : **treset** and **tread**.
treset parameter is the minimum time required from the active Reset to the output of the first data. The minimum value of this parameter is 24 clock periods.
In this application, the first data appears **168 clock periods** after the first address.
To determine when data coming from the ROM can be read , **tread** parameter must be taken into account . The minimum value of this parameter is 12 clock periods measured when the address is stable and the data can be read.
In this application, **tread** will be read **72 clock periods** after the address is driven. So, both of the parameters are not critical .

Conclusion

This application based on a MHS piggy-back is easy to implement and requires only few components.
Furthermore this basic application can be improved by adding a software interface developed on a Personal Computer to compare the dumped ROM and the original one.

Additional Information

For additional information on Microcontrollers, and Ordering Information, please refer to the following datasheets available on request :

- 80C31/51
- 80C32/52
- 80C154/83C154
- 83C154D