Working with the MDM9x4x Platform

The runtime environment of the bootloader (NPRG) running with the SBL (download mode) interface on the MDM9x4x platform family has an unfortunate feature. It lacks the ability to access the NAND controller registers, which is a crucial condition for the qtools utilities to work directly with flash memory, including qrflash and qwdirect. It is possible that access to these registers can be obtained, but numerous experiments in this direction have not yielded success.

Nevertheless, running a patched NPRG on such a platform is not entirely useless. At the very least, it allows reading and writing data, including memory and platform registers, in certain areas of the processor's address space using commands from utilities like qcommand and qrmem. Additionally, such a bootloader enables running custom applets, which advanced qtools users can leverage to implement various algorithms for working with the platform, taking into account the access restrictions imposed by the configured SBL.

One interesting application of the data reading/writing capabilities is the ability to "software" (without resorting to "barbaric" methods like short-circuiting a point on the device's board or erasing the SBL partition) gain access to the PBL interface. For the discussed platform family, this can be achieved by writing the value 1 to the BOOT_MISC_DETECT register (address 0x193d100) of the platform, followed by a reboot. This reboot should not be performed using the bootloader's standard method (command 0xb) but by executing an operation in the address space that triggers an exception, such as reading data at an address that does not correspond to any of the platform's components or reading protected data.

As a result, you can follow this approximate scenario to work with the flash memory on MDM9x4x platforms:
1. Launch NPRG using the SBL interface:

```
./qdload -p/dev/ttyUSB1 -k10 -q
```

```
 Waiting for the Hello package from the device...

 Download Image ID: 00000007

 Load loaders/NPRG9x45p.bin...

 Pass the bootloader to the device...

 Loader Handover Successfully
Hello ok, flash: MT29F4G08ABBDA3W
```

2. Write 1 to BOOT_MISC_DETECT:

```
./qcommand -p/dev/ttyUSB1 -c "m 193d100 1"
```

3. We attempt to read from a protected address:

```
./qcommand -p/dev/ttyUSB1 -c "d 7980000 4"
```

and interrupt the utility's operation (at this point, the system detects the PBL port):

```
^C
```

4. Launch ENPRG using the PBL interface:

```
./qdload -p/dev/ttyUSB2 -k10 -i

 Waiting for the Hello package from the device...

 Download image ID: 0000000d

 Load loaders/ENPRG9x45p.bin...

 Pass the bootloader to the device...

 Loader Handover Successfully

 HELLO protocol version: 3
 Chipset: MDM9x4x
 NAND Controller Base Address: 079b0000
 Flash: Micron MT29F4G08ABBDA3W, NAND 512MiB 1.8V 8-bit
 Sector size: 516 bytes
 Page size: 2048 bytes (4 sectors)
 Number of pages per block: 64
 OOB size: 64 bytes
 Type ECC: BCH, 4 bit
 ECC size: 7 bytes
 Spare: 4 bytes
 Defective Block Marker Position: user+1d1
 Total Flash Memory Size = 4096 Blocks (512 MB)
```

Perform further flash memory operations in normal mode.
For example, to view the partition table:

```
./qrflash -p/dev/ttyUSB2 -k10 -s@ -m

 #  Start size A0 A1 A2 F# format ------ Name------
============================================================
00       0  00000a   ff 01 00 00   LNX    0:SBL
01       a  00000a   ff 01 ff 00   LNX    0:MIBIB
02      14  0000b4   ff 01 ff 00   LNX    0:EFS2
03      c8  000008   ff 01 00 00   LNX    0:TZ
04      d0  000005   ff 01 00 00   LNX    0:RPM
05      d5  000008   ff 01 00 00   LNX    0:aboot
06      dd  000052   ff 01 00 00   LNX    0:boot
07     12f  000002   ff 01 00 00   LNX    0:SCRUB
08     131  000236   ff 01 00 00   LNX    0:modem
09     367  00000c   ff 01 00 00   LNX    0:misc
10     373  000053   ff 01 00 00   LNX    0:recovery
11     3c6  000006   ff 01 00 00   LNX    0:fota_none
12     3cc  0000b6   ff 01 00 00   LNX    0:recoveryfs
13     482  000449   ff 01 00 00   LNX    0:system
14     8cb  00007c   ff 01 00 00   LNX    0:PAD1
15     947  0000a2   ff 01 00 00   LNX    0:USERRW
16     9e9  0001d6   ff 01 00 00   LNX    0:HDATA
17     bbf  0003ae   ff 01 00 00   LNX    0:NTGFOTA
18     f6d  000050   ff 01 00 00   LNX    0:CUST
19     fbd  000030   ff 01 00 00   LNX    0:PERSIST
============================================================
 Partition table version: 4
```

To read a partition:

```
./qrflash -p/dev/ttyUSB2 -k10 -s@ -f1

 #  Start size A0 A1 A2 F# format ------ Name------
============================================================
01       a  00000a   ff 01 ff 00   LNX   0:MIBIB
 * R: block 000013 [start+009] (100%)
```

To write a partition:

```
./qwdirect -p/dev/ttyUSB2 -k10 -fo -b12f pattern.bin

 Entry from pattern.bin file, starter block 12f, size 002
 Recording Mode: Linux Format on a USB Flash Drive
 Block: 0130 Page: 3f
```

And so on.