

Emulation

Takanen Edoardo

March 25, 2025

Abstract

Contents

1	Introduction	3
2	Premises	4
3	General Structure	5
4	Memory	6
4.1	Memory mapping	6
4.2	Choices for this project	7
4.3	Implementation	7
5	CPU	8
5.1	Architecture and considerations	8
5.2	The op-tables	8

1 Introduction

As a kid, I used to play with some Nintendo (copyright symbol) consoles like the Wii or the DS and I've always been keen about the games they make. This passion for videogames grew on me so that I got interested in the making process of them, leading to game development. I never asked myself one question, though, until this year, which is how are these games able to run onto this consoles? and how can people make emulators so that I could play on my personal computer? Thus, I decided to embrace the unknown world of emulation, because I have always been fascinated by it and always took it for granted. Emulation is not well explained on the Internet. Mainly, the results you will find if you search for it are "the program pretends to be the console" or "you will be able to play old titles". I was not satisfied with these responses, I wanted to know more. Thus, my emulation journey started with looking for a full definition of this process. I will try to give my own definition of emulation, so that I can lay a starting point to a general knowledge that will be then deepened during the paper. With this being said, to "make an emulator" means to develop the software that will do exactly what the hardware of the console does, so that when plugging the game data, the program will know how to read and handle it.

Emulation can only happen when the machine in which we run the software is more powerful than the hardware we want to emulate. For example, if our console has 2Kb of memory, for sure we are not able to emulate it on a computer that has 2Kb or less, since we also have to consider that the host computer will have an operating system running (which uses some of the RAM). I chose to make a Game Boy emulator, because while looking for the retro consoles, it seemed the least difficult when talking about the hardware structure complexity, meaning a good way to start tackling this subject.

2 Premises

This emulator project is purely for understanding the concepts and the theory about how a machine like a console (or similarly a computer) is made (and also for fun). There are many better-developed Game Boy emulators online, and making one that could compete with the other popular ones is nowhere near my goals. Therefore, I could not achieve the level of knowledge I want to reach if I just looked at other people's codes, I want to **fully** understand the subject. Obviously though I have to start somewhere, I do not have the skills to reverse-engineer a real Game Boy (although it would be an extremely interesting challenge), for this reason I will only consult theory guides made by many passionate developers and hackers that already did the work of studying the Game Boy from scratch for us. For a better understanding, I used two sources for this project, in order to have a dual perspective on the study.

For anyone who would like to dig into this challenge, the guides are [GBDev](#) and [GBEDG](#).

What this paper is not.

This paper is not and was not intended as a guide, I previously attached some real references. This document is a report of my journey through the development of the emulator, made for understanding the fundamentals of what is around us, from personal computers to smartphones. It could also be a way for readers to get passionate about this topic and an inspiration for them to make their own emulators (or even better, their own consoles!).

3 General Structure

The first thing I want to cover is in what way we want to structure our emulator.

```
1 int main() {
2     // Hardware components definition
3     Memory mem;
4     CPU cpu;
5     // ...
6
7     // Components initialization
8     mem.init();
9     cpu.init();
10    cpu.load_boot();
11    // ...
12
13    while (true) {
14        cpu.exec_op(mem); // Executing an operation
15        // emulate all the other components
16    }
17
18    return 0;
19 }
```

Actually, when we look at the circuit inside the Game Boy, all the components are, on one side, all on their own, they all execute at the same time. The CPU could be executing a simple addition, while the PPU could be rendering graphics onto the screen, all of these things happen simultaneously. This **can** be done with software, but would mean more complexity. Hence we will pick a less complicated path, and decide to execute the components one at a time.

```
1 while (true) {
2     // Returns how many clock cycles the instruction took
3     int cycles = cpu.exec_op();
4
5     // Updating all the other components
6     timers.update(cycles);
7     ppu.update(cycles);
8     // ...
9 }
```

The real hardware is driven by the clock, while my implementation will be driven by how many clock cycles an instruction took.

4 Memory

Before looking at the main components that shape the Game Boy hardware, I would like to focus on how memory is subdivided inside the console.

4.1 Memory mapping

The address bus had 16 bits, meaning there could be 65'536 unique addresses (64Kb).

Since the Game Boy did not have a flash memory, those 64Kb were all the console could access (this includes all the different RAMs, the cartridge data, and the registers made to control various components). Internally inside the Game Boy, there is some logic that specifies what component will be activated based on the requesting address.

These are the regions into which the memory is split, along with a brief description of their use. Notice that some areas are marked as "Prohibited", though Nintendo has not provided an explanation for this.

Start	End	Description
0000	3FFF	16Kb cartridge ROM
4000	7FFF	16Kb cartridge ROM*
8000	9FFF	8Kb VRAM
A000	BFFF	8Kb External RAM
C000	CFFF	4Kb Work RAM
D000	DFFF	4Kb Work RAM
E000	FDFE	Prohibited area
FE00	FE9F	OAM
FEA0	FEFF	Prohibited area
FF00	FF7F	I/O Registers
FF80	FFFE	High RAM
FFFF	FFFF	IE register

* switchable

Table 1: Game Boy's memory mapping

Another interesting fact I found out when making this emulator is what is inside a cartridge. It is fascinating to know that some cartridges would not only include the ROM banks with the game code, but they could also supply their own additional SRAM (Static Random-Access Memory), as well as a battery to preserve the game saves. Due to limiting memory sizes, games could also have a Memory Bank Controller (MBC) to change what ROM should be pointed for memory region 4000 – 7FFF.

Notice that all these additional components are **not** supported on my emulator, since the original Tetris DMG cartridge just had a 32 Kb ROM.

4.2 Choices for this project

For simplicity, I decided not to break down all these areas into different regions of memory in the emulator, but I opted for an easier solution, which is to create an array of 65'536 bytes, since the data bus was 8 bits-long, so every address will have exactly one byte of data.

There is a trade-off in choosing this approach though. On one hand, it makes things simpler to manage, we can have all the memory in one place and it really helps when debugging, but on the other hand, it is not entirely correct. Each region of memory has different restrictions, cartridge memory should be read-only, some areas might not be fully readable and writable sometimes (we will see an example when implementing the PPU).

By choosing this option, we are making all the memory readable and writable for everyone, so technically, the game could edit its own code (and this actually happened when I was emulating Tetris!).

4.3 Implementation

```
1 struct Memory {
2 private:
3     static constexpr u32 MAX_MEM = 64 * 1024;
4     // Array of bytes to emulate all the Gameboy's addresses
5     Byte Data[MAX_MEM] = {};
6 public:
7     void init();
8
9     /**
10    * Functions used for setting and accessing memory as
11    * mem[addr] = value          to set
12    * Byte value = mem[addr]     to access
13    * */
14     Byte operator[](u32 addr) const;
15     Byte& operator[](u32 addr);
16
17     /**
18    * Dumps all the memory in a file,
19    * used for debugging purposes
20    * */
21     void dump(const char* filename);
22 };
```

This is the entire memory structure. Every component we create will have access to this structure in order to read from and write to memory using the two operator[] functions. I have also added a **dump** function that writes all the bytes to a binary file at the moment the function is called, for easier debugging.

5 CPU

The first component we likely want to implement is the Central Processing Unit (CPU). This component is the most important in our circuit, and is the one that coordinates the other components, executes the program we give to it etc. Thus, the first thing I had to implement were all the instructions that the processor could run.

5.1 Architecture and considerations

The Game Boy's CPU is a custom-made by Sharp Corporation (which had a close relationship with Nintendo at that time), it is often referred to as **DMG-CPU** or **Sharp SM83** and runs at around 4.19 MHz. When making the processor a lot of inspiration was taken from the Zilog 80 and the Intel 8080. Personally, I recently had the possibility to work with a real Z80, and over the past few months, I have gained hands-on experience with its architecture. Specifically, when studying the Zilog, I noticed some differences and similarities with the Game Boy's processor.

For example, the Nintendo processor lacks the IX and IY registers, which in the Zilog were used to set a base address that could be offset with the $LD(IX+d), r$ and $LD(IY+d), r$ to save instruction bytes. Instead, the DMG-CPU introduced a brand new load instruction, LDH (load from high memory), which always offsets from address **FF00**, pointing to **High-RAM** and the **I/O registers**.

I think custom-making their own CPU was the perfect choice for Nintendo, as it allowed them to implement changes like these to better suit their needs, save instruction bytes, and increase performance.

5.2 The op-tables

The list of all instructions is usually arranged in tables, called opcode-tables. The Game Boy has 2 op-tables.

8-bit opcodes

[illegible]

16-bit opcodes, where the first 8 bits are 0xCB

[illegible]

Figure 1: Game Boy's opcode-tables