

Szegedi Tudományegyetem
Informatikai Intézet

**Nintendo Game Boy Zilog Z80 emulátor
implementálása**

Diplomamunka

Készítette:
Krizsák Tibor
programtervező informatikus MSc
szakos hallgató

Témavezető:
Dr. Tanács Attila
egyetemi adjunktus

Szeged
2018

Tartalomjegyzék

Feladatkiírás	4
Tartalmi összefoglaló	5
Bevezetés	6
1. Az emulátorok és a Nintendo Game Boy	7
1.1. Az emulátorokról	7
1.1.1. Az emulátor fogalma	7
1.1.2. Az emulátorok típusai	7
1.1.3. Az emulátorok jövője	8
1.2. Nintendo Game Boy	8
1.2.1. Története, jelentősége	9
1.2.2. Hardver specifikáció	9
1.2.3. Boot ROM	11
2. A fejlesztési folyamat	13
2.1. A fő ciklus	14
2.2. Alkalmazott eszközök	15
2.2.1. A Rust programozási nyelv	15
2.2.2. A minifb könyvtár	16
2.2.3. Fejlesztői környezet	17
2.2.4. Debugger	17
2.2.5. Memóriatérkép	18
2.3. A feladat specifikációja	19
3. A processzor és a memória implementációja	21
3.1. CPU	22
3.1.1. Regiszterkészlet	22
3.1.2. Ciklusok, frekvenciák	23
3.1.3. Betöltés - dekódolás - végrehajtás	24
3.2. Interrupt kezelés	25
3.3. Utasításkészlet	26
3.3.1. <i>Load</i> utasítások - LD	26
3.3.2. Aritmetikai utasítások - ADD, ADC, SUB, SBC, INC, DEC	27
3.3.3. Logikai utasítások - AND, XOR, OR, CP	29
3.3.4. Verem utasítások - PUSH, POP	30
3.3.5. Eljárás utasítások - JP, CALL, RET	30
3.3.6. Bitmanipulációs utasítások - BIT, RES, SET, SWAP	30

3.3.7. <i>Rotate</i> és <i>Shift</i> - RLC, RRC, RL, RR, SLA, SRA, SRL	31
3.3.8. Egyéb, speciális utasítások	32
3.4. Memória	33
3.4.1. DMA	34
3.4.2. Memory Bank Controller	35
3.5. Időzítők	35
3.5.1. TIMA	35
3.5.2. DIV	37
4. Függelék	38
4.1. A Nintendo Game Boy hivatalos architektúrája	38
4.2. A processzor opkód táblái	39
Nyilatkozat	41
Köszönnetnyilvánítás	42
Irodalomjegyzék	43

Feladatkiírás

A Nintendo Game Boy egy 1989-ban bemutatott, 8 bites kézi videojáték-konzol. A konzolban egy Zilog Z80 (az Intel 8080 utódja) processzor működik, kiegészítve néhány specifikus utasítással. A Game Boy emulátor fejlesztésének bemutatása során a CPU utasításait, a GPU renderelésének működését, a memóriakezelést, és a megszakítás-vezérlést kell implementálni. Ahhoz, hogy ezek megfelelően működjenek, a CPU frekenciájára, illetve a képfrissítési gyorsaságra is tekintettel kell lenni.

A játékkonzol emulátorok fejlesztése során a szűk, ezzel foglalkozó fejlesztői réteg kialakított egy egyértelmű, jól követhető fejlesztési folyamatot. A dolgozatban ezen keresztül kerüljenek bemutatásra a Nintendo Game Boy emulátor fejlesztési fázisai.

A tesztelés a más Zilog Z80 emulátor fejlesztők által készített teszt ROM-okon történjen.

Tartalmi összefoglaló

– A téma megnevezése:

Egy emulátor fejlesztési fázisainak bemutatása a Nintendo Game Boy hardveren keresztül, Rust nyelven implementálva.

– A megadott feladat megfogalmazása:

A feladat egy Nintendo Game Boy emulátor implementálása, és fejlesztési fázisainak bemutatása. A bemutatás során a CPU utasításait, a GPU renderelésének működését, a memóriakezelést, és a megszakítás-vezérlést kell érinteni, illetve az egyéb kisebb, de a működéshez elengedhetetlen megoldások is megemlítésre kerülnek. Ahhoz, hogy ezek megfelelően működjenek, a CPU frekvenciájára, illetve a képfrissítési gyorsaságra is tekintettel kell lenni.

– A megoldási mód:

Az emulátor fejlesztő közösség által összegyűjtött, – *reverse-engineered* – információkra, illetve a processzor gyártója által kiadott technikai dokumentációra hagyatkozva felépítettem és implementáltam a CPU struktúráját, utasításkészletét, majd a többi modult, részegységet. Meghatároztam a modulok közti kommunikációt, időzítéseket, adatfolyamatot. A videójáték-, illetve teszt ROM-ok byte-jait sorra beolvasva az emulátor meghatározza a megfelelő műveletet, meghatározott időközönként renderel, illetve kezeli a megszakításokat.

– Alkalmazott eszközök, módszerek:

Az emulátor Linux rendszeren, Rust nyelven került implementálásra, a `rustc` fordító, illetve a `cargo` package manager segítségével. A rendereléshez a `minifb` libraryt használtam, ami egy nagyon egyszerű framebuffer használatát teszi lehetővé. A fejlesztésre került egy debugger eszköz, illetve egy memóriatérkép eszköz is, ami nagyban megkönnyítette a hibakeresést.

– Elért eredmények:

Az implementált emulátor képes futtatni Memory Banking nélküli videójáték ROM-okat, az inputra az elvárásoknak megfelelően reagálva. A processzor műveletek és a renderelés az eredeti konzollal megegyező eredményt adnak. A közösségi Game Boy teszt ROM-ok szinte mindegyikét sikerrel végrehajtja.

– Kulcsszavak:

Nintendo, Game Boy, emulátor, fejlesztés, Rust

Bevezetés

A számítástechnikában az emuláció fogalma nem új keletű. Különböző területeken, különféle problémák megoldására használnak emulátorokat, ugyancsak különböző okokból. A nyomtatóktól kezdve, a DOS-kártyákon keresztül, a többmagos rendszertervezésen át egészen a videojáték konzolokig terjed a paletta - nem túlzás azt állítani, hogy az emulátorok ott vannak a minden napjainkban.

Ezen diplomamunka a videojáték konzolok emulátorainak fejlesztésére fókuszál. Többféle cél állhat a háttérben, ha valaki ilyen emulátor fejlesztésére adja a fejét: a régi hőskorbeli konzolok digitális megőrzése vagy életre keltése, későbbi szoftverfejlesztés az emulált hardveren, esetleg hobbiként. Az utóbbi évek tendenciája azt mutatja, hogy ez utóbbi ok egyre gyakoribb - az emulátor fejlesztői közössége napról napra nagyobb és aktívabb, szokások és kisebb fejlesztői folklór alakult ki az emulátor készítését illetően - a dolgozat ennek bemutatására helyezi a hangsúlyt.

Az emulátor fejlesztés szemléltetése Nintendo Game Boy kézi videojáték konzolon keresztül fog történni, amely a maga idejében egy igazán sikeres konzol volt, és tulajdonképpen kultusz épült köré. A 8 bites architektúrájából adódóan kevéssé bonyolult felépítéssel rendelkezik, népszerűségéből adódóan jól dokumentált, így az emulálásának implementációjához nincs szükség túl sok *reverse-engineering* gyakorlatra.

A dolgozat első néhány fejezetében az emulátorokról, a Nintendo Game Boy hardveréről, specifikációjáról, illetve a későbbi fejlesztés workflow-járól fog szó esni. Ezekben a fejezetekben van megfogalmazva, illetve leírva az, hogy pontosan mi az az emulátor, milyen hardver emulációjáról van szó, és hogy az emuláció teljes implementálásáig milyen ponton keresztül vezet az út. A következő nagyobb logikai egység az implementáció. Ennek részeként először bemutatásra kerülnek az alkalmazott eszközök, technológiák, majd az emulátor pontos és elvárt specifikációjának leírását az igazi implementációs szakasz követi.

A processzor modellezése a regiszterek, flagek, és egyéb jellemzők megtervezésével kezdődik, majd következő lépésként az utasításkészlet megvalósításával folytatódik. A CPU-hoz szorosan kapcsolódó memória ez után kerül tárgyalásra. A memória ismertetése után az időzítők, majd a PPU felépítése és működése szerepel. Az implementáció ezen pontján a Boot ROM már futtathatóvá válik, erről is esik majd néhány szó. A fejlesztési részt a joypad jellemzői és megoldásai zárják.

A dolgozat zárásként bemutatásra kerül az emulátor használata, illetve a fejlesztésből adódó dependenciák, majd végül a teszt ROM-ok jellemzői, futtatásuk, és a futtatási eredményeik.

1. fejezet

Az emulátorok és a Nintendo Game Boy

1.1. Az emulátorokról

Az utóbbi évtizedekben végbement – és jelenleg is tartó – technikai fejlődés következményeként rendkívül gyors a technológiai elavulás. Ennek következményeképp az eszközök életciklusa megrövidül, értékük rohamosan csökken. Gyakran előfordul azonban, hogy szükség van a régi *legacy* rendszerekre, vagy elengedhetetlen a visszafelé kompatibilitás, esetleg szeretnénk az adott hardvert a számítástechnikai jelentősége miatt valamilyen formában megőrizni, használhatóvá tenni. Az emulátorok ezekre a problémákra igyekszenek megoldást kínálni – persze rendkívül sok egyéb felhasználási terület mellett.

1.1.1. Az emulátor fogalma

Definíció szerint olyan hardvert vagy szoftvert nevezünk **emulátornak**, amely lehetővé teszi, hogy egy számítástechnikai rendszer (szokás ezt *host*-nak nevezni) úgy viselkedjen, mint egy másik számítástechnikai rendszer (ez pedig a *guest*). Jellemzően az emulátor a *host* rendszer számára teszi lehetővé olyan szoftver futtatását vagy periféria használatát, amely a *guest* rendszerhez lett kifejlesztve. Röviden megfogalmazva az emulátor egy olyan hardver vagy szoftver, ami egy másik eszközöt vagy programot emulál, imitál.

1.1.2. Az emulátorok típusai

Az emulátorok többsége csak a hardver architektúrát emulálja – ha operációs rendszer vagy egyéb szoftver is szükséges az emuláláshoz, akkor azt is biztosítani kell. Ebben az esetben az operációs rendszert és a szoftvert *interpretálni* (értelmezni) fogja az emulátor. A gépi kód *interpreteren* kívül azonban az emulátornak tartalmaznia kell a *guest* hardver minden lehetséges jellemzőjét, és viselkedését is virtuálisan: ha például egy adott memóriahezre való írás befolyásolja azt, hogy mi jelenik meg a képernyőn, úgy azt is emulálni kell. Habár lehetne az emulációt extrém részletességgel, atomi szinten végezni – például az áramkör adott részei által kibocsátott pontos feszültségingadozás emulálásával, stb. –, ez egyáltalán nem gyakori, az emulátorok általában megállnak a dokumentált hardver specifikáció, és digitális logika szimulációjának szintjén.

Némely hardver hatékony emulálásához extrém pontosság szükséges: az óraciklusokat, nem dokumentált jellemzőket, kiszámíthatatlan analóg elemeket, és *bugokat* mind-mind

implementálni kell. A klasszikus otthoni számítógépek esetében (például a Commodore 64) ez hatványozottan igaz, mert az ezekre a hardverekre írt szoftverek gyakran kihasználtak alacsony szintű programozási trükköket, melyeket főként a videojáték programozók és a *demoscene*¹ fedeztek fel.

Ezzel szemben léteznek azonban olyan platformok, amelyek alig használják a közvetlen hardver elérést, jó példa erre a PlayStation Vita. Ezekben az esetekben elég egy kompatibilitási réteget megvalósítani, amely a *guest* rendszer rendszerhívásait fordítja le a *host* rendszer hívásaira.

1.1.3. Az emulátorok jövője

A videojáték-konzol emulátorok világa, illetve az emulátor fejlesztő közösség helyzete igen érdekes. Az egyik oldalról megvizsgálva azt tapasztalhatjuk, hogy egyre nagyobb népszerűségnek örvendő területről van szó. Ami a másik oldalt illeti – a helyzet nagyon homályos. Újabb és újabb konzolok jelenniekn meg, egyre rövidebb életciklussal és egyre bonyolultabb architektúrával. Jól mutatja ezt a PlayStation 3 példája: 12 éve, 2006-ban jelent meg, és tökéletes emulátor még nem készült hozzá. A közösség nem tudja tartani a tempót a bonyolultság, és a rövid életciklusokból adódó szoros határidők miatt.

Sokak szerint viszont a jövőben nemhogy nehezebb, hanem inkább könnyebb lesz az emuláció: véleményük szerint a hardver emulációja nem lesz könnyű, viszont az utóbbi években nagyon sokat javult a szoftverek minősége és tisztasága egyaránt. A játékfejlesztők rá vannak kényszerítve az API-k (*Application Programming Interface* – alkalmasprogramozási interfész) használatára a hardver *bugjainak* kihasználása és a trükközés helyett, és ez lehetőséget adhat az API-kon alapuló emuláció elterjedése felé.

Fontos megemlíteni egy 2010-ben induló közösségi projektet, a RetroArch-ot, amely a videojáték konzol emulátorok számára biztosít egy prezentációs réteget, ún. *frontend*-et, amely egybefogja, és használhatóvá, futtathatóvá teszi a vele kompatibilis emulátorokat. Ez a megoldás nagyban megkönyíti a felhasználók életét, hiszen több tucatnyi rendszer emulátorát érhetik el egyetlen felületen keresztül, és a fejlesztők számára is jelent egy enyhe szabványosítási törekést.

Ahogy a fenti két vélemény, és a RetroArch példája is mutatja, sokan sokféleképpen vélekednek az emulátorfejlesztés jövőjéről, nem beszélve a frissen induló közösségi projektekről – szinte biztosan kijelenthető, hogy ez a terület nem fog egyhamar megszűnni.

1.2. Nintendo Game Boy

Egy emulátor fejlesztési folyamatának bemutatására a Nintendo Game Boy tökéletes példa több szempontból is. Elsősorban széleskörűen ismert, ebből adódóan az emulátor fejlesztői közösség által is jól dokumentált, a hardver szinte az utolsó részletig vissza lett fejtve. Ezekből a dokumentációk tehát jó kiindulási alapot nyújtanak. Az is fontos szempont, hogy a hardver a 8 bites érából származik, ami szinte garantálja az egyszerűbb architektúrát (ez persze relatív), így a könnyebb implementálhatóságot. Szintén megemlítendő, hogy a fejlesztői közösség által készített teszt ROM-ök nagyban segítik a

¹ A *demoscene* nemzetközi underground számítástechnikai szubkultúra, amelynek célja különböző számítógépes digitális művészeti alkotások (*demók*) készítése.

hibakeresést, verifikációt.

1.2.1. Története, jelentősége



1.1. ábra. A *Nintendo Game Boy* logója

A Game Boy egy Nintendo által gyártott hordozható videojáték konzol, amit a nagyközönség számára 1989-ben mutattak be. Ez volt a gyártó első 8 bites kézi konzolja, amihez a játékokat cserélhető kazetta formájában (angolul *cartridge*) lehetett megvásárolni.

Az okos marketingnek, és a jó Nintendo *brand*-nek köszönhetően a Game Boy kora legsikeresebb kézi konzolja lett, annak ellenére, hogy a versenytársaihoz (Atari Lynx, Sega Game Gear) mérten elavult technológiát használt. Ez egyben azt is jelentette, hogy a Game Boy-ban használt alkatrészek olcsóbbak, ismertebbek és kiforrottabbak voltak, mint a riválisoké. A tervezők alapgondolata az volt, hogy régebbi technológiát használnak fel innovatív módon. A konzol sikerét az olcsósága, az akkumulátor időtartama, és a platformon elérhető rengeteg játék mennyisége és minősége koronázta meg. Az 1997-ig értékesített 60 millió példányszám a Game Boy-t a gyártó egyik legsikeresebb termékévé tette. A készülék jellegzetes logója a 1.1-es ábrán látható.

1.2.2. Hardver specifikáció

A hardver specifikációját két logikai egységre lehet osztani: a Game Boy hardverére és a *cartridge* hardverre. Ugyan ezek együtt alkotnak egészet, hiszen egyik sem használható a másik nélkül, ám technikailag két különálló egységről beszélhetünk.

Game Boy

A konzol külseje, és kezelőszervei a 1.2-es ábrán figyelhetők meg, az általa tartalmazott hardver elemek pedig a következők[2]:

- **CPU:** a 8 bites Zilog Z80-as CISC-processzor architektúrán alapuló – annak utasításkészletén enyhén módosított változata – Sharp LR35902.
- **RAM:** 8 kB beépített S-RAM
- **VRAM** (video memória): 8 kB beépített
- **ROM:** 256 Byte (Boot ROM-nak fenntartva)

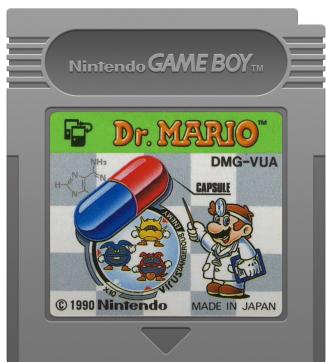
- **Hang**: 2 négyszögjel generátor, 1 programozható 32 mintás 4 bites PCM hullám, 1 fehér zaj, és egy audio bemenet a kazettából. (A külső kazetta bemenetet soha egy piacra dobott játék sem használta.) A jack kimeneten keresztül sztereó hangot ad.
- **Kijelző**: 166×144 pixel felbontású LCD kijelző, mérete átlósan 66 mm.
- **Színpaletta**: 4 árnyalat 2 biten tárolva – világos zöldtől a sötét zöldig.
- **Tápellátás**: 4 db AA elem, amely megközelítőleg 14-35 óra játékidőt biztosít.



1.2. ábra. A Game Boy és részei

Cartridge

A konzolhoz tartozó játék kazettákat a konzol hátuljába kellett címkkével kifelé fordítva becsúsztatni. Ezek a kazetták jól felismerhetők voltak a jellegzetes (nagyrészt) szürke színükről, illetve az elejükre ragasztott, az adott játékot ábrázoló címkéjükön, ami a 1.3-es ábrán is megfigyelhető. A Game Boy-hoz több típusú kazetta volt forgalomban, melyet az indokolt, hogy némely játék nagyobb erőforrást igényelt a futásához. A konzolnak köztudottan kicsi volt a memória mérete, így a játékfejlesztőknek különféle trükköket kellett bevetniük ahhoz, hogy a játékaikat futásra bírják. Erre a problémára a *Memory Bank Controller* alkalmazása volt a megoldás, ennek használatával a fejlesztők számára nagyobb ROM, illetve *MBC* verziótól függően nagyobb RAM volt elérhető. Az *MBC* részleteiről és típusairól az egyik későbbi fejezetben lesz szó.



1.3. ábra. A *Dr. Mario* játék kazettája

A kazetták többségében volt egy CR2025-ös típusú gombelem is, ami az elmentett játékállások tárolásából adódó erőforrás-ellátásért felelt. Az elem viszont nem tartott örökké – így mikor hosszú idő után ugyan, de lemerült, az összes mentett állás elveszett.

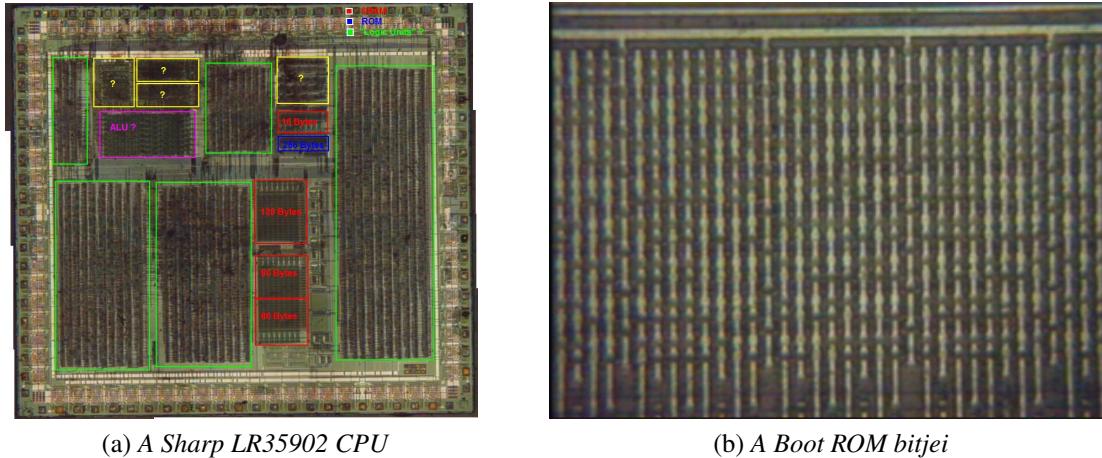
További érdekesség még a *cartridge*-ekkel kapcsolatban a Nintendo által kifejlesztett korabeli (de meglepően hatékony) másolásvédelmi és *homebrew*²-fejlesztőket kizáró mechanizmus. Annak érdekében hogy a kazettákat ne lehessen lemásolni és így terjeszteni, illetve a gyártóval kapcsolatba nem lépő hobbi fejlesztők ne tudjanak játékot kiadni a platformra, a Nintendo szokatlan, de hatékony megoldást választott. Amikor a felhasználó behelyezi a kazettát a Game Boy-ba, és bekapcsolja azt, akkor a Boot

ROM lefutását követően a játék csak akkor indul el, ha a játék kódjában megtalálhatók a Nintendo logót alkotó byte-ok. Ha ez hiányzik, akkor a játék nem fog futni. A trükk az, hogy ugyan a törvény nem tiltja, hogy játékokat fejlesszenek a hobbi fejlesztők a konzolra, viszont a Nintendo logó felhasználását szerzői jogi törvények védik. Így, ha a hobbi fejlesztő terjesztené a játékát, akkor be kell ágyaznia a Nintendo logót a kódba, amivel viszont szerzői jogi szabályokat sért. Ezzel a Nintendo elérte, hogy a konzolra kiadott játékok minősége magas legyen, hiszen minden játék kiadásáról végső soron ők döntöttek.

1.2.3. Boot ROM

A Nintendo Game Boy Boot ROM-ja végzi a hardver elindulását követő inicializáló folyamatokat, illetve az előző részben említett másolásvédelmi eljárást. A ROM pontos tartalma egészen 2003-ig ismeretlen volt – ekkor viszont egy *Neviksti* nevű felhasználó publikálta a *cherryroms.com* fórumára a program teljes változatát. *Neviksti* azt is leírta, hogy hogyan sikerült visszafejtenie a kódot: a Game Boy processzor chip tetejének leszedése után mikroszkóppal megvizsgálta az áramkört, majd amint megtalálta a Boot ROM

² A *homebrew* fogalmat azokra a videojátékokra vagy egyéb szoftverekre használjuk, amelyeket a fogyasztói réteg készít el a zárt forrású hardverekre, platformokra – tehát nincsenek kapcsolatban a célhardver gyártójával.



(a) A Sharp LR35902 CPU

(b) A Boot ROM bitjei

1.4. ábra. A CPU és a Boot ROM

lehetséges helyét (256 kB ROM van elkülönítve erre a CPU-ban), lefényképezte azt, majd bitről bitre haladva rekonstruálta a bináris állományt. A teljes processzor madártávlati nézete a 1.4-es ábrának (a) részén látható, a belenagyított (b) ábrán pedig az áramkör Boot ROM-ot tároló része szerepel, amin szemmel is jól láthatók a programot alkotó bitek.

2. fejezet

A fejlesztési folyamat

Ahogy már az előző fejezetekben is említésre került, az emulátor fejlesztői szubkultúrában többé-kevésbé kialakult egyfajta irányelv, amit érdemes követni az emulátor fejlesztésénél. Természetesen olyan leírást nem lehet készíteni ami bármilyen konzol emulátorának fejlesztésére használható – a hardverek különbözősége és a speciális megoldások nem teszik ezt lehetővé. Azt viszont meg lehet tenni, hogy egy általános tervezési mintát meghatározunk, és a tervezésnél - implementálásnál ezt követjük.

Az első teendő mindenkorban a lehető legtöbb tudásanyag összeszedése ilyen-olyan forrásokból: internetről, régi szaklapokból, esetleg magát a hardvert tanulmányozva. Nagy segítséget jelenthet például ha már valaki belekezdett ugyanazon hardver emulátorának fejlesztésébe, hiszen fontos információkkal szolgálhat. Egyes hardver emulátorok köré közösségek is összegyűlnek: így van ez a Game Boy esetén is. Ez a közösség egy honlapon gyűjtötte egybe az elérhető összes – eddig fellelt – információt a konzolról. A legfontosabb dokumentum azonban minden emulátor fejlesztése kapcsán a processzor dokumentációja, hiszen – ahogy majd látni a későbbiekben erre ki is térek – ezt fogjuk először implementálni. Mielőtt az implementációs szakaszba lépnénk, célszerű átgondolni az emulátor leendő struktúráját, működését, illetve az alkalmazott eszközöket. Továbbá az elvárt működést, az *inputot* és az *outputot* is át kell gondolni a tényleges fejlesztési munkálatok előtt.



2.1. ábra. Az emulátor architektúrája

A 2.1-es ábrán látható módon fog alakulni az emulátor felépítése, architektúrája. Ahogy az jól megfigyelhető, a CPU áll a középpontban, ez tartalmazza a fő ciklust is. A többi modul ehhez csatlakozva, de külön álló egységként képzelhető el. Ennek megfelelően a fejlesztést a processzor megvalósításával kell kezdeni, majd a különálló modulok implementálásával folytatni. Ezen részegységek fejlesztésének időrendi sorrendje többnyire szabadon megválasztható, viszont célszerű a CPU - MMU - IRQ - PPU sorrendet követni. A 2.1-es alfejezetben lesz szó az emulátor "magjáról", a fő ciklusról, amely a processzor (és így a többi modul) alapját képezi.

2.1. A fő ciklus

A fő ciklus a Game Boy utasítás-végrehajtását emulálja, aminek egy leegyszerűsített modellje bármilyen Neumann-elvű számítógép processzorára illeszkedni fog. Ezt a fő ciklust elterjedtebb nevén **betöltő-dekódoló-végrehajtó** ciklusnak is nevezik. Lépései a következők[1]:

1. A soron következő utasítás betöltése a memóriából az utasításregiszterbe.
2. Az utasításszámláló (másnéven *Program Counter*, vagy PC) beállítása a következő utasítás címére.
3. A beolvasott utasítás típusának meghatározása.
4. Ha az utasítás memóriabeli szót használ, a szó helyének meghatározása.
5. Ha szükséges, a szó beolvasása a CPU egy regiszterébe.
6. Az utasítás végrehajtása.
7. Vissza az 1. pontra.

A fenti szerkezet valamilyen módon minden emulátorban megtalálható, ez a felépítés alapja. A ciklus addig ismétlődik, amíg egy HALT, vagy egyéb kilépést/megállást szolgáló utasítás nem érkezik végrehajtásra. Természetesen a megszakításkezelő valamelyest bele-szól a ciklus működésébe, de erről majd egy későbbi fejezetben lesz szó.

A Game Boy emulátorban a fenti szerkezet egy egyszerűbb változata működik, ami vázlatszerűen így néz ki:

```
loop { // endless loop
    let next_byte = fetch_byte();
    let instruction = decode_instruction(next_byte);
    execute(instruction);
}
```

A fenti függvényeket, és azok működését a későbbiekbén fogom részletezni.

A fő ciklus megtervezése tipikusan a CPU alap struktúrájának (regiszterek, RAM, stb.) implementálása után következik. Ezek után jöhet csak a legtöbb emulátor leghosszabb és legrepetitívebb része: a CPU műveleteinek implementálása.

2.2. Alkalmazott eszközök

A fejlesztéshez alkalmazott eszközök meghatározása fontos tényező, hiszen nagyban megkönnyíthetjük vagy megnehezíthetjük a saját munkánkat. Először is célszerű egy programozási nyelvet választani, lehetőség szerint olyat, amihez léteznek olyan *library*-k, amelyekkel megvalósítható a program. Emellett az is lényeges, hogy a programozási nyelv gyors binárist generáljon – természetesen megvalósíthatjuk az emuláltot *Javascript* nyelven is, csak észrevehetően lassabb lesz, mint mondjuk a C++-os variánsa.

A programozási nyelv mellett a *debug*-olást nagyban megkönnyíti egy *disassemblers*, vagy optimális esetben egy másik emulátorhoz készített *debugger*. A ROM fájlokhoz szükséges lehet még egy *hex editor*¹, hogy pontosan lássuk azt, hogy milyen bájtokkal dolgozunk. Ahhoz hogy lássuk, hogy a memóriában milyen adatok szerepelnek, célszerű egy memóriatérkép eszközt készíteni a fejlesztés során.

2.2.1. A Rust programozási nyelv

Az emulátor fejlesztéséhez a Rust programozási nyelvet választottam, több okból. Egyrészt ez előtt egy kisebb emulátor projekten dolgoztam a nyelvvel, és már akkor megtetszett az egyszerűsége, a környezete, a nyelv köré alakult közösségi. Másrészt a nyelvet az ehhez hasonló performancia-orientált feladatokra terveztek.

A **Rust** a fejlesztők weboldala szerint egy 2006 óta fejlesztett, rendszerfejlesztésre készített nyelv, amely villám gyorsan dolgozik, megelőzi a szegmentációs hibákat, és garantáltan gátolja a versenyhelyzetek kialakulását. Erősen típusos nyelv, szintaktikailag a C++-hoz hasonlít, viszont hozzá képest biztonságosabb memóriakezelést biztosít a sebesség megtartásával. A Rust világában tehát nincsen null pointer, lógó pointer, és versenyhelyzet sem. A fejlesztését és tervezését a Mozilla kutatói részlege kezdte el, majd idővel közösségi projektté alakult. Jelenleg 1.24.1-es jelzésű az aktuális verzió.

Fontos még megemlíteni, hogy a *Stack Overflow* weboldalon megrendezett éves fejlesztői kérdőív kitöltések alapján 2016-ban, 2017-ben és 2018-ban is a Rust nyerte a "leginkább kedvelt programozási nyelv" kategóriát. Egyéb érdekesség, hogy jól megfigyelhető, hogy az emulátor fejlesztő közösségi túlnyomó többsége vagy C++-ban, vagy Rust-ban fejleszt – ez a nyelv kényelmességének, eleganciájának és sokoldalúságának is köszönhető.

Maga a nyelv szépsége azonban még minden – a nyelv mellett a **Cargo** eszköz egy fontos szempont. A Cargo nyilván tartja és rezolválja a Rust projektekben összeszedett függőségeket, illetve *buildeli* a projektet. Két *metadata* fájlban tárolja a projekttel kapcsolatos információkat, melyek alapján beszerzi és buildeli a projekt függőségeit. Ezt követően meghívja és futtatja a *rustc* fordítót a megfelelő paraméterekkel. A Cargo a külső *library*ket, illetve függőségeket a *crates.io* közösségi központi repozitóriumból szerzi be.

¹A *hex editor* egy olyan szoftver, amely segítségével megtekinteni és módosítani lehet egy bináris adatfájlt. A "hex" előtag a hexadecimális rövidítésből ered: a bináris fájl bájtjait 16-os számrendszerben mutatja a program.

2.2.2. A `minifb` könyvtár

Mivel grafikus programról beszélünk, ezért az ablakkezelés és az emulátor vizuális *outputja* fontos tényező. Ehhez – ha lehetséges – minél egyszerűbb és gyorsabb külső könyvtárat kell használnunk, ha szeretnénk megkönnyíteni és felgyorsítani a munkafolyamatunkat. A `minifb` crate ezt teszi lehetővé, hiszen ez egy platformfüggetlen, Rustban írt *library*, amivel az operációs rendszer által kínált natív ablakokat lehet megnyitni, és feltölteni egy 32 bites *bufferrel*. Támogatja a billentyűzet és egér eseménykezelést, és némely operációs rendszer esetén (Windows, macOS) a menürendsereket.

A használata nagyon egyszerű:

```
window : Window::new("RUST BOY",  
                     160, // name  
                     144, // width  
                     WindowOptions { // height  
                         resize: false,  
                         scale: Scale::X2,  
                         ..WindowOptions::default()  
                     }.unwrap()  
}
```

Amint látható, négy kötelezően megadandó paramétere van a `Window` struktúra konstruktornak, melyek rendre:

- `name`: az ablak címsorában szereplő szöveg,
- `width`: az ablak szélessége pixelben,
- `height`: az ablak magassága pixelben,
- `WindowOptions`: az egyéb ablakbeállításokat tartalmazó struktúra.

A negyedik paraméternél kiválaszthatjuk, hogy a `default` ablakbeállításokat szeretnénk-e – amennyiben igen, `WindowOptions::default()`-ot kell megadni. Ha saját beállításokat kívánunk megadni ebben a `WindowOptions` struktúrában, rendre ezek közül választhatunk:

- `borderless`: ezzel megadható, hogy az ablaknak legyen-e kerete vagy sem,
- `title`: ezzel megadható, hogy az ablaknak legyen-e címe vagy sem
- `resize`: ezzel megadható, hogy az ablak átméretezhető legyen-e vagy sem
- `scale`: ezzel a struktúrával megadható, hogy az ablak mekkora nagyítással jelenjen meg, választható opciók: X1, X2, X4, X8, X16, X32.

A konstruktor meghívását követően az ablak tartalmát (és a `framebuffert`) a következőképpen frissíthetjük:

```
window.update_with_buffer(&framebuffer).unwrap();
```

ahol a `&framebuffer` egy `&[u32]` típusú, `u32` számokat tároló, `width * height` méretű tömbre mutató referencia. A tömbben lévő számok tárolják el az adott pixel színét az ablakban: hexadecimálisan megadva az első két karaktert figyelmen kívül hagyjuk, majd az utána következő 6 karakter adja a szín hexadecimális megfelelőjét:

`FF FF FF FF`

A fentiek alapján látszik, hogy a második `FF` tag a piros (R), a harmadik `FF` tag a zöld (B), a negyedik `FF` tag pedig a kék (B) színért felel. Külön-külön tehát az RGB kódokat, még együtt a hexadecimális színkódot kapjuk.

2.2.3. Fejlesztői környezet

A fejlesztést *elementary OS*² rendszeren végeztem. Az emulátor fejlesztés sajátosságai miatt feleslegesnek éreztem egy IDE³ használatát, hiszen ha a programkód szintaxisa megfelelő, onnantól kezdve a hibakeresést az IDE-k által kínált eszközök sem tudják megkönnyíteni, ahhoz saját *debuggert* kell írni. Ilyen fejlesztői környezet használata helyett tehát a klasszikusnak mondható szövegszerkesztő (Atom, Rust *linterrel*⁴) és terminál párost használtam, a `rustc` fordító *warningjaira* és *errorjaira* hagyatkozva.

A `rustc` fordító *targetjeként* a `stable-x86_64-unknown-linux-gnu` beállítást használtam (alapbeállítás), ami a "hagyományos" 64 bites Linux disztribúcióra optimalizált fordítási paraméterezés. A fordítást, futtatást és a külső függőségek (*libraryk*) beszerzését a Cargo eszközzel valósítottam meg.

2.2.4. Debugger

Fontos eszköz volt a fejlesztés során a *debugger*, amelyet az emulátorral párhuzamosan fejlesztettem. Nagyon hasznos, hogy pontosan végig lehet követni az emulátor működését, és az egyes processzorműveletek után beállt állapotokat, hiszen ez nagyban megkönnyíti a hibakeresést. A 2.2-es ábrán láthatjuk az eszköz működés közben: bal oldalon találhatóak a már elvégzett műveletek, a jobb oldal pedig a regiszterek állapotát mutatja.

Az elvégzett műveletek listájában legfelül a legutóbb végrehajtott művelet szerepel, a végén pedig a legrégebbi. A program az utolsó 50 állapotot tudja eltárolni, melyek közül az éppen kijelölt, aktív elemet piros kiemelés jelzi. Az egyes listaelemek az alábbi módon épülnek fel:

`0x21 : LD HL,nn 0xFF 0xE6`

A `0x21` jelzi az aktuális művelet *opkódját*⁵, mellette szerepel a művelet *mnemonikja*⁶, jelen esetben az `LD HL, nn`. A harmadik tag a művelet által beolvasható, és (operandusként) felhasznált bájtokat tartalmazza, itt: `0xFF 0xE6`. A példában (és a *debuggerben*

² Az *elementary OS* egy *Ubuntu* alapú Linux disztribúció.

³ Az integrált fejlesztői környezet (angolul IDE, azaz Integrated Development Environment) a neve a számítógép-programozást jelentősen megkönnyítő, részben automatizáló programoknak.

⁴ Olyan eszközöket nevezünk *linternek*, amelyek a forráskódot analizálva programozási hibákat, *bugokat*, stílusbeli hibákat, vagy gyanús felépítéseket jeleznek a felhasználónak.

⁵ Operációkód, azaz műveleti kód, vagy műveleti jelkód, utasításkészletek leírásában műveleti jelrész. A CPU által beolvasható bináris szám, amit végrehajtható utasítás kódjaként értelmez.

⁶ A mnemonik az informatikában általában hosszabb elnevezésű művelet(sor) elnevezésére használatos rövidítés, amelyet az egész kifejezés helyettesítésére alkalmaznak, pl.: ADD, SUB.

0x34 : INC (HL)	A 0x00	B 0x00
0x21 : LD HL,nn 0xFF 0xE6	C 0x08	D 0x00
0x34 : INC (HL)	E 0x10	F 0x00
0x21 : LD HL,nn 0xFF 0xE5	H 0xFF	L 0xE6
0x34 : INC (HL)	SP 0xFFFF	
0x21 : LD HL,nn 0xFF 0xE2	PC 0x354	
0x20 : JR M2	FLAG 0b0000	
0x05 : DEC B		
0x2C : INC L		
0x28 : JR Z, 0x1		
0xA7 : AND A,A		
0x7E : LD A,(HL)		
0x20 : JR M2, - 0x9		
0x05 : DEC B		
0x2C : INC L		
0x28 : JR Z, 0x1		
0xA7 : AND A,A		
0x7E : LD A,(HL)		
0x06 : LD B, 0x2		
0x21 : LD HL,nn 0xFF 0xA6		
0x20 : JR M2, 0x1B		
0xFE : CP A, 0xF		
0xFF : AND A, 0xF		

2.2. ábra. Az emulátorhoz fejlesztett debugger

is) be van színezve az utasítás – ennek egyszerű oka van: az utasításokat kategóriákra bontottam, majd külön színeket rendeltem hozzájuk, így már ránézésre is meg lehet mondani, hogy milyen típusú műveletről van szó. A mellékletként csatolt opkód táblázatban lévő színek megegyeznek a *debuggerben* látható színekkel.

A *debugger* jobb oldalában foglal helyet a regiszterek nézete, itt található meg rendre az összes regiszter, a *Stack Pointer*, és a *Program Counter* értéke, valamint az F *Flag* regiszter értéke binárisan – hogy látható legyen az összes általa tartalmazott flag állapota. Ezen értékek annak függvényében változnak (és mutatják az aktuális értékeket), hogy épp melyik művelet van kijelölve.

2.2.5. Memóriatérkép

A *debugger* mellett a másik sokat használt eszköz a memóriatérkép. Ebben az ablakban megjelenik a Game Boy memóriájának összes bájtja, egy-egy pixel által reprezentálva. Az adott pixel világos, ha a bájt nulla, egyébként pedig sötétebb árnyalatú. A 2.3-es ábrán megfigyelhető, hogy több féle szín is megjelenik – ezek jelölik az egyes fontosabb, elkülönölt részeket a memóriában. A színeket is bevonta a reprezentációba a *debuggerhez* hasonlóan ennél az eszközönél is ránézésre leolvashatók adatok. Ahhoz, hogy pontosan megtudjuk egy adott bájt értékét és pozícióját a memóriában, rá kell kattintani, és a terminál ablakban kiírásra kerülnek a szükséges információk. A kiírt adatok a következő formában jelennek meg a terminál ablakban:

BYTE : 0x46 0b01000110 – POSITION : 0x7984

Értelemszerűen a BYTE után szereplő két szám az egérrel kijelölt bájt értékét mutatja, míg a POSITION után szerepel a bájt helye a memóriában.



2.3. ábra. Az emulátorhoz fejlesztett memóriatérkép eszköz

A Game Boy architektúrájában gyakori, hogy egyes regiszterek a memóriában kapnak helyet – erről a későbbiekben szó lesz –, és a memóriatérkép megoldással könnyedén meg lehet figyelni ezek értékeit, esetleg változásait. Emellett a dedikált és külön színnel kiemelt memória részeiken látszik, hogy fel van-e töltve, vagy teljesen üres – egy *sprite* renderelési *bug* kijavítását nagy mértékben megkönnyítette az, hogy látszott a memóriatérképen a *spriteok* hiánya.

2.3. A feladat specifikációja

Az emulátornak a feladatkiírásban meghatározott feltételeket kell teljesítenie, azaz:

- a CPU utasításokat és működését,
- a PPU renderelésének működését,
- a memóriakezelést,
- a megszakításvezérlést.

Ahhoz, hogy ezeket a feltételeket teljesíteni tudja, szükséges az *input* és *output* adatok (működés) pontos meghatározása.

Az input elvárt formai és tartalmi követelményei:

Az emulátor *inputjaként* a Game Boy DMG⁷ videojáték konzolhoz írt videojátékok ROM-jait adhatjuk meg, illetve a visszafejtett Boot ROM-ot. Videojátékok esetén az emulátor csak a MBC (*Memory Bank Controller*) nélküli ROM-okat képes futtatni. Előfordulhatnak olyan nem ismert, videojáték programozók által kihasznált *bugok*, amelyek gátolják a

⁷ Az eredeti, klasszikus 1989-ben kiadott Game Boy kódneve DMG.

ROM tökéletes futtatását. Szükséges hogy a ROM tartalmazza a *headerjében* a Nintendo logó bájtjait (a Boot ROM-ban lévő *checksum* kiszámolja ezt), mert ellenkező esetben a játék nem fog elindulni.

Inputnak tekinthetők még az emulált *joypaden* történő gombnyomások is, melyek hatással vannak az emulált szoftver működésére. A felhasználó egyszerre több gombot is lenyomhat – ennek emulációja megfelel az eredeti hardverével.

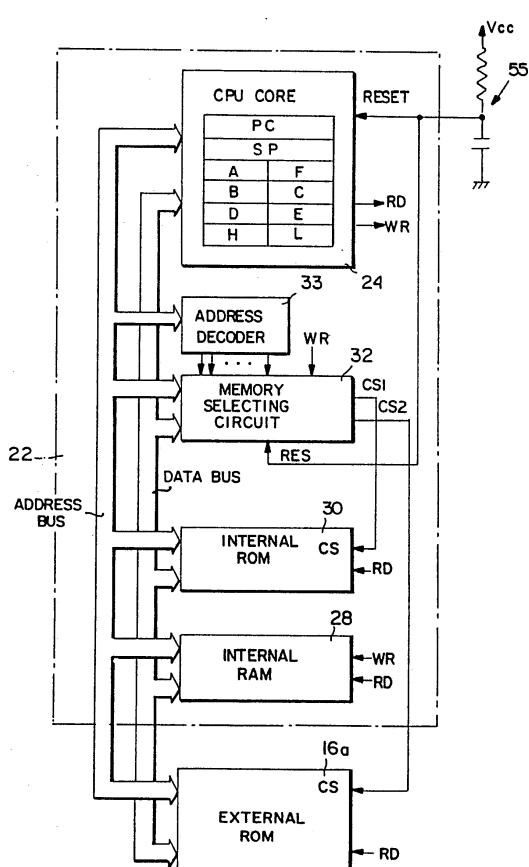
Az output elvárt formai és tartalmi követelményei:

Az emulátor több féle *outputot* is előállít. A legfontosabb az emulált kijelzőre renderelt kép, amelynek meg kell egyeznie az eredeti konzol által kirajzolt képpel. A korhűség érdekében célszerű a 4 féle árnyalatot a konzol folyadékkristályos kijelzőjének jellegzetes zöld színeivel megegyező színekkel megjeleníteni.

Egyéb *outputnak* tekinthetjük a *debugger*, és a memóriatérkép által adott információkat is, hiszen az emulátor aktuális állapotáról a dnak visszajelzéseket. Természetesen ezek elhanyagolhatóak, de a hibakeresést – és így a fejlesztést – segítik.

3. fejezet

A processzor és a memória implementációja



3.1. ábra. A Game Boy szabadalmában ábrázolt processzor felépítés

függelék 4.1-es ábráját, amely szintén a Nintendo által benyújtott szabadalom része. Ez az ábra később nagy segítségünkre lesz a modulok felépítésének, és a rendszer struktúrájának implementálása során, hiszen elég részletesen mutatja be az egyes elemek közti kapcsolatokat, kommunikációt.

A korábban írtaknak megfelelően az implementációt a processzorral és a memóriával kezdjük – a megfelelő tudásanyag birtokában a processzor felépítésének modellezése az első feladat. Fontos már a korai tervezési folyamatotól kezdve szem előtt tartani a belső felépítés modelljét, és ennek tudatában úgy alakítani az implementálást, hogy egyrészt az eredeti hardverrel nagyrészt megegyező módon működjön (és épüljön fel), másrészt a további modulok, egységek és funkciók jól illeszkedjenek ehhez a fő komponenshez. Ehhez nyújt nagy segítséget a Nintendo által bejegyzett Game Boy szabadalmban ábrázolt felépítés, amit a 3.1-es ábrán figyelhetünk meg. Jól látszik a processzor és a memória kapcsolata, illetve ez előbbi felépítésébe is nyújt némi betekintést, utóbbinak egyes részeit pedig már ezen az ábrán is láthatjuk, a későbbiekben ezt jobban meg is vizsgáljuk. Az előző fejezetben ismertetett betöltő-dekódoló-végrehajtó ciklust alkotó elemek közül is megfigyelhetjük az utolsó kettőt. A hardver teljes felépítéséről tágabb képet kaphatunk, ha megfigyeljük a 4. fejezetbeli

3.1. CPU

3.1.1. Regiszterkészlet

Ahogy az első fejezetben már említésre került, a Game Boy-ban egy *Zilog Z80* alapú, *Sharp LR35902* típusú 8 bites processzor dolgozik. A Z80-hoz képest annyi változás történt, hogy a regiszterek elrendezését a *Sharp* mérnökei az *Intel 8080*-as processzortól vették kölcsön, illetve több utasítást is kivettek, helyükre sajátokat téve.

A 3.1-es ábrán látható, hogy a processzor nyolc darab 8 bites, és két darab 16 bites regiszterrel rendelkezik. A 8 bitesek név szerint: A, F, B, C, D, E, H, L, míg a 16 bitesek a PC és az SP. A 8 bites regiszterek felsorolásának sorrendje nem véletlen: a CPU egyik igen hasznos funkciója az, hogy regisztereket tud összevonni, két 8 bitesből 16 biteseket varázsolva – így ezekben a nagyobb regiszterekben el lehet tárolni memóriacímeket, vagy egyéb 16 bites adatokat. Az összevont regiszterek rendre: AF, BC, DE, HL.

Az A regiszter hagyományosan az akkumulátorregiszter¹, míg az F tárolja a *flageket*.

7	6	5	4	3	2	1	0
Z	S	H	C	0	0	0	0

3.1. táblázat. Az F Flag regiszter bitjei

A 3.1-es táblázatról leolvashatók az F regiszter *flagjainak* helyzete. A rövidítések jelentései a következők:

- *Z*: *Zero Flag*, értéke akkor 1, ha valamilyen logikai vagy aritmetikai művelet eredménye 0.
- *S*: *Subtract Flag*, értéke akkor 1, ha valamilyen kivonás műveletet végzett a processzor.
- *H*: *Half Carry Flag*, értéke akkor 1, ha valamilyen logikai vagy aritmetikai művelet során az akkumulátorregiszter alsó 4 bitjén túlcordulás vagy alulcsordulás keletkezett.
- *C*: *Carry Flag*, értéke akkor 1, ha valamilyen logikai vagy aritmetikai művelet során az akkumulátorregiszteren túlcordulás vagy alulcsordulás keletkezett. Nem összekeverendő a *Half Carry Flaggel*.

Az alsó 4 bit használaton kívüli, minden 0. Ezeket a *flageket* a processzor utasításai vezérlők a művelet kimenetétől függően. Az emulátor fejlesztése szempontjából ez egy kritikus pont – a *flagek* pontos emulációján nagyon sok műlik, elképesztő mennyiségű hibakeresést spórolhatunk meg magunknak azzal ha odafigyelünk az implementációkor. Érdemes készíteni a CPU struktúrába *flag* beállító és lekérdező függvényeket is az utasítások implementálásához.

A két 16 bites regiszter szerepe megegyezik ehhez hasonló architektúrákban tapasztalatakhoz: a PC, azaz *Program Counter* azt mutatja, hogy a processzor hol tart az utasítási

¹ Olyan regiszter, amiben az aritmetikai-logikai egység által végzett műveletek operandusai, illetve az eredmény átmenetileg tárolódi.

sorban (a memóriában), míg az SP, vagy *Stack Pointer* mutatja a hívási verem (*Call Stack*) aktuális címét, azaz hogy éppen hol helyezkedik el a memóriában a verem legfelső eleme. Érdemes megjegyezni, hogy a verembe pakoláskor – azaz a PUSH művelet hívásakor – a verem új, legfelső elemét a memóriában lefelé haladva szúrjuk be, azaz a legkisebb memória című verembeli elem képzi a verem tetejét.

Ami az implementációt illeti, a 8 bites regisztereket 8 bites *Unsigned Integer*ként, azaz u8-ként, a 16 biteseket pedig u16-ként deklaráltam, hiszen negatív értéket nem fog felvenni egyik regiszter sem. A processzort modellező struktúra tehát ilyen módon fog kinézni:

```
pub struct CPU {
    pub A : u8,
    pub B : u8,
    pub C : u8,
    pub D : u8,
    pub E : u8,
    pub F : u8,
    pub H : u8,
    pub L : u8,
    pub SP : u16,
    pub PC : u16,
    pub RAM : [u8; 65536],
}
```

3.1.2. Ciklusok, frekvenciák

A Nintendo Game Boy processzorának frekvenciája 4.194304 MHz. Azonban az egész rendszer a memóriához kötött, tulajdonképpen a memória elérésének sebessége meghatározza az összes egység sebességét is. Jelen esetben a memória az architektúra szűk keresztmetszete, ugyanis ~1 MHz sebességgel működik. A hardver egyes komponenseinek sebessége az alábbiak szerint alakul:

CPU	4,194,304 Hz = ~4 MHz
RAM	1,048,576 Hz = ~1 MHz
PPU	4,194,304 Hz = ~4 MHz
VRAM	2,097,152 Hz = ~2 MHz

3.2. táblázat. A Game Boy fő elemeinek sebessége

A fenti 3.2-es táblázaton látható, hogy az alkotóelemek sebességei nem egységesek, viszont hiába gyors a processzor, ha a memória visszafogja a rendszert. Így praktikussági okokból kétféle ciklust különböztetünk meg:

- az *órajel ciklust*, ami a specifikációban írt 4,194,304 Hz (azaz 4 MHz)-nek felel meg,

- és az *gépi ciklust*, ami megegyezik a RAM frekvenciájával, így 1,048,576 Hz (azaz 1 MHz) lesz.

Ettől a ponttól kezdve az utasítások időszítését gépi ciklus szerint tekintjük, és a ciklus kifejezés alatt a gépi ciklust értjük. Az oka ennek az, hogy az 1 MHz-es gépi ciklus minden komponens sebességére visszavezethető, egyfajta közös nevezőnek tekinthető.

3.1.3. Betöltés - dekódolás - végrehajtás

A betöltés-dekódolás-végrehajtás ciklus függvényeit az Opcode struktúra tartalmazza. A betöltést a `fetch` függvény valósítja meg, amely visszatér a CPU RAM-ot reprezentáló tömbjének PC regiszter értékével megegyező indexű elemével (amely `u8` típusú). A dekódolás és a végrehajtás műveletek az `execute` függvényben történnek. A `fetch` által visszatérít bájt dekódolása úgy történik, hogy az Opcode struktúra rendelkezik egy `opc` és egy `cb_opc` tömbbel, a processzor műveletet azonosító bájtot átadjuk az `opc` tömb számára, mint tömbindex. Az `opc` és a `cb_opc` tömbök rendre 256 eleműek, és függvényekre mutató pointereket tartalmaznak, így a bájt tömbindexként való használatával meghívható az adott opkóhoz tartozó utasítást megvalósító függvény.

Amennyiben CB prefixű opkód az aktuális utasítás, úgy először az `opc[0xCB]` által mutatott függvény hívódik meg, amely meghívja a `fetch` függvényt, hogy az betöltsse a CB prefixű táblán értelmezett művelet opkódját. Ugyaninnen hívódik meg a konkrét műveletet megvalósító függvény a `cb_opc` függvény pointer tömb használatával.

A processzor műveleteit megvalósító függvények visszatérési értéke egy `u8` szám, amely azt mutatja, hogy a konkrét művelet teljes végrehajtása hány processzor ciklus alatt történik meg. Az Opcode struktúra `execute` függvénye ezt az értéket szintén visszatérési értékként fűzi tovább.

A processzor a fenti műveleteket hívja meg a ciklus minden egyes iterációjában, majd a műveletek által visszaadott műveleti ciklus értékeit összeadva szinkronizálja össze a művelet végrehajtást a *rendereléssel*. A 60 FPS² renderelési sebességet céloztam meg, amely az eredeti konzol képernyőfrissítési értékével is nagyságrendileg megegyezik. A *renderelés* ideje így a következő számítás alapján megkapható:

$$4194304/60 = 69905,$$

ahol a 4194304-es érték a processzor órajel ciklusa, a 60 jelzi az FPS értéket, a végeredmény pedig megmutatja, hogy mekkora összegig kell folytatni a processzor műveleteinek végrehajtását. A fő ciklus sémája kiegészítve a szinkronizált PPU *rendereléssel* tehát így alakul:

```
loop { // endless loop
    while cycle <= 69905 {
        cycle += opcode.execute();
    }
    ppu.render();
}
```

² *Frames Per Second*, azaz képkocka per másodperc – a *renderelés* frissítési gyakoriságát megadó mértékegység.

3.2. Interrupt kezelés

Az utasításkészlet részletes bemutatása előtt fontos szót ejteni a Game Boy *interrupt* kezeléséről – több utasítás kapcsán is elő fog jönni ez a téma.

Adott események bekövetkezése (ez hardverenként eltér) *interruptot*, vagy **megszakítást** vált ki, ezzel kényszeríti a CPU-t, hogy az éppen futó programot azonnal felfüggesse, és egy speciális eljárást, a **megszakításkezelőt** végrehajtsa, amely a hibaellenőrzést és egyéb speciális teendőket elvégezve értesíti a vezérlőt, hogy a megszakítás befejeződött.[1]

A Nintendo Game Boy architektúrájában kétféle megszakítást különböztetünk meg: létezik szoftveres, és hardveres megszakítás is. Ami a szoftveres megszakításokat illeti, ezeket a hardver programozói használhatták, az egyes RST (a RESET rövidítése) műveletekkel lehet előre definiált memóriacímekre ugrani. A hardveres megszakítások témaköre már kicsit bonyolultabb.

Alapvetően 5 féle hardveres megszakítást különböztetünk meg:

- *V-Blank*: A képernyő frissítése során periodikusan előidézett megszakítás, a későbbiekben – a PPU-t taglaló fejezetben – részletesebben is szó lesz róla.
- *LCD STAT*: Többféle esemény is előidézheti ezt a típusú megszakítást, az egyik leggyakoribb ezek közül az, amikor a hardver egy adott sor újratárolásánál tart az LCD kijelzőn.
- *Timer*: Akkor következik be ez a megszakítás, amikor a *TIMA* időzítő regiszter túlcordul. A későbbiekbén erre is kitérek.
- *Serial*: A hardveren található soros port működése közben következik be a *Serial* megszakítás, ha egy konkrét adatátvitel befejeződött. Ezen emulátor esetében ezt a megszakítást nem implementáltam.
- *Joypad*: Ez a megszakítás bármelyik hardveres gomb lenyomásakor aktiválódik.

A megszakításokhoz a CPU kapcsán három dolog köthető a fentieken kívül. Egy fő interrupt kapcsoló, az *Interrupt Master Enable Flag*, amivel le lehet tiltani, vagy éppen engedélyezni lehet a megszakításokat *en bloc*, egy ún. *Interrupt Enable* regiszter, ahol külön-külön lehet engedélyezni vagy letiltani az egyes megszakításokat, illetve egy *Interrupt Flag* regiszter, amiben a megszakítási sorban várakozó, még (a CPU által) teljesítetlen megszakítások szerepelnek.

0xFFFF	Interrupt Enable	Jump Location	0xFF0F	Interrupt Flag
4	<i>Joypad</i>	0x60	4	<i>Joypad</i>
3	<i>Serial</i>	0x58	3	<i>Serial</i>
2	<i>Timer</i>	0x50	2	<i>Timer</i>
1	<i>LCD STAT</i>	0x48	1	<i>LCD STAT</i>
0	<i>V-Blank</i>	0x40	0	<i>V-Blank</i>

3.3. táblázat. Az *Interrupt Enable* és az *Interrupt Flag* regiszterek megszakítások szerinti bit kiosztása, és a hozzájuk tartozó memóriacímek

Előfordulhat, hogy egyszerre több megszakítás érkezik. Ebben az esetben a prioritási sorrend az *Interrupt Flag* regiszterben elfoglalt helyek alapján alakul: a *V-Blank interrupt*

a legfontosabb, míg a *Joypad* megszakítás marad utoljára. Miután a prioritás alapján a megszakításvezérlő kiválasztotta, hogy melyik megszakítás következzen, a 3.4-as táblázaton szereplő adatoknak megfelelően az adott megszakításhoz tartozó memóriacímre ugrik a vezérlés.

Ami az implementálást illeti, a megszakítás vezérlő feladatait az `Interrupt` struktúra, és annak függvényei látják el. Az `IRQ` függvény segítségével tudnak az egyes modulok (PPU, időzítő, stb.) megszakítást kérni, melyet aztán a `handler` függvény dolgoz fel. A feldolgozás oly módon történik, hogy minden CPU művelet után a fő ciklusban meghívódik az `interrupt_checker` függvény, amely folyamatosan ellenőrzi, hogy érkezett-e új megszakítás, és hogy az engedélyezve van-e az *Interrupt Enable* regiszterben – ha igen, akkor a megszakítás azonosítóját paraméterként átadva meghívja a `handler` függvényt, amely a megszakításhoz tartozó memóriacímre ugrasztja a CPU-t.

3.3. Utasításkészlet

Ahogy azt már az előző alfejezetben ismertettem, az `Opcode` struktúrában implementált processzor műveletek visszatérési értéke egy `u8` típusú egész szám, amely a művelet végrehajtási idejével lesz egyenlő. Azt azonban még nem ismertettem, hogy hogyan néz ki egy utasítás sematikusan.

```
fn opcode_name_ff(&mut self, cpu : &mut CPU) -> u8 {  
    //...  
    4  
}
```

A fenti kódrészleten látható, hogy az egyes utasítások függvényeinek neve tartalmazza az utasítás nevét – *mnemonik* vagy bővebb alakban –, illetve az *opkódját*. A paraméterlistában szerepel a `&mut self` paraméter, amely a Rust nyelvben azt jelenti, hogy az adott függvény egy osztályfüggvény, és hogy módosíthatja az osztályt reprezentáló objektumot. A második paraméter (`&mut CPU`) pedig a fő CPU struktúrára mutató *mutable* referencia, azaz olyan `cpu` objektumot kapunk, amely módosítható – Rust nyelven *borrow*-oltuk, azaz kölcsön kaptuk az objektumot.

Sok esetben előfordul, hogy egy művelet egy vagy két operandussal rendelkezik, melyeket külön be kell tölteni a memoriából. Ezt a művelet függvényén belül tesszük meg a `fetch` metódus meghívásával.

3.3.1. Load utasítások - LD

A *Load*, azaz betöltő műveletek legnagyobb része nagyon egyszerűen működik: adott két regiszter – a példánkban legyen ez most X és Y –, ekkor a művelet így alakul:

`LD X, Y`

Ez triviálisan az Y regiszter értékét tölti be az X regiszterbe – ennek megvalósítása tulajdonképpen egy egyszerű kifejezés. Fontos hozzáenni, hogy az Y helyén állhat egy bájt is. Egyik *Load* művelet sem befolyásolja a *flagek* állapotát.

A továbbiakban ismertetésre kerülnek a fenti alapesettől eltérő betöltő utasítások.

Beltöltés memóriacímről, vagy memóriacímre

A *Load* műveletek másik típusa esetén az X vagy Y regiszter helyett állhat memóriacím is. A cím értéke átadható (HL) összevont regiszter formában: `LD A, (HL)`, vagy két külön betöltött bájt összevonásaként: `LD A, (0x2f44)`.

A *Stack Pointer* betöltője

A *Stack Pointer* betöltése a HL regiszterpárba az előzőhekhez képest bonyolultabb művelet. Egyetlen paraméteréből várja azt a *signed*, tehát előjeles(!) értéket, amely a betöltendő memóriahely címének távolságát mutatja az SP regiszterhez képest. A `fet ch` függvényel betöltött bájtot először *castolni* kell `i8` típusúra, majd az előjel vizsgálatát követően betölteni az adatot a HL-be a megfelelő helyről. A művelet az alábbiak szerint néz ki:

`LDHL SP, 0x42`

Egyéb speciális betöltők

Több speciális betöltő művelet is elérhető, ezeket a fentiekhez való hasonlóságuk miatt csak felsorolásszerűen fogom ismertetni:

- `LD A, (C)`: ezzel a művelettel a *High RAM* részre tudunk írni – a C regiszter értékéhez hozzáadódik még a 0xFF00 cím, ezzel megkapva a pontos címet. Fordított operandusokkal is működik.
- `LDH A, (0x42)`: az előzőhez hasonló művelet, annyi különbséggel, hogy itt a C regiszter helyett paraméterben megadható az 0xFF00-hez mért eltolás értéke. Fordított operandusokkal is működik.
- `LD A, (HL+)`: a HL értékének megfelelő memóriahely A regiszterbe töltése után inkrementálja a HL értékét eggyel. Fordított operandusokkal is működik.
- `LD A, (HL-)`: az előzővel megegyező módon működik, inkrementálás helyett dekrementálással.

3.3.2. Aritmetikai utasítások - ADD, ADC, SUB, SBC, INC, DEC

Az aritmetikai utasítások alatt ezen az architektúrán az összeadás, kivonás, inkrementálás és dekrementálás műveleteket értjük. Ezek lényegi működése persze triviális, viszont a műveletek hatása a *flag* regiszterre fontos tényező, így ezt célszerű részletesebben megvizsgálni. Külalakukban megegyeznek, példaként szerepeljen az összeadás szintaxisa:

`ADD A, B`

amely értelemszerűen az A regiszter értékét teszi egyenlővé az A és B regiszterek értékeinek összegével.

Összeadás

Két típusú összeadást megvalósító művelet áll a programozók rendelkezésére: az [ADD](#), és az [ADC](#). Ezen utasítások esetében közös probléma a túlcsordulás – hogyan kezeljük ha az összeg nagyobb, mint 255, azaz nem fér bele az [u8](#) adattípusba? Szerencsére a Rust nyelv biztosít erre egy olyan megoldást, amely a hardver viselkedésével megegyezik. A két [u8](#) típusú operandust nem a hagyományos módon ([u8 + u8](#)) adjuk össze, hanem a `wrapping_add` függvény segítségével a következő módon:

```
let a : u8 = 5;
let b : u8 = 6;
println!("{} ", a.wrapping_add(b)); // Output: 11
```

A fenti függvény abban az esetben, ha az összeg nagyobb lenne, mint 255, körbe *wrappeli* az eredményt, azaz elvégez egy $\text{mod } 256$ műveletet az összegen. Így a túlcsordulás problémáját sikerült kiküszöbölni, az összeadás bármely értékkal elvégezhető úgy, hogy biztosan nem lépünk ki az adattípus méretéből.

Ami a *flageket* illeti, az összeadások esetében mindegyikük érintett:

- Z: állítsuk be 1-re, ha az összeg értéke 0, egyébként legyen az új értéke 0,
- N: mivel nem kivonásról van szó, az értékét állítsuk 0-ra,
- H: ha *half-carry* történik, állítsuk 1-re, egyébként 0-ra,
- C: ha túlcsordulás történik, állítsuk 1-re, egyébként 0-ra.

A *half-carry* avagy fél-túlcsordulás detektálása a következő képpen történik:

```
if (a & 0xF) + (b & 0xF) > 0xF {
    cpu.set_flag("H");
} else {
    cpu.reset_flag("H");
}
```

Látható, hogy az elágazás logikai kifejezésének bal oldalán a két operandus értékének vesszük külön-külön az alsó 4 bitjét (`a & 0xF`, `b & 0xF`), majd ha azok összege nagyobb, mint 15 (binárisan 00001111), akkor fél-túlcsordulás következett be. Ekkor állítsuk a H *flaget* 1-re, egyébként pedig 0-ra.

A C-vel jelölt túlcsordulás ellenőrzése triviális.

A különbség az [ADD](#), és az [ADC](#) műveletek között az, hogy – mint az a *mnemonikból* is kikövetkeztethető – az [ADC](#) az egyszerű összeadás mellett az összeghez hozzáadja a C flag értékét is (*ADD with Carry*). A flag értékének hozzádását szintén a `wrapping_add` függvénnyel tesszük.

Kivonás

A [SUB](#), és az [SBC](#) kivonás műveletek nagyon hasonlóak a fentebb részletezett összeadás műveletekhez, természetesen kivonásos formában. `wrapping_sub` függvény helyett `wrapping_sub` függvényt használunk, amely negatív különbség esetén a másik irányba *wrappeli* át a végeredményt, szintén a $\text{mod } 256$ számítást alkalmazva.

A *flagek* az összeadás műveletekhez képest a következőképpen alakulnak:

- Z: megegyezik az összeadásnál ismertetettel,
- N: ebben az esetben kivonásról van szó, így az értéke legyen 1,
- H: megegyezik az összeadásnál ismertetettel,
- C: ha alulcsordulás történik, állítsuk 1-re, egyébként 0-ra.

A *half-carry flag* beállítása megegyezik ugyan az összeadásnál tapasztalattal, viszont a detektálása más módon történik:

```
if (a & 0x0F) < (b & 0x0F) {
    cpu.set_flag("H");
} else {
    cpu.reset_flag("H");
}
```

Az elágazás feltételes logikai kifejezésében láthatjuk, hogy a két operandus alsó 4 bitjeit hasonlítjuk össze egymással. Ha a kivonandó ilyen módon nagyobb mint a kisebbítendő, akkor fél-alulcsordulás történik – ekkor állítjuk 1-re a megfelelő bitet, egyébként pedig 0-ra.

Alulcsordulás akkor történik, ha a különbség kisebb, mint 0.

Az **SBC** művelet ebben az esetben is annyiban különbözik a hagyományos kivonástól, hogy a C *carry flaget* is kivonja a kisebbítendőből.

Inkrementálás, dekrementálás

Az inkrementálást (**INC**) és a dekrementálást (**DEC**) megvalósító műveletek gyakorlatilag rendre megegyeznek az összeadás, illetve kivonás műveletekkel, annyi különbséggel, hogy a második operandust minden esetben 1-nek tekintjük.

3.3.3. Logikai utasítások - **AND**, **XOR**, **OR**, **CP**

Az és (**AND**), kizáró vagy (**XOR**), vagy (**OR**), és összehasonlító (**CP**, *compare*) műveletek is legalább olyan alapvetőek, és fontosak mint az előzőekben tárgyalt aritmetikai műveletek. Közülük az első három nagyon egyszerű megvalósítani, hiszen a legtöbb programozási nyelv képes ezen műveletek elvégzésének reprezentálására az & (és), ^ (kizáró vagy), és a | (vagy) operátorok segítségével.

Az fent említett első három művelet implementálása tehát könnyű feladat, a *flagok* beállítása pedig szintén egyszerű. A **XOR** és **OR** flag kezelése megegyezik: ha a végeredmény 0, akkor a Z flag legyen 1 (egyébként 0), az összes többi flaget pedig állítsuk 0-ra. Az **AND** esetén is hasonló a helyzet, annyi különbséggel, hogy a H flaget minden esetben 1-ra kell állítani.

A **CP** művelet kicsit különbözik a többitől – maga a művelet összehasonlít két értéket, és ha az értékük megegyezik, a Z flaget 1-re állítja. Ennek működése tulajdonképpen megegyezik a kivonás műveletével, csak a különbséget nem tároljuk sehol, a *flagok* beállítása a fontos – ebben a tekintetben teljesen ekvivalens az összehasonlítás a kivonással.

3.3.4. Verem utasítások - **PUSH**, **POP**

Lehetőség van regiszterpárok eltárolására a veremben – ezt a funkciót a **PUSH** és a **POP** utasítások valósítják meg. A **PUSH** az AF, BC, DE, HL (konkrét műveletben szereplő) regiszterpárokat teszi bele a verembe (az SP által mutatott memóriacímre), a második regiszter taggal kezdve. A **POP** művelet pedig fordított sorrendben veszi ki az értékeket a veremből, majd állítja be velük a megfelelő regiszterek értékeit.

3.3.5. Eljárás utasítások - **JP**, **CALL**, **RET**

Ahhoz, hogy a programozók eljárásokat tudjanak írni a programok fejlesztése során, különféle utasításokra van szükségük. Ezek az utasítások a Game Boy architektúrájában az ugrás (**JP**), az eljáráshívás (**CALL**) és a visszatérés (**RET**).

A **JP** utasítás működése nagyon egyszerű: a CPU PC regiszterét állítja a paraméterben megadott memóriacímre, így a processzor ott fogja folytatni a futását. Több típusú **JP** művelet is szerepel a CPU utasításai között:

- **JP** **(HL)**: a HL regiszterpárban tárolt címre ugrik,
- **JP** **0x4a2a**: a paraméterben megadott 16 bites címre ugrik,
- **JP** **NZ 0x4a2a**: akkor ugrik a paraméterben megadott 16 bites címre, ha a **Z flag** értéke 0,
- **JP** **NC 0x4a2a**: akkor ugrik a paraméterben megadott 16 bites címre, ha a **C flag** értéke 0,
- **JP** **Z 0x4a2a**: akkor ugrik a paraméterben megadott 16 bites címre, ha a **Z flag** értéke 1,
- **JP** **C 0x4a2a**: akkor ugrik a paraméterben megadott 16 bites címre, ha a **C flag** értéke 1.

A **CALL** művelet annyiban hasonlít az előző **JP** művelethez, hogy szintén a paraméterben megadott címre fog ugrani a PC regiszter átállításával, előtte azonban az aktuális PC értékét beleteszi a verembe, elmentve azt. A **JP** művelethez hasonlóan szintén vannak feltételes eljárás hívás utasítások, melyek a **Z** és a **C flag** aktuális állapota szerint működnek.

A **RET** utasítás az előző (**CALL**) utasítással kéz a kézben jár: kiveszi a veremből a két legfelső értéket – amelyek együtt egy memóriacímet alkotnak –, majd a PC regisztert erre az értékre állítja be, így tulajdonképpen az eljárás hívás végeztével a CPU visszatér arra a címre, ahol az eljárás hívása előtt tartott. Szintén vannak a **Z** és **C flag** kötött **RET** utasítások, illetve létezik még egy **RETI** opkódú utasítás is, amely a visszatérés után engedélyezi az *Interrupt Enable* regiszterben az összes *interruptot*.

3.3.6. Bitmanipulációs utasítások - **BIT**, **RES**, **SET**, **SWAP**

Rendelkezésre állnak bitmanipulációs utasítások, amelyekkel regiszterek, vagy a memóriában lévő bájtok bitjeivel végezhetünk műveleteket: változtathatjuk (**RES**, **SET**, **SWAP**),

vagy lekérhetjük (**BIT**) őket. Ezek természetesen fontos műveletek, így a többi CPU utasításhoz hasonlóan törekedni kell a pontos emulációjukra.

A **RES** és **SET** esetében rendre 0 (*reset*) vagy 1 (*set*) értéket adhatunk az utasítás paramétereiben³ megadott bitnek. Az *első paraméter* a módosítandó bit indexe az adott bájtban, a *második paraméter* pedig maga a módosítandó bitet tartalmazó regiszter vagy (**HL**) regiszterpárral megadott memóriacím. Ezek az utasítások nincsenek hatással az F *flag* regiszterre. Az implementációt tekintve egy egyszerű bitmaszkolással, majd *vagy*, ill. *és* műveletekkel lehet elérni egy-egy bit módosítását egy **u8** változó esetén.

A **BIT** műveettel lehet lekérni egy konkrét bit értékét – az utasítás az eredményét a Z *flag* segítségével tudjuk kiolvasni: amennyiben az eredmény 0 volt, a Z 1-gel lesz egyenlő, egyébként pedig 0-val. Ami a további *flageket* illeti, az N *flaget* mindig *reseteli*, a H-t pedig minden esetben beállítja az utasítás. Implementációban bitmaszkolással tudjuk megkapni egy adott bit értékét.

A **SWAP** utasítás esetében egy paraméter adott: a módosítani kívánt regiszter. Maga a művelet nagyon egyszerű: fel kell cserálni a regiszterrel vagy memóriacímmel megadott bájt felső és alsó 4 bitjét egymással, így tehát például a 11110000_2 bájtból a **SWAP** elvégzése után 00001111_2 lesz. Ha a végeredmény nullával egyenlő, akkor az utasítás beállítja a Z *flaget* 1-re, egyébként pedig nullára. A maradék három *flag* minden esetben *resetelésre* kerül.

3.3.7. Rotate és Shift - **RLC**, **RRC**, **RL**, **RR**, **SIA**, **SRA**, **SRL**

Rotate műveletek

A Game Boy processzorának architektúrájában több bitforgató utasítás is van: **RLC**, **RRC**, **RLCA**, **RRCA**, **RL**, **RR**, **RLA**, és **RRA**. Ezek többé-kevésbé ugyan olyan módon működnek. Vegyük példának a legegyszerűbb, balra forgató utasítást, az **RLC**-t. Egy 11110000_2 bájt esetén a balra forgatás eredménye a következő lesz: 11100001_2 . Ez az érték úgy született, hogy minden bitet egygyel balra tolunk, a 7. bit pedig *körbefordul* – belőle lesz a 0. bit. A forgató műveleteket ez a körbefordulás különbözteti meg az eltoló műveletektől, ott ilyenről nincs szó. Ha az eredeti érték 7. bitje 1-es értékű volt, akkor be kell állítani a C *flaget* is 1-re (egyébként 0-ra). Ami a többi *flaget* illeti, a Z-t akkor állítjuk 1-re ha a végeredmény 0 lett (egyébként 0-ra), a többi *flaget* pedig *reseteljük*. Az **RL** utasítás pontosan ugyanígy működik azzal a kivételel, hogy nem az eredeti bájt 7. bitjéből lesz az új bájt 0. bitje, hanem a C *flagból*.

Az **RRC** és az **RR** is a fentiek szerint alakul, csak nem balra forgat az utasítás, hanem jobbra – az eredeti bájt 0. bitjéből lesz az új bájt 7. bitje. Ebből adódóan az eredeti bájt 0. bitje szerint módosítjuk a C *flaget*.

Az **RLCA**, **RRCA**, **RLA**, és **RRA** utasítások esetén a különbség az előzőekhez képest csupán annyi, hogy mindegyikük esetében 0-ra állítjuk a Z *flaget*, valamint az összes utasítás az A regiszterrel dolgozik.

³ Paraméter alatt jelen esetben nem külön beolvasott bájtokat tekintünk, hanem a konkrét művelethez (a processzor architektúrájának részeként) specifikált paramétereket.

Shift műveletek

Mint ahogyan a fenti bekezdésben említésre került, a *shift* – azaz eltoló – utasítások esetén nincsen körbeforduló bit: az **SLA** (*Shift Left*) és **SRL** (*Shift Right*) esetén rendre balra, illetve jobbra tolódnak el a bitek, az újonnan bejövők pedig mindenkorban a 0 értéket veszik fel. A *flagek* beállításai is megegyeznek a forgató műveletekkel.

Az **SRA** utasítás kivételt képez, ugyanis ebben az esetben az eredeti bájt 7. bitje helyére nem 0, hanem az eredeti 7. bittel megegyező értékű bit érkezik.

3.3.8. Egyéb, speciális utasítások

Azok az utasítások kerültek ebbe a csoportba, amelyek egytől egyik speciálisak, nem lehet őket nagyobb kategóriához sorolni.

Üres műveletek - NOP, STOP, HALT

A **NOP**, **STOP** és **HALT** műveletek hasonlítanak egymásra abban a tekintetben, hogy mindegyikük végrehajtása alatt a CPU tulajdonképpen nem csinál semmit. A **NOP** esetében egy előre eltervezett üres műveletről van szó, amelyet várakozások esetén használnak, a **STOP** utasítás addig leállítja a processzort és a kijelzőt amíg gombnyomás nem történik, a **HALT** pedig addig kikapsolva tartja a CPU-t amíg egy megszakítási kérés nem érkezik. Az utolsó két utasítás tipikusan olyan amit egy emulátor kapcsán nem szükséges implementálni, a hardver energiafogyasztásának optimalizálásában van szerepe.

Carry flag műveletek - SCF, CCF

Két, konkrétan a *flageket* állító utasítás az **SCF** és a **CCF**. Az **SCF**-fel be tudjuk állítani a *Carry flaget*, a **CCF**-fel pedig komplementálni tudjuk az értékét. Az N és H *flageket* mindenkorban *reseteli*.

Komplementer, binárisan kódolt decimális műveletek - CPL, DAA

Az A regisztert módosító utasítások közé sorolható a **CPL** és a **DAA** művelet.

A **CPL** utasítás – a nevéből is adódóan – az A regiszter fogja komplementálni (minden bitjét az ellentétre állítja), és az N és H *flageket* beállítani. A Rust nyelvben a komplementálás egy egyszerű felkiáltójel operátorral érhető el, így az A regiszter komplementere az ! A lesz.

A **DAA** művelet az A regiszter értékét binárisan kódolt decimális formájúra hozza, amely azt jelenti, hogy sorra veszi a decimálisan ábrázolt A regiszter számjegyeit, majd azokat binárisan ábrázolja helyiértékük szerint csökkenő sorrendben. Ha a végeredmény 0 lesz, beállítja a Z *flaget* (egyébként *reseteli*), a H-t minden esetben *reseteli*, a C-t pedig a művelettől függően állítja be vagy *reseteli*.

Restart műveletek - RST

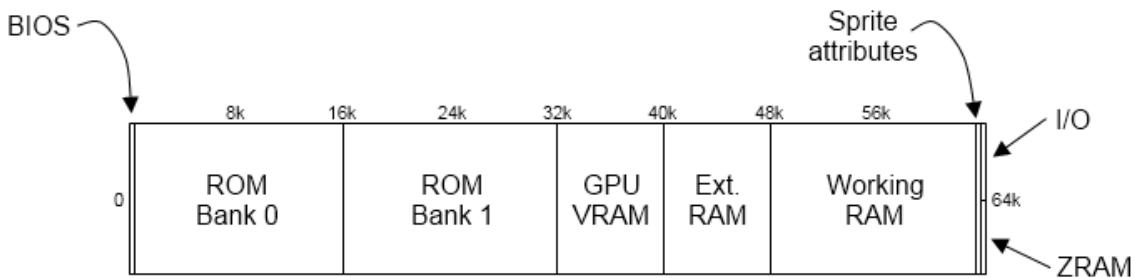
A **RST** műveletekkel a programozók szoftveres megszakításokat tudtak előidézni, melyek – **RST** utasítástól függően – az alábbi memóriacímekre állítják a PC regisztert az aktuális cím verembe helyezése után:

0x00, 0x08, 0x10, 0x18, 0x20, 0x28, 0x30, 0x38.

Interrupt műveletek - EI, DI

A megszakítások letiltására és engedélyezésére a **DI** és **EI** utasítások valók, melyekkel szabályozni lehet a korábban már említett *Interrupt Master Enable Flaget*. Ez a flag egy, a CPU struktúrájában létező **bool** típusú változó értékét módosítja.

3.4. Memória



3.2. ábra. A memória térkép

A Game Boy memóriájának térképe a fenti, 3.2-es ábrán figyelhető meg. Jól látható, hogy több nagyobb részre van osztva, melyek működésükben igencsak elkülönülnek egymástól. Az emulátor implementációját nagyban megkönnyíti, hogy annak ellenére, hogy több modul is használja valamilyen módon a beépített memóriát, annak csak egy címtartománya van, amelyet a következő intervallumbeli bájtok alkotnak: 0x0000 - 0xFFFF. Az alaplapra forrasztott memória tehát 64 kB, amelynek rögtön az első felét a játék ROM-ja teszi ki.

A konzol elindítását követően a hardver első feladata a Boot ROM futtatása. Ez a szoftver a *bootolási* folyamat alatt a 0x0000 - 0x0100 területet foglalja el, amely a folyamat végeztevel kikerül a memóriából (*átmappelődik*), helyére pedig a betöltött játék első 256 bájtja kerül. Ez azt is jelenti, hogy az *átmappelés* után a Boot ROM bájtai többé nem elérhetők.

A játék ROM-jának 32 kB-ja után, a 8 kB méretű 0x8000 - 0x9FFF tartományon helyezkedik el a *Video Memória* (vagy *Grafikus Memória*, VRAM). Itt vannak eltárolva *tile*-ok (csempék), a játékokat felépítő grafikus építőelemek, illetve azok az adatok, melyek leírják, hogy melyik *tile* hol helyezkedik el a képernyőn. A csempék helyét leíró adatok segítségével tudja a Game Boy PPU-ja felépíteni a játék háttereként szolgáló grafikai elemeket. Ezekről bővebben a későbbi, PPU-t részletező fejezetben lesz szó.

A sorban következő 8 kB méretű blokk az 0x8000 - 0x9FFF intervallumon található, a neve pedig *External RAM* vagy *xRAM*. Ez a rész fizikailag a játék kazettáján helyezkedett el, többnyire a játék mentéseket tárolták itt.

A hagyományos értelemben vett RAM a 0xC000 - 0xDFFF területet foglalta el – a programozók ezen a részen tároltak el tetszőleges adatokat. *Work RAM*-nek is hívták emiatt. Ez a terület szorosan összefügg az 0xE000 - 0xFFFF memória résszel: a második, ún. *Shadow RAM* (Árnyék RAM) terület a *Work RAM* bitre pontos másolata. Érdekesség, hogy a Nintendo a hivatalos programozóknak szánt dokumentációjában megtiltja, hogy

a *Shadow RAM* területére írás történjen, ha ezt mégis megtesszük, akkor a *Work RAM* azonos bájtja is átiródik ugyanarra a bájtra, amit a *Shadow RAM*-ba írtunk. Szintén érdekes, hogy ha megnézzük, a két RAM területe nem egyezik meg, a *Shadow RAM* 128 bájttal "rövidebb", mint a *Work RAM*. Ennek az az oka, hogy a RAM legfelső 128 bájta a leggyorsabban írható és olvasható *High RAM* számára van fenntartva.

Az utolsó egység tehát a memóriában a *High RAM*, amely az 0xFE00 - 0xFFFF területet foglalja el. Itt található nagyon sok fontos adat, regiszter és *flag*. Az 0xFE00 - 0xFE9F területen az OAM, vagy *Sprite Attribute Table* található. A Game Boy képernyőjén megjelenő mozgó objektumok az itt eltárolt *sprite*-okból épülnek fel.

A kijelző, hanggenerátor, soros port, *joypad*, és az időzítők fontos attribútumait és működési elemeit tartalmazza az 0xFF00 - 0xFF7F szakasz. A diplomamunka további részében a megfelelő helyeken ezekről bővebben lesz szó.

Az 0xFF80 - 0xFFFF részt a *High RAM* programozók által saját célra használható (gyors elérésű) része foglalja el.

A 0xFFFF címen lévő bájt a korábban már említett *Interrupt Enable* regiszter.

3.4.1. DMA

A DMA vagy *Direct Memory Access* (Közvetlen Memóriaelérés) a Game Boy architektúrájának egy olyan eljárása, amely segítségével adatot lehet másolni a fentebb említett *Sprite Attribute Table*-be. Egy játék akkor tudja alkalmazni a DMA eljárást, ha az 0xFF46-es memóriacímre ír. Ahhoz, hogy ezt a működést emulálni tudjuk, készíteni kell egy csapdát a memória írást megvalósító függvénybe:

```
pub fn write_ram(&mut self, address : u16, value : u8) {
    // ...
    // if writing address is 0xFF46 -> DMA
    if address == 0xFF46 {
        self.dma(value);
    }
    // ...
}
```

A 0xFF46-os címre kérelmezett írás esetén tehát maga az írás történik meg, hanem a vezérlés a fenti csapdába kerül. A DMA-t aktiváló memóriacímre írandó adat adódik át a DMA függvénynek.

A *Sprite Attribute Table* a 0xFE00 - 0xFE9F memóriacímek között helyezkedik el, tehát 160 bájtot tárol. Ezt a 160 bájtot kell feltölteni az új adattal úgy, hogy a DMA függvény paraméterében átadott érték alapján kiszámoljuk a kezdőcímét, ahonnan a 160 darab bájt másolása fog megtörténni. Ennek a kezdőcímnek a kiszámolása könnyű feladat: el kell osztani 100-zal, vagy – ha gyorsabb véghajtást szeretnénk –, *shifteljük* el balra 8-cal. A DMA függvény tehát a következők szerint alakul:

```
pub fn dma(&mut self, value : u8) {
    // copyable data start address
    let addr : u16 = (value as u16) << 8;

    // start copying
    for i in 0..0xA0 {
        let n : u8 = self.RAM[(addr + i) as usize];
        self.write_ram(0xFE00 + i, n);
    }
}
```

Ezzel a szükséges bájtok másolása megtörtént.

3.4.2. Memory Bank Controller

3.5. Időzítők

A Game Boy hardver architektúrájának elengedhetetlen részét képezik az időzítők. Ahhoz hogy a rendszer egyes elemei között meglegyen a tökéletes együttműködés, szinkronizált végrehajtásra van szükség. Erre jelentenek megoldást a *timerek* (időzítők), amelyek segítségével meg lehet teremteni a modulok közti kohéziót.

Két típusú *timer* áll rendelkezésre az architektúrában: a TIMA (*Timer Counter*), illetve a DIV (*Divider Register*). Ezek alapjaikban ugyan megegyeznek, és így egymással összehasonlíthatók, viszont különböző feladatok ellátására szolgálnak, ebből kifolyólag pedig a működésük végső soron mégis eltérő – ezt a továbbiakban láttni fogjuk. Ami az implementálást illeti, minden időzítő esetén a processzor minden műveletet követően leellenőrzi hogy szükséges-e léptetni az időzítőt. A részletesebb bemutatást a TIMA-val kezdjük, majd pedig a DIV fog következni.

3.5.1. TIMA

A *Timer Counterhez*, vagy TIMA-hoz három memóriacím, azaz három folyton változó adat kapcsolható. Ezeket a következő táblázatban gyűjtöttem össze:

TIMA	0xFF05
TMA	0xFF06
TMC	0xFF07

3.4. táblázat. A TIMA időzítőhöz köthető adatok memóriacímei

Ahogy a 3.4-es táblázatból kiolvasható, a három érték maga a TIMA, a TMA és a TMC. Az időzítő leegyszerűsített működése könnyen megérthető és implementálható. Ha elég idő telt el ahhoz hogy léptessük az időzítőt, akkor megtesszük ezt a léptetést. A léptetés során azonban figyelni kell arra, hogy túlcordulás történik-e: ha az időzítő új értéke nagyobb mint 255 (egy byte) akkor 2-es számú megszakítási kérést kell küldeni a processzornak, és be kell olvasni az időzítő új, bázis értékét – ez az az érték, ahonnan folytatódni fog a számlálás. Ha nincs túlcordulás, akkor a léptetésen kívül nincs további

teendő.

Persze felmerülhet több kérdés is. *Honnan olvassuk ki az új bázis értékét? Honnan tudjuk hogy milyen gyakorisággal kell léptetni?* A fenti 3.4-es táblázatban szereplő adatok fogják megadni ezekre a kérdésekre a válaszokat.

A TMA, vagy *Timer Modulo* az az érték, amelyet a fentebb taglalt időzítő eljárás során is használtunk: ebből olvassuk ki az időzítő túlcordulás utáni új bázis értékét, melyet abba a TIMA regiszterbe töltünk, amely az időzítő aktuális állapotát tartalmazza, és amelyet folyton inkrementálunk. Azzal, hogy nem egyszerűen minden 0-ról kezdjük újra a számozást, modulálni lehet a Game Boy időzítőjét.

A másik kérdésre a TMC, azaz a *Timer Control* fogja megadni a választ. Ez a byte tartalmazza az időzítő frekvenciáját, illetve segítségével ki-be lehet kapcsolni a *timer* működését. Ez utóbbi funkció 1 bittel (a 3.5-ös ábrán T), míg az aktuális frekvencia sebessége 2 bittel van ábrázolva (a 3.5-ös ábrán F) – így a TMC egy három bites regiszter. A bitek kiosztása a következők szerint alakul:

0	0	0	0	0	T	F	F
---	---	---	---	---	---	---	---

3.5. táblázat. A TMC regiszter bitjeinek kiosztása

A fenti táblázat szerinti 0. és 1. bitek tárolják el tehát az időzítő frekvenciáját. Az egyes frekvenciák a következő táblázatban ábrázolt értékekkel vannak jelölve.

FF	Frequency
00	4096 Hz
01	262144 Hz
10	65536 Hz
11	16384 Hz

3.6. táblázat. A választható frekvencia opciók és az ábrázolási értékek

Tudjuk, hogy a CPU frekvenciája 4194304 Hz, így könnyen kiszámolható az, hogy hány processzor művelet után kell léptetni az időzítőt az egyes időzítő frekvenciák esetében – egyszerűen el kell osztani őket egymással. Ez az implementációt nagyban megkönnyíti, hiszen a fő ciklus minden iterációja egy órajelciklussal ekvivalens. Az órajelciklusokra átszámolt frakvenciák tehát a fenti táblázat szerint rendre: 1024, 16, 64 és 256. Látható, hogy ezek igen kerek értékek.

A TIMA időzítő implementálása tehát minden összevetve így alakul:

```
// Is the clock enabled?
if CPU::get_bit(2, cpu.RAM[self.TMC as usize]) {
    // Is enough time passed to update the timer?
    if cycle as u32 > self.timer_counter {
        // Update the current frequency.
        self.update_freq(cpu);
        // Check for the overflow.
        if cpu.RAM[self.TIMA as usize] >= 255 {
            // If an overflow occurs, load TMA to TIMA,
        }
    }
}
```

```
    let TMA = cpu.RAM[self.TMA as usize];
    cpu.write_ram(self.TIMA, TMA);
    // and send an interrupt request.
    self.interrupt.IRQ(cpu, 2);
} else {
    // If no overflow, increment the TIMA.
    let TIMA = cpu.RAM[self.TIMA as usize];
    cpu.write_ram(self.TIMA, TIMA + 1);
}
} else {
    // Sync the time with the CPU.
    self.timer_counter -= cycle as u32;
}
}
```

A fenti kódrészletet tartalmazó, Timer struktúra beli Update függvényt kell meghívni a fő ciklus minden iterációjában.

3.5.2. DIV

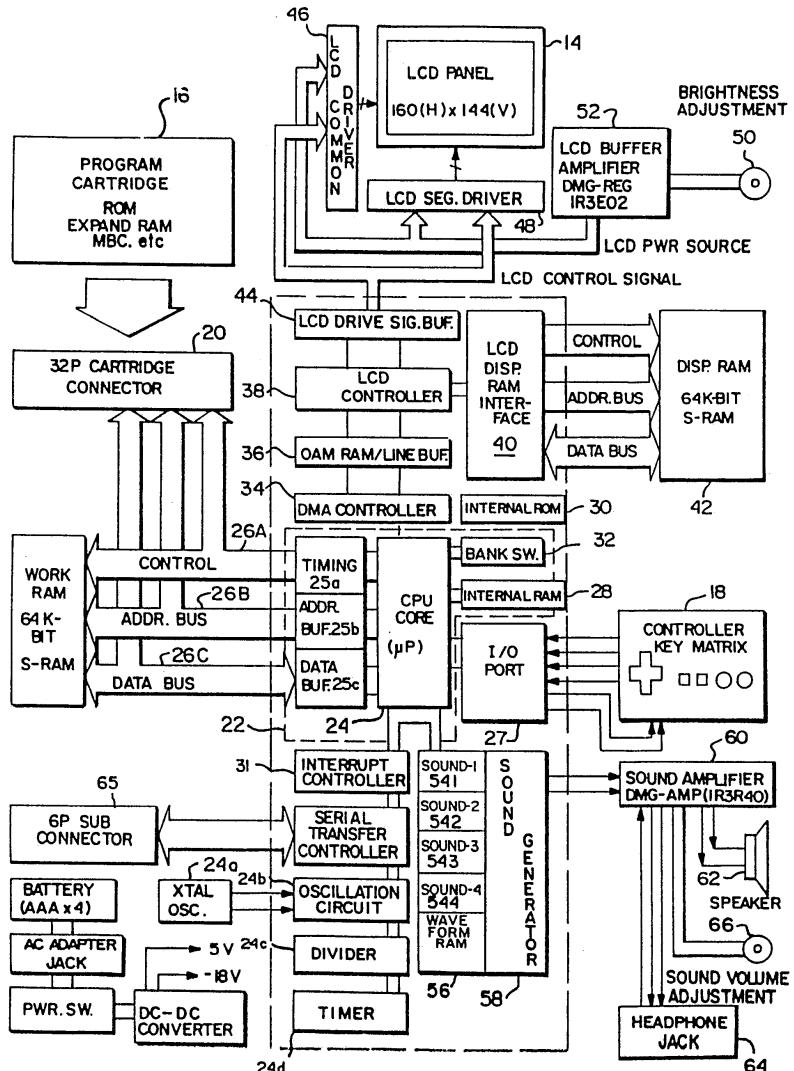
A DIV időzítő, ahogy már említésre került, úgy működésben, mint viselkedésben eltér a TIMA-tól. A DIV minden tekintetben sokkal egyszerűbb, mint a társa: nem lehet változtatni a frekvenciáját, és modulálni sem lehet.

A frekvencia fixen 16384 Hz, ami azt jelenti, hogy minden 256 CPU ciklus után kell inkrementálni az időzítő értékét. A moduláció hiánya pedig abból fakad, hogy túlcordulás esetén nem egy másik memóriahelyről töltünk értéket a DIV-be, hanem alapértelmezés szerint 0-ról kezdjük ismételten a számlálást. A TIMA-tól eltérően ennek az időzítőnek nincsen egyéb adata, egyedül a *counter* értéke adott.

4. fejezet

Függelék

4.1. A Nintendo Game Boy hivatalos architektúrája



4.1. ábra. A szabadalomban szereplő Game Boy architektúra

4.2. A processzor opkód táblái

X0	X1	X2	X3	X4	X5	X6	X7	X8	X9	XA	XB	XC	XD	XE	XF
NOP	1	LD BC,d16	LD (BC),A	INC BC	INC B	DEC B	LD B,08	RCL A	LD (16),SP	AUD HL,BC	DEC BC	INC C	DEC C	LD C,d8	RCCA
0x	4	3,12	1,8	1,8	1,4	1,4	2,8	1,4	3,20	1,8	1,8	1,4	2,8	1,4	0,0,0,C
STOP	0	LD DE,d16	LD (DE),A	INC DE	INC D	DEC D	LD D,08	RLA	JR r8	ADD HL,DE	LD A,(DE)	DEC DE	INC E	DEC E	LD E,d8
1x	2,4	3,12	1,8	1,8	1,8	1,4	2,8	1,4	2,12	1,8	1,8	1,4	2,8	1,4	0,0,0,C
JR NZ,r8		LD HL,d16	LD (HL),A	INC HL	INC H	DEC H	LD H,08	DAA	JR Z,r8	ADD HL,HL	LD A,(HL)	DEC HL	INC L	DEC L	CPL
2x	2,12/8	3,12	1,8	1,8	1,4	1,4	2,8	1,4	2,12/8	1,8	1,8	1,4	2,8	1,4	-1,1,-
JR NC,r8		LD SP,d16	LD (HL),A	INC SP	INC (HL)	DEC (HL)	LD (HL),08	SCF	JR C,r8	ADD HL,SP	LD A,(HL)	DEC SP	INC A	DEC A	COP
3x	2,12/8	3,12	1,8	1,8	1,12	1,12	2,12	1,8	2,12/8	1,8	1,8	1,4	2,8	1,4	-0,0,C
LD B,B		LD B,D	LD B,E	LD B,L	LD B,A	LD C,B	LD C,D	LD C,E	LD C,H	LD C,L	LD C,(HL)	LD C,L	LD C,A	LD C,A	RRA
4x	1,4	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4
LD D,B		LD D,C	LD D,D	LD D,H	LD D,L	LD D,A	LD E,B	LD E,C	LD E,D	LD E,H	LD E,L	LD E,L	LD E,A	LD E,A	RRA
5x	1,4	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4
LD H,B		LD H,C	LD H,E	LD H,H	LD H,L	LD H,(HL)	LD L,B	LD L,C	LD L,E	LD L,H	LD L,L	LD L,L	LD L,A	LD L,A	RRA
6x	1,4	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4
LD (HL)B		LD (HL)C	LD (HL)D	LD (HL)E	LD (HL)H	LD (HL)L	HALT	LD (HL)A	LD A,B	LD A,C	LD A,D	LD A,E	LD A,H	LD A,L	LD A,A
7x	1,8	1,8	1,8	1,8	1,8	1,8	1,8	1,4	1,8	1,4	1,4	1,4	1,8	1,4	1,4
ADD A,B		ADD A,C	ADD A,D	ADD A,E	ADD A,H	ADD A,(HL)	ADD A,L	ADD A,B	ADC A,B	ADC A,C	ADC A,D	ADC A,E	ADC A,H	ADC A,L	ADC A,(HL)
8x	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4
SUB B,Z		SUB C,Z	SUB D,Z	SUB E,Z	SUB H,Z	SUB L,Z	SUB (HL)Z	SUB A,Z	SBC A,B	SBC A,C	SBC A,D	SBC A,E	SBC A,H	SBC A,L	SBC A,(HL)
9x	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	1,4	SIC A,A
AND B,A		AND C,A	AND D,A	AND E,A	AND H,A	AND L,A	AND (HL)A	AND A,A	XOR B,C	XOR C,D	XOR D,E	XOR E,F	XOR F,G	XOR G,H	XOR A,A
Ax	1,4	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4
Z0,1,0		Z0,1,0	Z0,1,0	Z0,1,0	Z0,1,0	Z0,1,0	Z0,1,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0
OR B,A		OR C,D	OR D,E	OR E,F	OR H,G	OR L,P	OR (HL)P	OR A,C	CPB	CPD	CP E	CP G	CP L	CP P	CP A
Bx	1,4	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4	1,4	1,4	1,4	1,8	1,4	1,4
Z0,0,0		Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0	Z0,0,0
RET NZ		POP BC	JP NZ,a16	PUSH BC	ADD A,d8	RST 00H	RET Z	JP Z,a16	PREFIX CB	CALL Z,a16	CALL a16	ADC A,d8	REST 0B	REST 0B	RRA
Cx	1,20/8	1,12	3,16/12	3,16	3,24/12	1,16	1,16	1,20/8	1,4	3,24/12	3,24	2,8	1,16	1,16	RRA
RET NC		POP DE	JP NC,a16	PUSH DE	SUB 08	RST 0H	RET C	JP C,a16	CALL C,a16	CALL C,a16	CALL C,a16	SIC A,d8	REST 1B	REST 1B	RRA
Dx	1,20/8	1,12	3,16/12	3,16	3,24/12	1,16	1,16	1,20/8	1,16	3,24/12	3,24	2,8	1,16	1,16	RRA
LDH (A),B		POP HL	LD (C),A	PUSH HL	ADD 08	RST 0H	ADD SF,r8	JP (HL)A	LD (A16),A	LD (A16),A	LD (A16),A	LD (A16),A	REST 2B	REST 2B	RRA
Ex	2,12	1,12	2,8	2,8	2,8	1,16	2,16	1,16	2,16	0,0,H,C	0,0,H,C	2,8	1,16	1,16	RRA
LDH A,(A,B)		POP AF	LD A,(C)	PUSH AF	OR 08	RST 30H	LD HL,SP+1B	LD SP,HL	LD A,(A16)	LD A,(A16)	LD A,(A16)	LD A,(A16)	GP,DG	REST 3B	RRA
Fx	2,12	1,12	2,8	1,4	1,16	2,8	2,8	2,8	2,12	1,8	1,8	1,4	2,8	1,16	RRA

4.2. ábra. Az első 256 opkódot tartalmazó tábla

Nintendo Game Boy Zilog Z80 emulátor implementálása

4.3. ábra. A második, CB prefixű 256 opkódot tartalmazó tábla

Nyilatkozat

Alulírott szakos hallgató, kijelentem, hogy a dolgozatomat a Szegedi Tudományegyetem, Informatikai Intézet Tanszékén készítettem, diploma megszerzése érdekében.

Kijelentem, hogy a dolgozatot más szakon korábban nem védtem meg, saját munkám eredménye, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel.

Tudomásul veszem, hogy diplomamunkámat a Szegedi Tudományegyetem Informatikai Intézet könyvtárában, a helyben olvasható könyvek között helyezik el.

Szeged, 2018. április 7.

.....

aláírás

Köszönetnyilvánítás

Irodalomjegyzék

- [1] Andrew S. Tanenbaum, *Számítógép-architektúrák*, Panem Könyvkiadó Kft., Budapest, 2006.
- [2] Wikipedia, *Game Boy*, https://hu.wikipedia.org/wiki/Game_Boy.