

学 号： 2014218760

密 级： 绝密 * 启用前

合肥工业大学

Hefei University of Technology

本科毕业设计（论文）

UNDERGRADUATE THESIS



类 型： 设计

题 目： 基于 6502 cpu 的 NES 模拟器设计与实现

专业名称： 计算机科学与技术

入校年份： 2014 级

学生姓名： 罗能

指导教师： 安鑫-副教授

系名称： 信息工程系

完成时间： 2018 年 5 月

合 肥 工 业 大 学

本科毕业设计（论文）

基于 6502 cpu 的 NES 模拟器设计与实现

学生姓名：_____罗能_____

学生学号：_____2014218760_____

指导教师：_____安鑫-副教授_____

专业名称：_____计算机科学与技术_____

系名称：_____信息工程系_____

2018 年 5 月

A Dissertation Submitted for the Degree of Bachelor

**Design and Implementation of a NES Emulator Based
on 6502 cpu**

By

Neng Luo

Hefei University of Technology

Hefei, Anhui, P.R.China

5 Month, 2018 Year

毕业设计（论文）独创性声明

本人郑重声明：所呈交的毕业设计（论文）是本人在指导教师指导下进行独立研究工作所取得的成果。据我所知，除了文中特别加以标注和致谢的内容外，设计（论文）中不包含其他人已经发表或撰写过的研究成果，也不包含为获得合肥工业大学或其他教育机构的学位或证书而使用过的材料。对本文成果做出贡献的个人和集体，本人已在设计（论文）中作了明确的说明，并表示谢意。

毕业设计（论文）中表达的观点纯属作者本人观点，与合肥工业大学无关。

毕业设计（论文）作者签名： 签名日期： 年 月 日

毕业设计（论文）版权使用授权书

本学位论文作者完全了解 合肥工业大学 有关保留、使用毕业设计(论文)的规定,即:除保密期内的涉密设计(论文)外,学校有权保留并向国家有关部门或机构送交设计(论文)的复印件和电子光盘,允许设计(论文)被查阅或借阅。本人授权 合肥工业大学 可以将本毕业设计(论文)的全部或部分内容编入有关数据库,允许采用影印、缩印或扫描等复制手段保存、汇编毕业设计(论文)。

(保密的毕业设计(论文)在解密后适用本授权书)

学位论文作者签名：

簽名日期： 年 月 日

指导教师签名:

簽名日期： 年 月 日

摘 要

NES¹(任天堂娱乐系统) 在 20 世纪 80 年代是世界上使用最广泛的电子游戏系统，将许多游戏带入了家庭，并为当今电子游戏产业铺平了道路。

随着科技的发展，许多 NES 游戏已经无法在当今系统上游玩，然而归功于模拟器的存在，使得这些经典能够延续下去。

本课题设计并用 C++ 实现一个跨平台²的 NES 模拟器，以达到在现代操作系统中能够模拟并运行上个年代的 NES 游戏。

关键词：模拟器；6502；计算机组成原理；NES

¹全称为 Nintendo Entertainment System

²在 Win/Linux/Mac 三大平台运行

ABSTRACT

The NES (Nintendo Entertainment System) was the world's most widely used video game console system in the 1980s, bringing many games to the home and paving the way for today's video game industry.

With the development of science and technology, many NES games can no longer play on modern operating systems, but thanks to the presence of emulators, these classics can continue.

This project designs and implements a cross-platform NES emulator in C++ to achieve the ability to emulate and run NES games of the last decade in modern operating systems.

KEYWORDS: Emulator; 6502; Computer Organization; NES

目 录

1	引言	1
1.1	课题背景及意义.....	1
1.2	课题研究现状	1
1.3	预期成果	2
2	任天堂娱乐系统	3
2.1	CPU	3
2.1.1	系统总线	3
2.1.2	内存	4
2.1.3	寄存器	5
2.1.4	中断	6
2.1.5	寻址模式	7
2.1.6	指令集	8
2.2	PPU	9
2.2.1	显存	9
2.2.2	寄存器	11
2.2.3	渲染	12
	参考文献	13
	致谢	14
	附录	15

插图清单

图 1.1	本模拟器模拟的一些经典游戏	2
图 2.1	基于 6502 改造的 2A03 处理器	3
图 2.2	NES 的系统总线	4
图 2.3	程序状态寄存器 P	6
图 2.4	超级马里奥的图块表	10

表格清单

表 2.1 NES 的内存区域	5
表 2.2 6502 CPU 各寄存器作用	5
表 2.3 NES 的中断	6
表 2.4 PPU 显存布局	10
表 2.5 PPU 的各个寄存器主要作用	11

1 引言

1.1 课题背景及意义

NES 是一个 8 位家用电子游戏终端系统,由任天堂公司开发与制作。最初于 1983 年 7 月 15 日发行于日本名叫 Famicom³的电子游戏机,后来于 1985 年发行于纽约,1986 到 1987 年遍布整个美国和欧洲,1987 年在澳大利亚发行。

当时在游戏机市场最畅销的时候,NES 在 1983 年的电子游戏行业崩溃⁴之后振兴了美国电子游戏行业。任天堂公司提出了严格的第三方开发者授权的商业模式来确保游戏质量,所有游戏必须通过任天堂的批准,并且第三方厂商每年只能开发一定数量的游戏,后来的 SNES⁵也采用了这种模式。正是因为这款游戏机的先进技术和严格的授权开发商业模式,使其成为电视游戏机的开山鼻祖。

在 2009 年时,NES 被 IGN⁶评为游戏历史上最伟大的电子游戏机⁷。

为了能够对大学所学知识加以应用,这个课题能够深入理解计算机是如何运行程序的,同时又能将经典游戏继续延续下去;为了能够跨平台流畅运行,还需要写出高兼容性、高性能代码;为了保证开发的效率,需要学习 6502 汇编,编写单元测试。

1.2 课题研究现状

由于任天堂未公布相关硬件细节,许多 NES 模拟器开发者通过对硬件逆向工程获得了许多信息,将这些信息整合起来就能够了解内部工作原理,足以实现一个模拟器了。

目前有以下三种方法来实现模拟器:

直接翻译 读取源程序 PC 指针上的指令,并翻译成目标机器指令,更新 PC 指针、内存。由于在执行过程中进行翻译,可能会导致性能问题。

³也叫红白机,美国称 NES

⁴由于市场饱和,同时又充斥着大量粗制滥造的游戏

⁵Super Nintendo Entertainment System,由任天堂于 1990 年发行的 16 位电子游戏机

⁶最大最权威的电子游戏评测网站

⁷<http://www.ign.com/lists/top-25-consoles/1>

静态编译 将源程序一次性编译到能够在目标系统上运行的程序，然而静态编译无法判断运行时遇到的分支跳转语句。

动态编译 结合以上两种方式，算是一种折中方案。

最终本课题采取直接翻译的方法来实现模拟器，考虑性能问题，利用 C++ 来实现，以达到最大性能。为保证模拟器能够正确工作、重构，利用 Google Unit Test 框架进行单元测试。

1.3 预期成果

由于写一个兼容目前所有游戏将超出本课题范围，这里最终成果是能够运行超级马里奥、吃豆人等经典游戏，如图1.1所示，从技术角度上来讲也极具挑战性，因为它们或多或少依赖一些硬件上的特性，实现起来需要特别处理。



图 1.1 本模拟器模拟的一些经典游戏

比较遗憾的是，本课题还未实现 Mapper⁸，声音模块，实现它们也将是一件有意思的事情。

⁸能够对换卡带中的程序 ROM 到 CPU 内存中，用来运行大容量游戏

2 任天堂娱乐系统

本章主要介绍一下 NES 的各个硬件模块相关细节。

2.1 CPU

NES 采用由 Ricoh 公司改造的 8 位 6502 的 MOS 处理器，代号 2A03/2A07⁹。该改造后的 CPU 不同于通用的 6502 的是，它能够处理声音，后果是无法处理 BCD 码¹⁰，除此之外其余部分例如指令集都是一样的。

6502 CPU 是一个小端 CPU，即高地址存放高字节，低地址存放低字节。举个例子，16 进制数 0x1234 的 0x34 字节的内存地址是 x ，那么 0x12 的地址是 $(x+1)$ 。CPU 主频为 1.79 MHz，基频为 21.48 MHz，即主频对基频 12 分频。

NES 使用内存 I/O 映射技术，使得处理器写入指定内存位置，即可对外设进行通讯（PPU、控制器设备等等）。

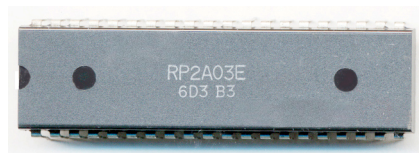


图 2.1 基于 6502 改造的 2A03 处理器

2.1.1 系统总线

如图2.2所示，NES 采用三总线结构：

数据总线 8 位双向数据总线，在 CPU 与 RAM、I/O 设备之间双向传输（读、写），在程序卡带 ROM 之间单向传输（只读）。

控制总线 8 位控制线，用于控制目标状态是读还是写。

地址总线 16 位地址总线，用于指定目标的位置。

同时，内存被划分为三个部分：

⁹2A03 用于 NTSC 版本，而 2A07 用于 PAL 版本，本课题采用 NTSC 制式

¹⁰用 4 个比特位来表示数字 0-9

- 卡带中的 ROM 区，只读存储器，由 MMC 组件来访问，扮演 Mapper 内存块兑换的角色
- CPU 的 RAM 区
- I/O 寄存器映射区，用于 CPU 与外部组件 PPU¹¹、控制器进行通信

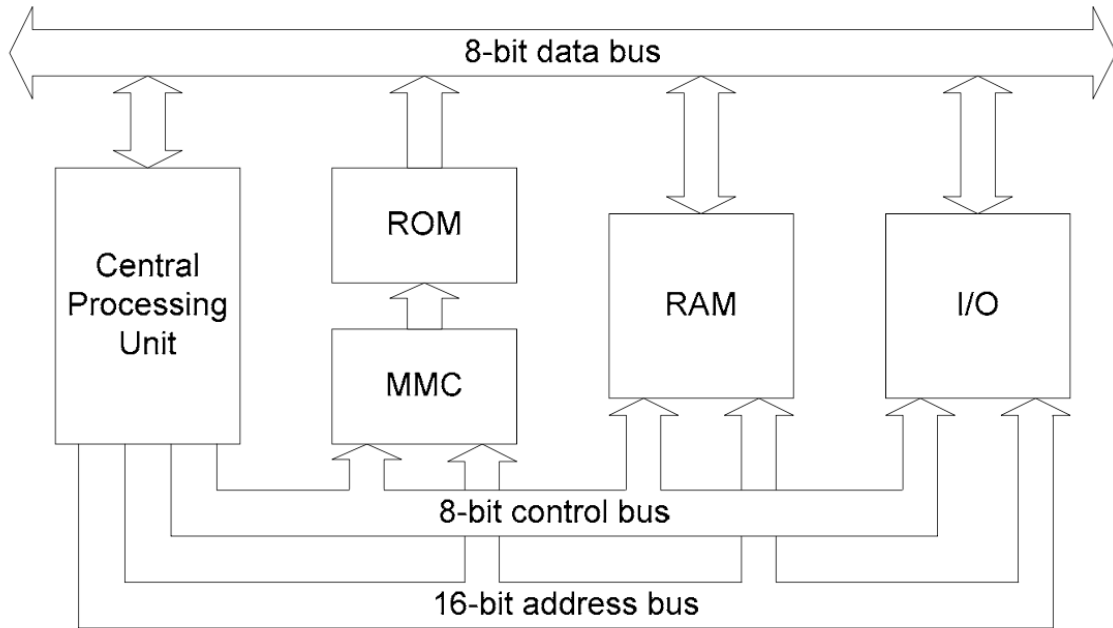


图 2.2 NES 的系统总线

2.1.2 内存

CPU 的 16 位的地址线，能够支持 64KB 大小的内存，寻址范围：0x0000-0xffff，如表2.1所示。

若游戏 ROM 只有一块（16KB 为单位），则加载到内存 0x6000，0x8000 这两部分中；若只有两块，则第一块加载到 0x6000，第二块加载到 0x8000；若游戏 ROM 超过两块 ($16KB \times 2 = 32KB$) 大小，将使用 Mapper 内存块对换来决定将哪块加载进内存，本课题暂未实现 Mapper。

¹¹ 图形处理器

表 2.1 NES 的内存区域

地址	大小	描述
0x0000-0x00FF	256B	Zero Page (也称为零页), 内存的第一页, 用于快速寻址
0x0100-0x01FF	256B	栈区, 空递减堆栈
0x0200-0x07FF	1.5KB	RAM 区
0x0800-0x1FFF	6KB	这块区域用于对 Zero Page 镜像 3 次, 意味着, 写到 0x0000, 同时也会写到 0x0800, 0x1000, 0x1800
0x2000-0x401F	16KB	内存映射 IO 寄存器, 从 0x2000-0x2007 这 8 个字节镜像填充满 0x2008-0x3FFF 区域
0x4020-0x5FFF		扩展区
0x6000-0x7FFF	8KB	SRAM, 用于访问卡带中的 RAM, 保存游戏用
0x8000-0xFFFF	32KB	这块区域被用于访问卡带的程序 ROM, 程序 ROM 以 16KB 为一个单位块 (bank), 一共两块

2.1.3 寄存器

6502 CPU 有 6 个寄存器, 其中 3 个特殊寄存器, 程序计数器 (PC)、栈指针 (SP)、程序状态寄存器 (P), 3 个通用寄存器, 累加器 (A)、X、Y 寄存器, 表 2.2 详细描述了各寄存器的作用。

表 2.2 6502 CPU 各寄存器作用

寄存器名称	寄存器位数	描述
程序计数器 (PC)	16	存放下一条待执行的指令地址
栈指针 (SP)	8	指向栈区 (0x0100-0x01ff), 从 0x0100 的内存位置作为偏移量, 空递减堆栈, 也不会检测栈溢出 (0x00-0xff)
程序状态寄存器 (P)	8	受到指令执行后的影响, 标记程序状态
累加器 (A)	8	存储算数、逻辑运算的结果
X 寄存器	8	一般做计数器或者用于一些寻址方式的偏移值, 或者 SP 的临时值
Y 寄存器	8	和 X 寄存器一样, 但是不能用来做 SP 的临时值

8 位状态寄存器 (P) 受到指令执行后的影响, 其中每一位都有特别的含义, 这些标志位在寄存器中的顺序如图 2.3 所示:

- 负数标志位 (N), 当运算结果最高位第 7 位为 1 的时候置位, 表明负数。

- 溢出标志位 (V)，当两个补码运算产生非法的结果置位，例如正 + 正为负的时候。
- Break 指令标志 (B)，用于标记当 BRK 指令执行后，产生的 IRQ 中断（软件中断）。
- 十进制模式 (D)，6502 通过设置该标志位切换到 BCD 模式，由于 2A03 不支持 BCD，所以这位是无效的。SED 指令置位，CLD 指令复位。
- 中断屏蔽标志位 (I)，通过设置该位可以屏蔽 IRQ 中断。SEI 指令置位，CLI 指令复位。
- 零标志位 (Z)，当运算结果为 0 的时候置位。
- 进位标志位 (C)，当运算结果最高位第 7 位符号翻转的时候置位。SEC 置位，CLC 复位。

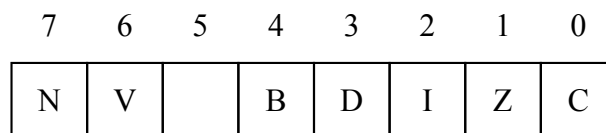


图 2.3 程序状态寄存器 P

2.1.4 中断

中断用于处理硬件、软件触发的信号，表明发生了某个事件需要注意。NES 有三种中断：不可屏蔽中断 (NMI)、可屏蔽中断 (IRQ)、复位 (Reset)，具体如表 2.3 所述。

表 2.3 NES 的中断

中断类型	向量地址	描述
NMI	0xFFFA	当 PPU 中每一帧图像渲染结束时产生 VBlank 信号触发该中断 (PPU 的控制寄存器 1 可设置是否发出 VBlank 信号)
Reset	0xFFFC	当用户按下复位按钮的时候产生
IRQ	0xFFFE	可屏蔽中断，受到中断屏蔽标志位 (I) 的影响，也能被 BRK 指令（软件中断）触发

各个中断优先级如下：Reset > NMI > IRQ。在中断产生的时候，执行一个中断一般需要 7 个机器周期，处理步骤如下：

1. 识别中断请求
2. 完成当前指令
3. 将 PC, P 寄存器入栈（保存现场）
4. 设置中断屏蔽标志，以防再次中断（关中断）
5. 将 PC 设置为位于中断向量表的中断程序地址
6. 执行中断程序
7. 执行 RTI 指令（相当于 x86 的 IRET 指令），出栈恢复到 PC, P 寄存器（恢复现场）
8. 程序继续执行

2.1.5 寻址模式

6502 有 13 种寻址模式，介绍如下。

隐式寻址 操作数隐藏在操作码中无需给出，也就是没有操作数

`CLC` ; 清除进位标志位

累加器寻址 只有累加器这一个操作数

`LSR A` ; 对累加器 A 进行逻辑右移

立即数寻址 操作数为第二个字节指明的常量，在 6502 汇编中用 # 号来表明

`LDA #10`; 将 10 存放到累加器 A 中

零页寻址 第二字节为操作数的地址，由于只用一个字节来表示地址，故操作数地址范围在 0x00-0xff，即零页，在 6502 汇编中用 \$ 来表明 16 进制地址

`LDA $00`; 将内存地址 0x00 上的存储单元的值作为操作数存放到累加器 A 中

零页 X 变址寻址 第二个字节作为基址，加上 X 寄存器的值作为最终操作数地址¹²

`STY $10,X`; 将内存地址 (0x10 + X) 上的存储单元的值存放到寄存器 Y 中

零页 Y 变址寻址 和零页 X 变址一样，只不过是换成了 Y 寄存器

`LDX $10,Y`; 将内存地址 (0x10+Y) 上的存储单元的值存放到寄存器 X 中

¹²需要注意的是地址高位不进位，地址始终限制在 0x00-0xff 范围内

相对寻址 分支跳转指令专用，第二个字节操作数（-128 到 127）加到 PC 指针上作为跳转目标的地址

`BEQ $2d`；若结果为 0 则跳转到 `PC+0x2d` 的地址

绝对寻址 操作数地址为第二、三字节组成的 16 位地址

`LDA $1234`；将内存地址 `0x1234` 上的存储单元的值存放到累加器 A

绝对 X 变址寻址 第二、三字节组成的 16 位地址加上 X 寄存器的值作为操作数地址

`STA $3000,X`；将内存地址 `(0x3000+X)` 上的存储单元的值存放到累加器 A

绝对 Y 变址寻址 和绝对 X 变址一样，只不过是换成了 Y 寄存器

`STA $3000,Y`；将内存地址 `(0x3000+Y)` 上的存储单元的值存放到累加器 A

间接寻址 JMP 跳转指令专用，第二、三字节组成的 16 位地址内存单元上的值作为地址

`JMP $FFFC`；跳转到 `Reset` 中断向量

零页变址间接寻址 第二字节为基址，加上 X 寄存器的值组成的零页内存地址（间址）单元上的值作为操作数地址

`LDA ($40,X)`；`(0x40+X)` 作为间址，作为操作数地址取操作数存放到累加器 A

间接寻址变址 第二字节为间址，取 16 位操作数并加上 Y 作为操作数有效地址

`LDA ($40),Y`；取 `0x40, 0x41` 组成 16 位地址，加上 Y 作为操作数有效地址，取操作数存放到累加器 A

2.1.6 指令集

6502 有 56 条不同的指令，各指令因为不同的寻址方式有不同的变种，总共有 151 个操作码¹³。指令长度在 1 到 3 字节，第一字节为操作码，后面的为操作数。具体的指令集细节可参考文献 [1]，指令可分为下几类：

- Load/Store 指令，读内存数据到寄存器，从寄存器写到内存
- 寄存器转移指令，复制 X 或 Y 寄存器内容到累加器（A）中，或相反
- 栈操作指令，入栈或出栈，根据 X 寄存器的值来读写栈指针

¹³还有 105 个未在 CPU 官方文档注明的操作码，本课题也对它们进行实现

- 逻辑运算指令，对累加器（A）和内存中的值进行逻辑运算
- 算术运算，对寄存器和内存进行算术运算
- 增减指令，对 X,Y 寄存器或内存的值进行增减运算
- 位移指令，对累加器（A）或内存中的值进行位移操作
- 跳转/调用指令，跳到指定地址继续执行
- 分支指令，当条件满足（P 寄存器）的时候跳到指定地址继续执行
- 操作状态寄存器指令，设置状态寄存器的某些标志位
- 系统指令，执行一些系统功能

2.2 PPU

Ricoh 公司也提供了 2C02/2C07¹⁴ 芯片作为图形处理器 PPU，PPU 的寄存器映射到 CPU 内存的 0x2000-0x2007 和 0x4014 区，这些特殊的寄存器用来控制图像信息，例如背景滚动、精灵图控制、数据传输等等。

PPU 的频率是基频的 4 分频，即 5.37MHz，正好是 CPU 频率的 3 倍。

2.2.1 显存

同样的，PPU 也有自己的内存，又称作显存（VRAM，Video RAM）。不像 CPU，虽然 PPU 也能寻址 64KB 范围空间，但是它只有 16KB 物理内存，其他区域是物理内存的镜像。表 2.4 为显存的布局。除了显存，PPU 还有一块 256 字节的 OAM 专门用来存放精灵信息（如坐标，图块号，是否翻转，颜色等等），每个精灵需要 4 个字节，一共能存放 64 个精灵信息。

NES 的调色板一共有 56 种颜色（用 6 个比特位来表示索引），然而这些颜色不能同时显示在图形上，显存中有 2 个调色板（分别位于 0x3F00-0x3F0F, 0x3F10-0x3F1F）：背景调色板、精灵调色板。每个调色板能够存放 16 种颜色，因为存放的是索引，所以也只需要用 6 个比特位来表达一种颜色，由于这两个调色板某些字节被镜像，最终只能显示 25 种颜色。

¹⁴2C02 用于 NTSC 版本，2C07 用于 PAL 版本

表 2.4 PPU 显存布局

地址	大小	描述
0x0000-0x0FFF	4KB	图块表 (Pattern Table)0, 存放背景、精灵图块的颜色索引的低两位
0x1000-0x1FFF	4KB	图块表 1, 同上
0x2000-0x23FF	1KB	名称表 (Nametable)0, 存放背景信息
0x2400-0x27FF	1KB	名称表 1, 同上
0x2800-0x2BFF	1KB	名称表 2, 同上
0x2C00-0x2FFF	1KB	名称表 3, 同上
0x3000-0x3EFF		0x2000-0x2EFF 的镜像
0x3F00-0x3F1F	32B	调色板, 存放背景/精灵的颜色索引
0x3F20-0x3FFF		0x3F00-0x3F1F 的镜像

显存中的图块表区域, 用来存放背景、精灵图块的调色板指针的低 2 位, 超级马里奥的图块表如图2.4。背景、精灵图块颜色信息需要一共需要 4 个比特位来存放。图块表一共有 2 个, 每个 4KB, 图块的尺寸为 8x8 像素, 每行 8 个像素点用一个字节来表示调色板指针的一位, 由于图块表只存放颜色索引的低 2 位, 所以需要 16 字节大小来存放一个图块, 一个图块表能存放 256 块, 图2.4按左右顺序排列了这 2 个图块表。

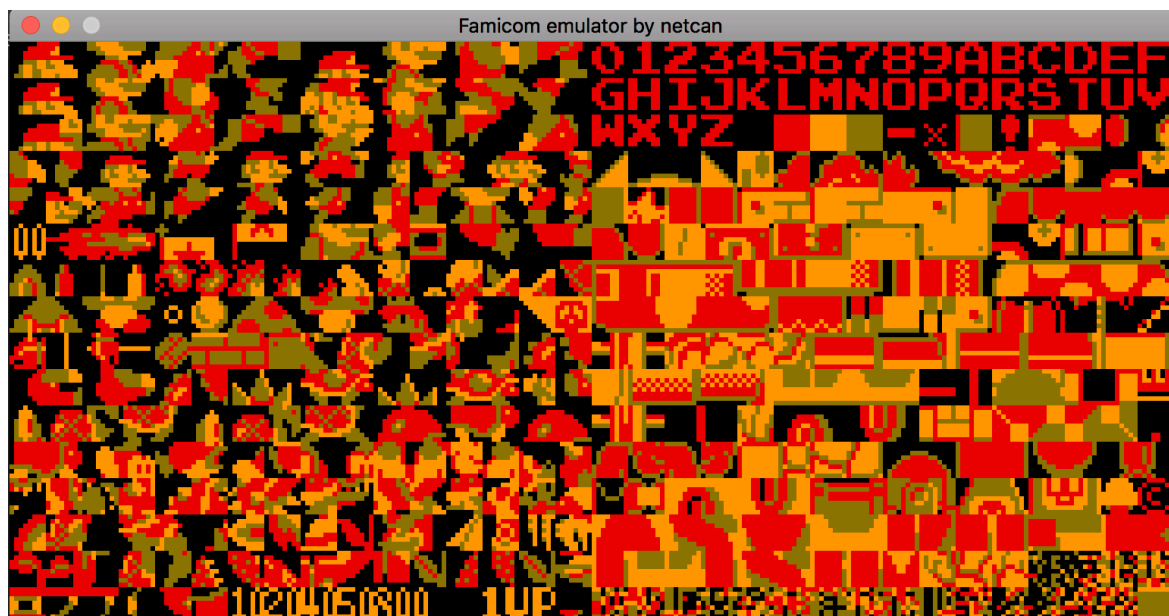


图 2.4 超级马里奥的图块表

而背景、精灵图块的调色板指针的高 2 位分别存放于名称表中的属性表、OAM

中。

虽然有 4 块命名表，每块 1KB，但实际上能用的只有 2 块，另外 2 块做镜像用，从而形成了垂直镜像、水平镜像等模式。命名表用来存放背景信息，每个字节表明图块表中的块号，由 PPUCTRL 控制寄存器来选择哪一个图块表。命名表由 $32 \times 30 = 960$ 块组成，形成 256×240 大小的背景图形，一共占用 960 字节，而剩下的 64 字节区域也叫属性表，用于保存背景图块的调色板指针的高两位。

OAM 用 4 个字节来描述一个精灵信息，第一个字节描述精灵的 Y 坐标，第二个字节描述精灵的图块号，第三个字节描述精灵的调色板指针的高两位、是否水平、垂直翻转，是否显示，最后一个字节描述精灵的 X 坐标。OAM 也支持 DMA，可高效地将 CPU 内存数据写入 OAM 中。通过写入 OAMDMA 寄存器来触发，写入 N 将会从 CPU 内存 $N \times 0x100$ 起始地址开始连续对 OAM 写入 256 个字节，这期间将会发生周期挪用现象，即 CPU 无法访存，也将无法进一步获取指令信息，直到 DMA 过程完成。

2.2.2 寄存器

PPU 的各个寄存器主要作用见表 2.5。

表 2.5 PPU 的各个寄存器主要作用

寄存器名	地址	属性	主要用途
PPUCTRL	0x2000	写	用于控制是否产生 NMI 中断、精灵的高度、背景块的图案表选择、名称表选择
PPUMASK	0x2001	写	是否显示背景、精灵
PPUSTATUS	0x2002	读	描述 PPU 的状态，是否处于 VBlank
OAMADDR	0x2003	写	OAM 读写地址
OAMDATA	0x2004	读、写	OAM 读写数据
PPUSCROLL	0x2005	写两次	背景滚动的位置（用于产生横、竖向滚动效果）
PPUADDR	0x2006	写两次	PPU 读写地址
PPUDATA	0x2007	读、写	PPU 读写数据
OAMDMA	0x4014	写	DMA

PPUSCROLL, PPUADDR 共用内部寄存器 [2]，各需要写两次生效，前者依次写摄像机的 x, y 坐标，后者依次写高、低地址。

2.2.3 渲染

参考文献

- [1] Andrew Jacobs. 6502 instruction reference. <http://obelisk.me.uk/6502/reference.html>.
- [2] Banshaku, Tepples, et al. Ppu scrolling. http://wiki.nesdev.com/w/index.php/PPU_scrolling, 2017.
- [3] Jonathan Sieber. *Implementing the Nintendo Entertainment System on a FPGA*. PhD thesis, 2013.
- [4] Art King. Fpga nes. 2012.

致谢

感谢我的母校，由于高考志愿填报问题导致我不能如愿以偿地进入本校计算机科学与技术专业进行学习，在食品与科学工程的两年里，依旧不忘初心地自学我所爱。凭借特长在各位老师、领导的支持与厚爱下转入信息工程系，让我得以深入学习，最后从事一份自己所感兴趣的工作。

感谢我的指导老师安鑫老师，安鑫老师严谨的治学态度和精益求精的工作作风，深深地感染着我，使我终生受用。从课题的开题到论文的最终完成，安鑫老师都始终给予我细心的指导，在这期间向我提出了许多宝贵意见和建议。当我遇到困难时，都是安鑫老师给我鼓励与指引，使我能够克服重重困难。在此谨向安鑫老师致以诚挚的谢意。

感谢支持和关心我的同学们，朋友职愈博、曹鑫，在毕业设计遇到问题能够提供建议与帮助，使我顺利地完成毕业设计。

最后，感谢我的家人，感谢你们在我的学习生活中所给予的支持和理解，让我能够不断进取。没有你们，就没有我的今天，你们的支持与鼓励，永远是支撑我前进的最大动力。

作者：罗能

2018 年 5 月 11 日

附录