6502 编程探秘

黄京

Apr 16, 2025

1 导言

在 Apple II 与 NES 等经典设备的黄金年代，程序员们用 1.79MHz 的 6502 处理器创造了无数奇迹。当现代开发者习惯于 GB 级内存时，这些先驱者却在 64KB 的「画布」上绘制出了精妙绝伦的代码画卷。本文将揭示如何通过精准的内存操控，让每个字节都发挥出最大效能。

2 6502 内存架构速览

6502 的寻址空间如同精密钟表，每个区域都有独特的设计哲学。零页（$0000-$00FF）的访问周期比普通内存少 1 个时钟周期，这看似微小的差异在循环中会产生惊人的累积效应。例如 `LDA $00` 仅需 3 个周期，而 `LDA $0100` 则需要 4 个周期。

栈空间的 256 字节限制催生了独特的编程范式。当处理器执行 `JSR` 指令时，返回地址被压入栈顶，但若在中断服务程序中过度使用栈空间，可能引发指针回绕灾难 —— 这是许多早期游戏出现随机崩溃的元凶之一。

3 零页攻防战

零页是 6502 编程的兵家必争之地。优秀开发者会为高频变量保留零页地址：

```
player_x = $10 ; 零页地址分配
bullet_cnt = $20
```

通过零页偏移可模拟额外寄存器。考虑以下伪寄存器扩展技巧：

```
MACRO LOAD_ZP_INDEX idx
   LDA $F0, X ; 当 F0 是零页基址时
ENDMACRO
```

动态重映射技术更将零页效用发挥到极致。在 NES 的《超级马里奥兄弟》中，通过 MMC3 芯片在飞行关卡时切换内存 bank，实现了零页空间的动态扩展。

4 内存拓扑设计

数据段规划需要遵循热力学第二定律 —— 高频访问数据应靠近处理器。将精灵坐标放在 $0200-$02FF 区域，而背景音乐数据置于 $C000 区域，这种冷热分离策略可减少跨页访问。页面边界惩罚的数学表达式为：

$$\text{周期惩罚} = \begin{cases} 0 & \text{当 addr}_{\text{新}} \,\&\, \texttt{0xFF00} = \text{addr}_{\text{旧}} \,\&\, \texttt{0xFF00} \\ 1 & \text{其他情况} \end{cases}$$

代码段优化则充满几何美感。将关键循环体置于内存中部的 $8000 地址，可使相对跳转指令 BCC 的覆盖范围最大化。一个经典的页面对齐案例：

```
   ORG $8100 ; 确保子程序起始于页面边界
draw_sprite:
   ; 高频调用代码
```

5 动态内存管理

在 64KB 世界中，静态分配是首选策略。《魂斗罗》的关卡加载器在切换场景时执行批量释放：

```
// 伪代码示意
void load_stage(uint8_t stage) {
   release_all_bullets();
   dealloc(prev_stage_data);
   alloc(stage_data[stage]);
}
```

固定大小内存池是粒子系统的救星。以下 256 字节管理器的核心逻辑：

```
mem_pool_init:
   LDA #<pool_start
   STA free_ptr
   LDA #>pool_start
   STA free_ptr+1 ; 初始化空闲指针

alloc_block:
   LDY #0
   LDA (free_ptr), Y ; 读取下一空闲块地址
   STA temp_ptr
   INY
   LDA (free_ptr), Y
   STA temp_ptr+1
   ; 更新空闲指针 ...
```

6 硬件协同优化

DMA 时序是艺术与科学的结晶。在 NES 的垂直消隐期执行 PPUADDR 设置，可实现无闪烁的画面更新。音频双缓冲的实现关键：

```
  LDA #<buffer1
  STA APU_ADDR
  LDA #>buffer1
  STA APU_ADDR ; 填充后台缓冲
  ; 等待 VSYNC
  LDA active_buffer
  EOR #1
  STA active_buffer ; 切换缓冲
```

内存镜像区域的写重定向技术，使得 Commodore 64 能在 $D000-$DFFF 区域通过 $0001 寄存器的第 0-2 位选择 I/O 设备，这种设计大幅减少了地址解码电路的复杂度。

7 调试与逆向

自制内存监视器是每个 6502 程序员的成人礼。以下断点处理代码可在触发时保存状态：

```
break_handler:
  PHA
  TXA
  PHA
  TYA
  PHA ; 保存寄存器
  LDA #<dump_area
  STA $FB
  LDA #>dump_area
  STA $FC ; 设置存储地址
  LDY #0
dump_loop:
  LDA ($FD), Y ; $FD 存储监视地址
  STA ($FB), Y
  INY
  CPY #16
  BNE dump_loop
```

《超级马里奥兄弟》的对象池复用机制，将敌人结构体大小压缩到 16 字节，通过状态字段的位掩码实现多态行为，这种设计使得同屏 5 个敌人仅消耗 80 字节内存。

6502 的内存管理艺术在今天仍闪耀着智慧光芒。从物联网设备到航天器控制系统，这些诞生于 8 位时代的优化思想仍在继续传承。当你下次面对现代系统的海量内存时，不妨设想：若将其视为 64KB 的珍宝，是否能用更优雅的方式解决问题？