# 真机启动改动

赵强龙 v0.1 撰写了 一(1-5)

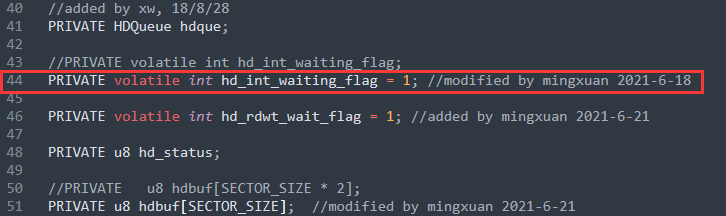
谷建华 2023-03-13 v0.2 添加了 一(0)

郭振豪 2023-4-19 v0.3 添加了 二、三

# 一、1.3.7及之后版本改动

## 0 变量初始化

Hd.c中hd\_int\_waiting\_flag必须初始化为1！



如果不初始化为1，它的默认值就是0。这在真机环境下的硬盘中断处理中会出问题。

## proc\_table[]的初始化

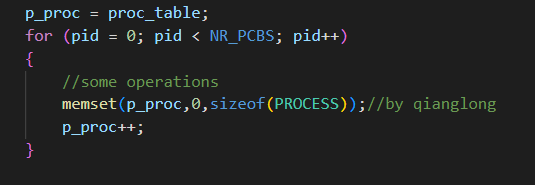
在真机上，1.3.7之后的proc\_table有着本不该有的值，目前影响到真机启动的值有如下:

proc\_table[i].task.cwd[]

proctable[i].task.sig\_set

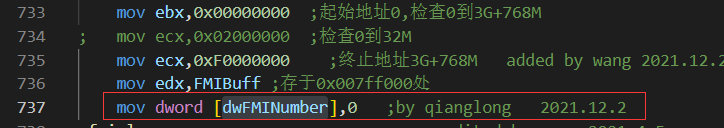
Protable[i].task.cr3

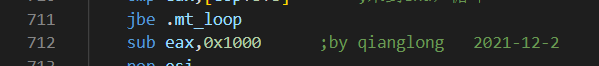
并未找到原因，只能在main.c中重新将proc\_table初始化清零。



## loader.asm

dwFMINumber处的值本应为0，但在1.3.7版本之后，该处的并不为0，导致检测到的内存信息无法使用，因此清零。



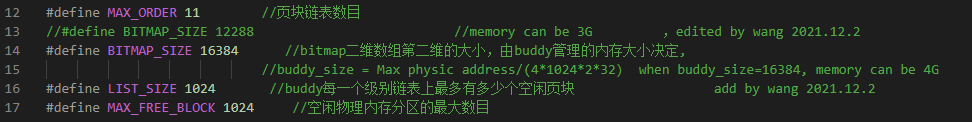


## Buddy.c以及buddy.h

block\_init函数中,只有对kbud的初始化时才需要调用fragmentUse函数

![$LFM4V0}Y0N](40N3%5@[CY](data:image/png;base64,)

修改了LIST\_SIZE与BITMAP\_SIZE两个宏。解决之前出现的buddy链表满的问题，以及未来内存可能接近4G导致bitmap不支持的问题。



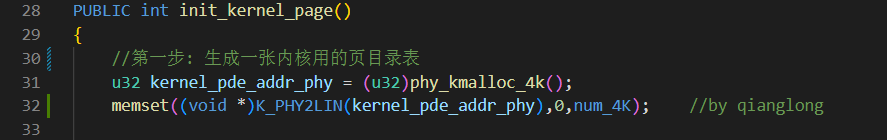
## loader.asm

应该用ja无符号比较跳转指令

10

## start.c

在此处重新初始化了内核页表。下图中申请的页目录，并未清零，导致后续判断页表是否存在的时候出错，所以进行清零处理。

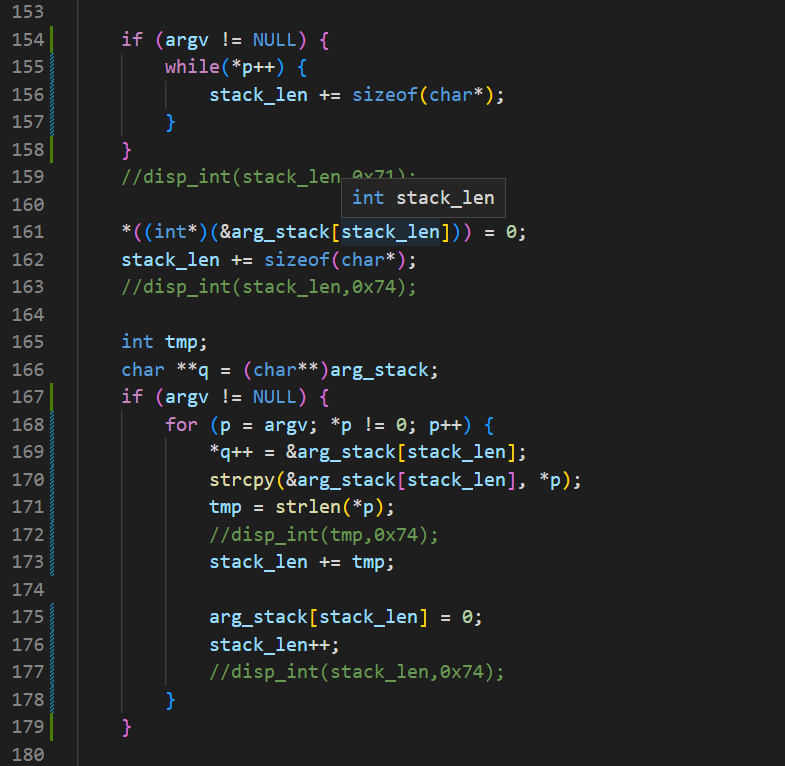


# 二、1.3.15及之后版本改动

## exec.c

kern\_exec() 函数中传递的参数char \*argv[], char \*envp[ ] 可能为NULL。NULL在mini-os中被定义为0，此时在内存中查询argv处存储的数据会造成野指针引用。

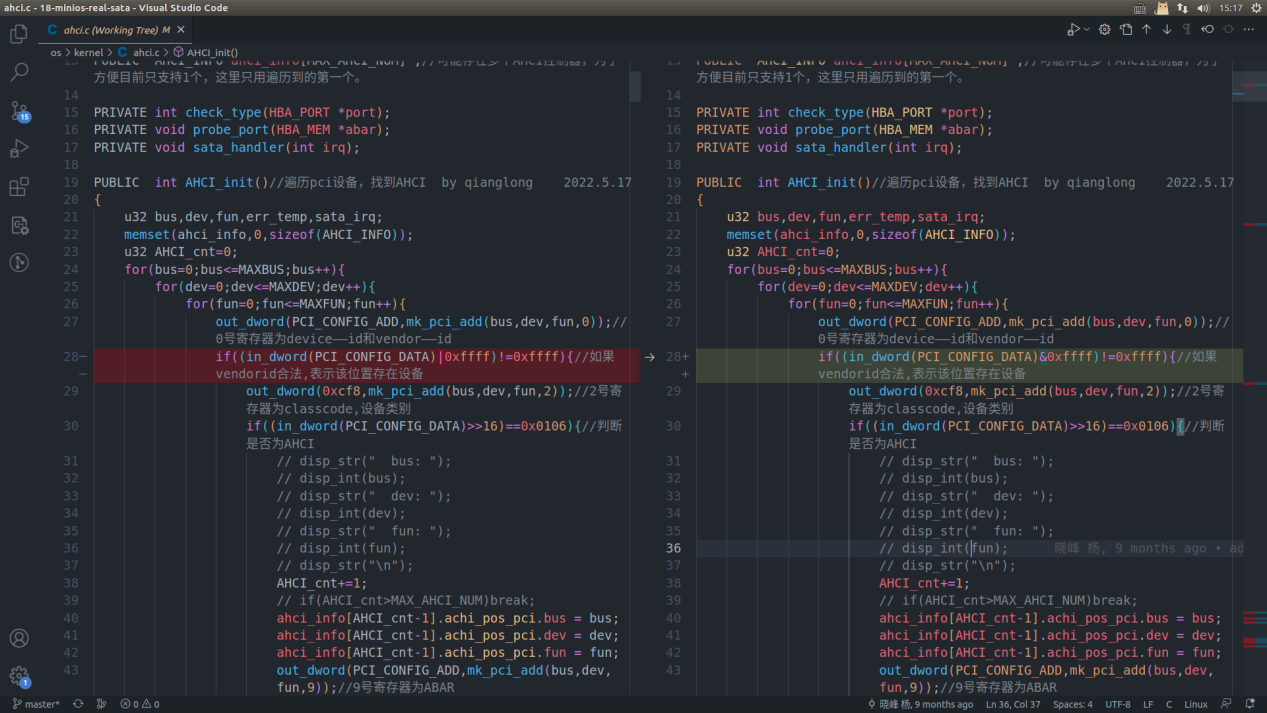
因此需要提前判断argv是否为NULL，不为NULL再进行相应的处理。



# 三、1.3.18及之后版本改动

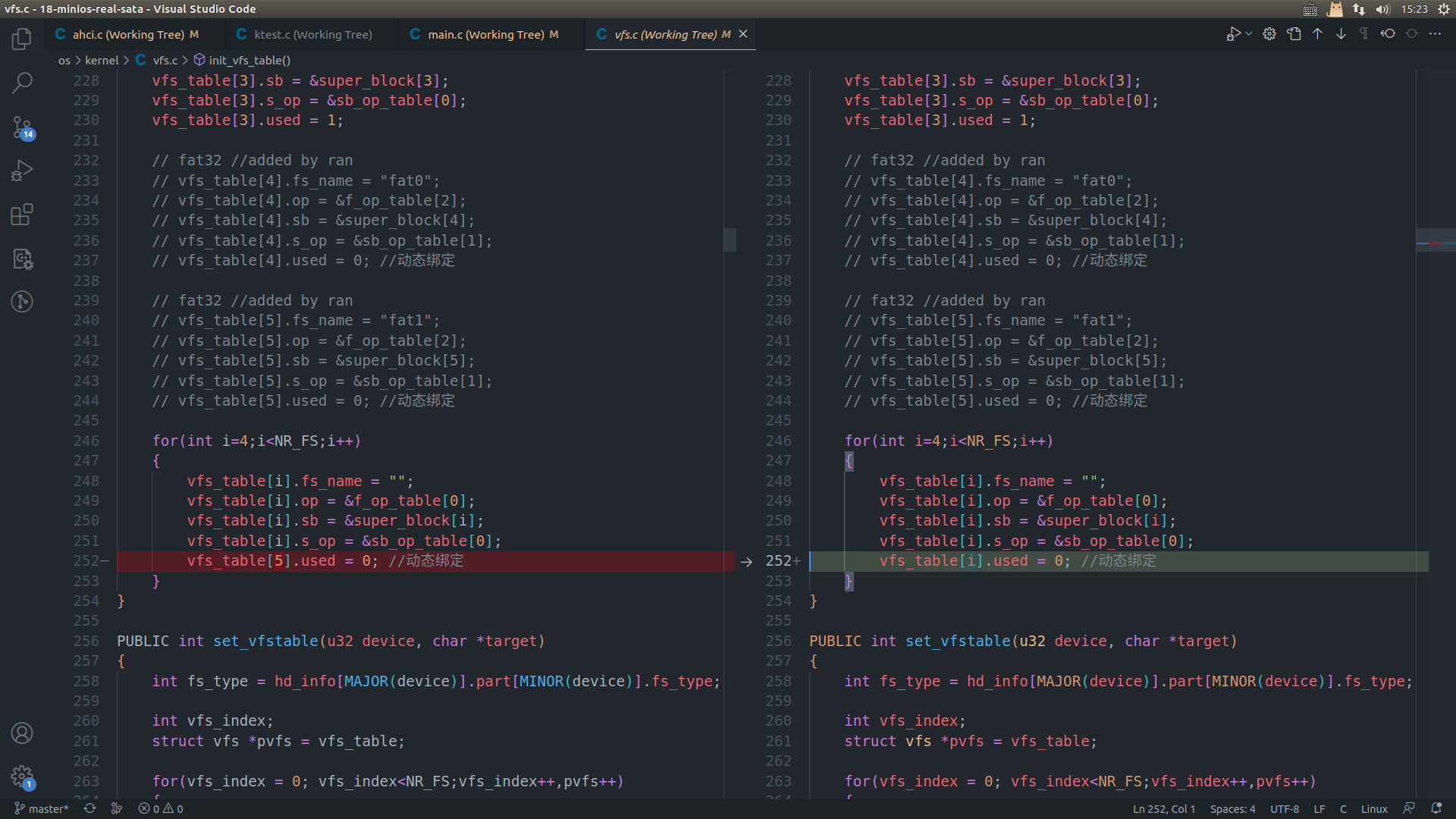
## ahci.c

AHCI\_init() 中下图标注的地方，判断vendorid是否合法，要将逻辑或（|）改成逻辑与（&）



## vfs.c

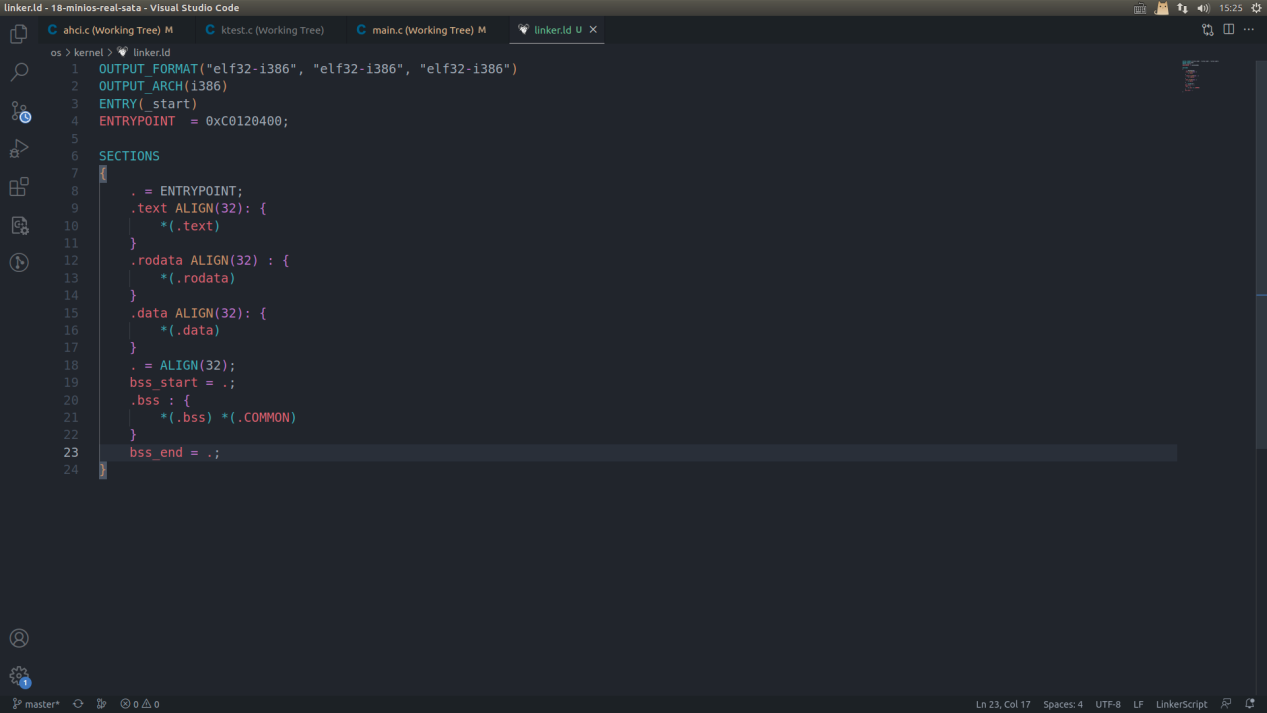
init\_vfs\_table()函数中初始化\_table之前笔误，将5改成i。



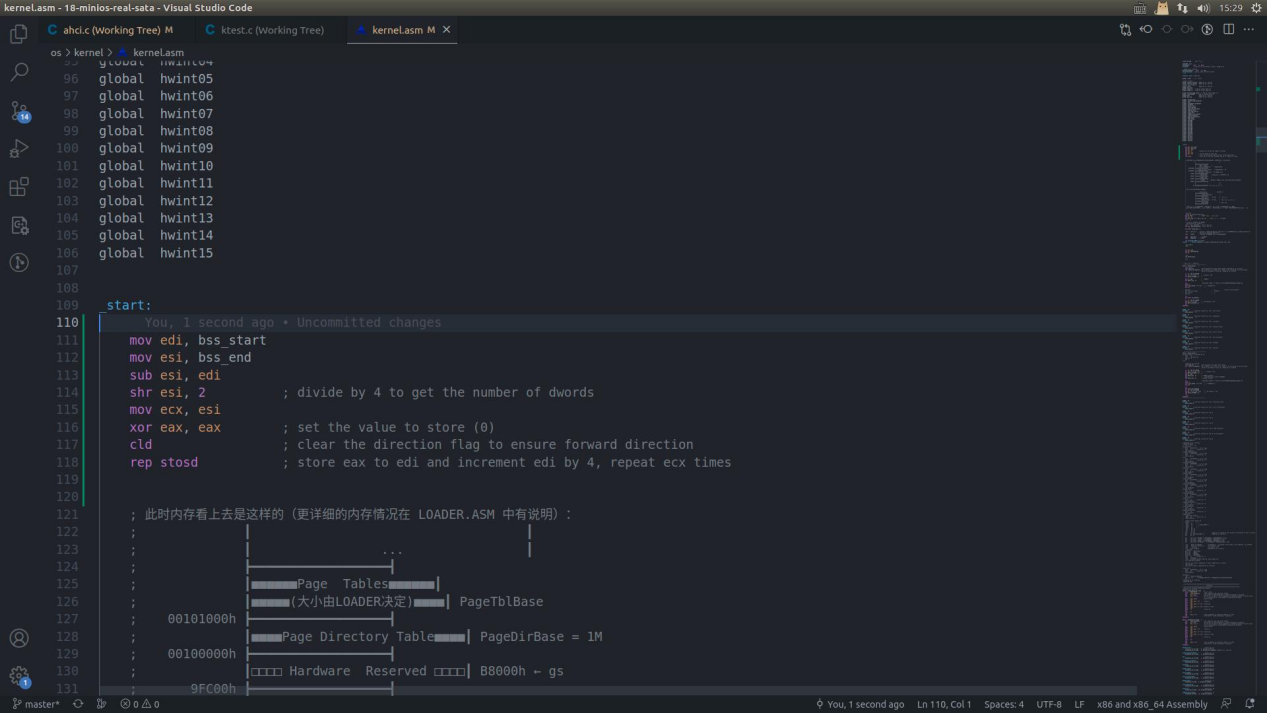
## 初始化bss段为0

由于bss段未初始化为0，会导致很多bss段中的变量（未初始化的静态变量和全局变量以及初始化为0的静态变量和全局变量）的初始值不为0，因此需要将bss段清空。

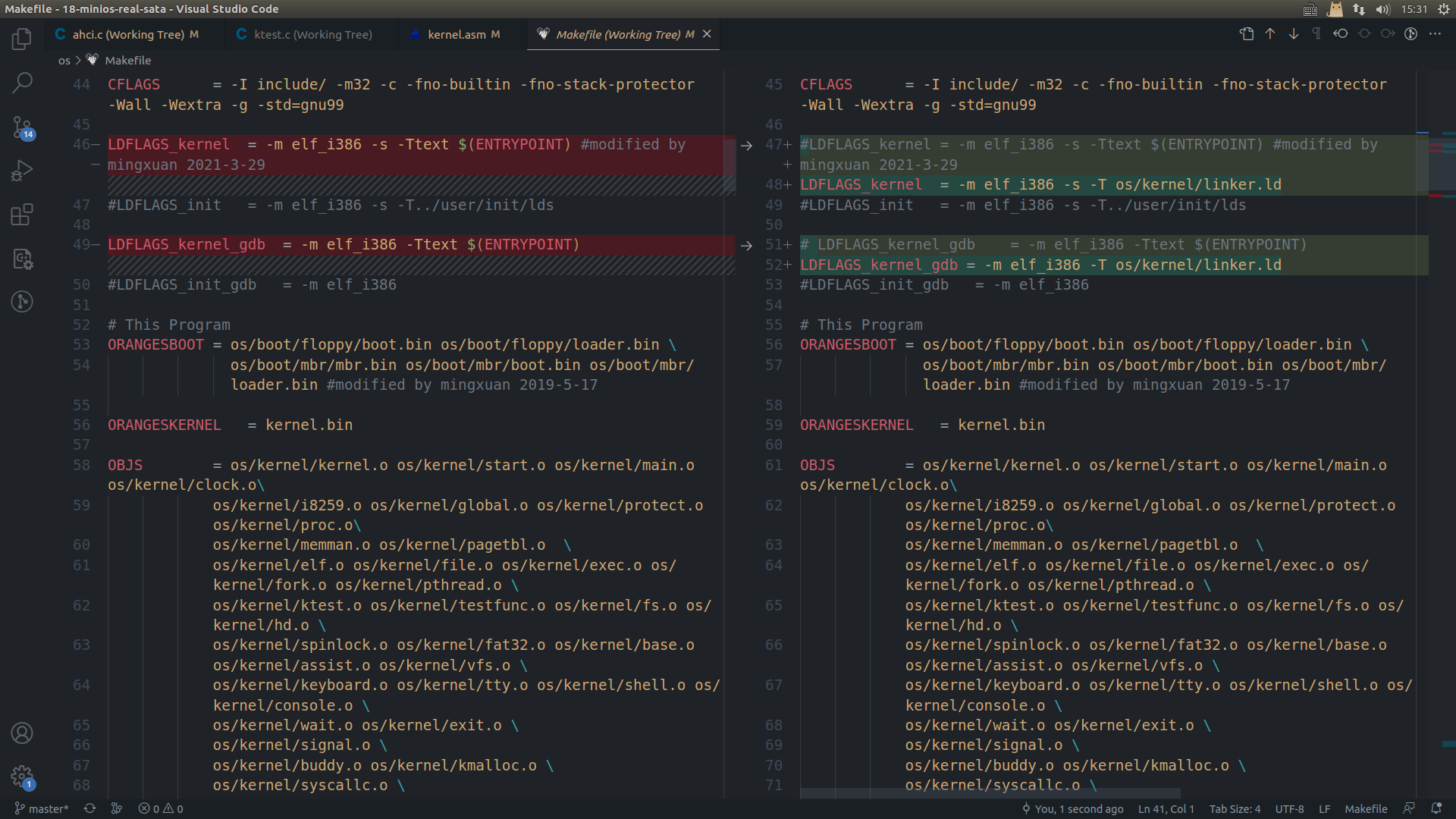
首先新增linker.ld文件，定义text段、rodata段、data段、bss段的相对位置，并且用变量bss\_start和bss\_end获取bss段的起始位置和结束位置。



在kernel.asm的\_start函数中，根据bss\_start和bss\_end清空bss段。



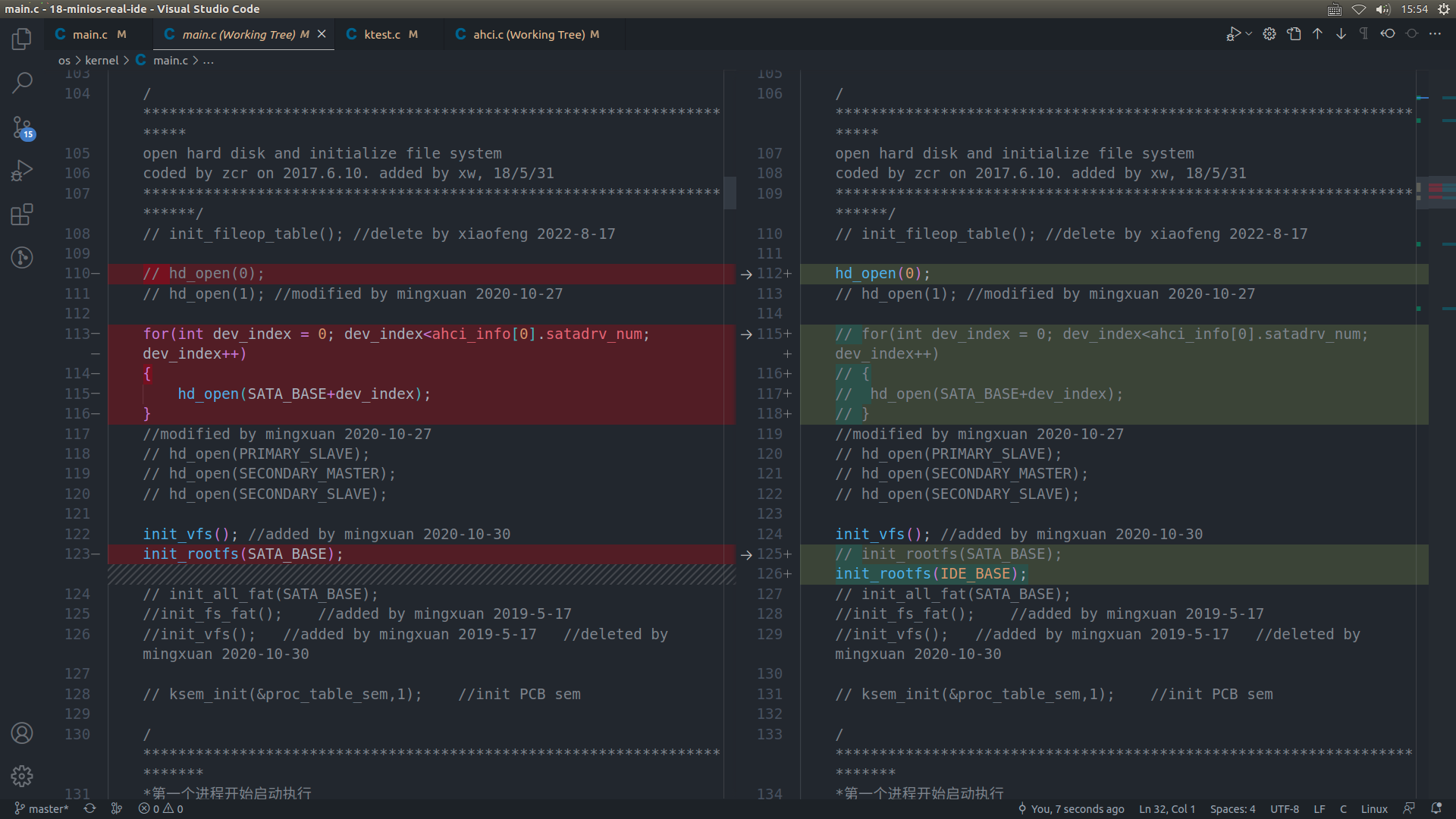
将os/Makefile中的LDFLAGS\_kernel和LDFLAGS\_kernel\_gdb修改为下图右方形式，以linker.ld作为链接脚本。



## 如果想调整为ide模式，需要如下步骤：

main.c的kernel\_main()

设备号0-3为ide设备，4以上是sata设备，调用hd\_open的设备号改为0，调用init\_rootfs（）的设备号改为IDE\_BASE。



ktest.c的initial()函数

调用init\_block\_dev()的设备号改为IDE\_BASE，调用mount()的设备名称改为dev\_hda1。

