准备：

1 MAME模拟器或Arcade模拟器

2 Notepad++及比较插件 [**自行下载或找我**]

若是不会基本的调试器操作，先看这个帖子

<https://www.ppxclub.com/forum.php?mod=viewthread&tid=697135>

敌兵量有两种情况，一种是**1至2名玩家**时的兵量，另一种是**3至4名玩家**时的兵量，

取决于当前玩家数量，找到玩家数量地址并将其值改为4后，

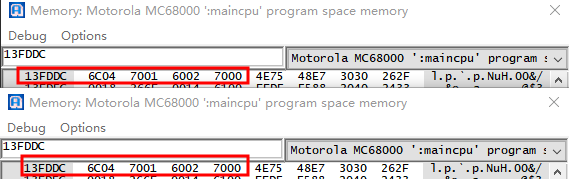
虽然可以直接4人兵量、敌将血量、敌将爆物，但会有各种问题，如**无法过图**、**死机**等等

每一个多玩家游戏都至少有一条敌兵初始化时检测玩家数量，以决定出兵量的语句，

然而某些游戏里不同的敌兵、不同的场景，甚至不同的关卡都会有独立判断初始化的语句，

而如果是这样的话，找到两个地方的兵量初始化判断地址，打开两个内存浏览区域，

**分别键入**这两个地址，并观察其**操作码及连续的字节码是否相同**，如



这是同一个地址，只是为了举栗，可以看到这一连串的都是一致的，

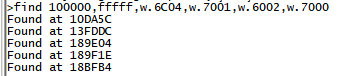
那就可以用 **find** 指令搜索字节码一致的地址了，在CE里可以称之为特征码搜索，

键入 find 100000,fffff,w.6C04,w.7001,w.6002,w.7000 (神剑伏魔录等游戏另当别论)

(find为搜索指令，100000是搜索的起始地址，fffff为后续搜索长度，因为已经有13FDDC，

一般游戏相似功能的地址都不会放太远，所以肯定都是包含在100000到1fffff里的，

而w为数据类型，其后用 点. 接字节码，用 逗号, 接连续的字节码，**某些游戏要字节反转**)



能搜索出这些相同操作码的地址，依次筛选或全部修改，比自己一个一个找要轻松很多

其次是**初始化时机**，就我所知的有

1 **入场景黑屏后显示敌兵前初始化，黑屏结束前敌兵就已出现**，如31下路第一个门上去，

单打**进门就能看到3个蛮兵**，因为敌兵初始化在黑屏时就完成了，但在黑屏前一直帧进，

直至黑屏，会发现玩家数量地址的值从1变成了0，继续帧进又会变成1，

可以从1出现的时候开始计算帧找关键帧，或者直接trace然后帧进十多次也行，

只是这样导出的无用指令会很多，找关键跳转很麻烦



2 **入场景黑屏后敌兵入场前初始化，黑屏结束敌兵出现**，如31下路，可以套公式，

如用张飞进入下路后，帧进让蛇矛的这个部位到边沿，**再帧进一次敌兵就会初始化并出现**，

在这个时候就可以trace差异



3 **移动至指定区域敌兵就会初始化并出现**，如我这篇教程，**再往右走一步敌兵就会出现**



**开始正文**，拿32-群雄争霸举栗，这游戏改起来比31麻烦多了

先说一下，有些游戏默认只能两名玩家同时游戏，为了方便要开启四名玩家，

**也可以直接跳过这一步**，



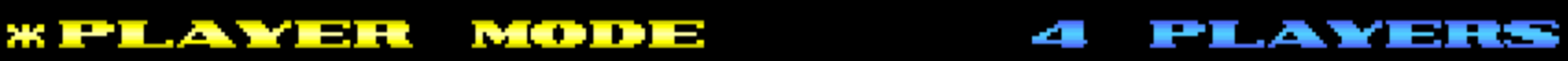
按出**Tab菜单**，**机台开关**-**维护模式**，然后**软重启**游戏，

按**1P上下方向键移动光标**至 OPERATOR SETTING ，按**攻击键选择**，移动到PLAYER MODE ，

按攻击键将其改为 4 PLAYERS ，这时就可以在Tab菜单里**关闭维护模式**，

然后两次移动至 EXIT 退出









正常投币选一般模式或专家模式进入游戏，

这时就可以找**玩家数量**，一个玩家时搜索1，增加一个搜索2，一般到4就得到唯一地址了，

若是没有，那就读档然后重复，若还是有几个，那就逐个改4**测试兵量是否增加**

群雄的玩家数量地址为 815907

将其改为4后兵量明显是三人以上时的量

Ctrl+M打开内存浏览窗口，键入玩家数量地址 815907 并回车两次，然后把窗口放一边

**保存游戏以便回档**，然后找一个好位置，如这个位置，

第一关BOSS前刷新最后一批敌兵前的地方，**再往右走一步就会刷新出敌兵**，

可不用这么麻烦，我这样只是为了尽量**减少trace出的无用地址**，

亦可开启trace后一路走到敌兵初始化区域，但需保证**在每一帧里发生的动作是相同的**，

差异只是玩家数量，这样trace出的指令差异会减到最少，即使测试所有跳转也很轻松



**再次保存游戏以便回档**

暂停游戏，按住方向右键不松的同时帧进一次，然后就可以松掉方向右键，

这时候留意帧进，开始测试，

把内存浏览区域玩家数量地址值的1改为4，解除暂停并看兵量变化

反复读档，每一帧都测试，直到发现某一帧改4解除暂停后兵量依然无变化，

那就找到关键帧了

我之前说了再往右走一步就会刷新出敌兵，

简单说若是人物变成走动的姿势，就已经移动到了敌兵初始化触发点，并完成了敌兵初始化

不出意外的话按上述步骤帧进并松掉右键后，再次帧进两次角色就会变为走动姿势，如这样



要做的就是在这一帧的前一帧开启trace记录

**先让玩家数量默认1**，**在关键帧的前一帧**键入 trace 1.txt ，**帧进一次后**键入 trace off 关闭，

**这次是记录的单人兵量初始化地址**，**读档后将玩家数量改为4**，

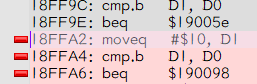
再重复**关键帧前一帧**键入 trace 2.txt ，**帧进一次后关闭**就记录到了**四人的兵量初始化地址**

差异对比文件有了，接下来就需要借助工具对比，工具在我发的全屏攻击修改教程贴里下载

将trace出的两个文件拖入Notepad++，并**以2.txt为主对比文件**开启差异对比分析，

这次没有改全屏攻击那样方便的切入点了，按**Alt+Page Down键跳转到下个差异点**，

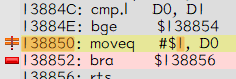
**尽量找红色区域且上一条指令为b开头的跳转指令**，如



(此处为举栗，可跳过) 复制 18FFA2 ，在调试器里键入 bp 18FFA2 ，会发现游戏立即中断，

这样还没见到敌兵就中断的肯定不是要找的关键跳转，键入 bpc 清除这一条断点，

并按F5运行，回到Notepad++，**继续往下找**，**依次测试**



13884E 就是群雄的兵量初始化判断地址，

bge意为大于等于就跳转，但这里有问题，实际应为ble，即小于等于跳转，不用纠结这个，

复制地址 13884E ，在调试器里键入 bp 13884E ，并没有立即中断，

这时候**再往右走一步**，人还没动就中断了，因为到了敌兵初始化区域

(值得一提的是几个三国战纪的兵量初始化关键跳转都是 bge ，除了盖世)



会看到如图所示，且按**回车**单步执行会发现**必定跳转**，因为人数小于3人，

要做的就是**让这个指令不跳转**，键入 maincpu.rw@13884E=4E71

(4E71即68K汇编的nop指令，将这条语句**无效化**，或者若是不跳转的话就改成让其跳转)

然后键入bpc清除断点或手动关闭断点，并按F5运行游戏，**读档后往右走**会发现兵量增多



如群雄最显著的就是多两个胖子，玩过的应该都知道这是三人以上才会出的

**简约版思路**：

1 玩家数量为1，小兵出现前 trace 1.txt 记录，出现后 trace off 关闭

2 玩家数量为4，小兵出现前 trace 2.txt 记录，出现后 trace off 关闭

3 将trace出的两个文件拖入Notepad++并对比差异

4 寻找小兵出现才会中断的跳转

5 处理跳转