目录：

本篇

01 概述

02 准备

03 如何启用调试器

04 如何通过精确搜索找到并修改无限气

05 如何将找到的地址保存到作弊菜单

06 如何通过共用指令找地址

07 如何修改汇编指令

08 如何通过模糊搜索找到并修改无限时间

09 如何通过断点修改寄存器的值

10 如何自定义条件断点

补充

扩展篇

01 如何修改穿戴装备无视等级限制

02 某些游戏如神剑伏魔录该如何搜索作弊码

附录

命令及解释集

ARM操作码字节模板

------------------------------------------------------------------------------------------------------------

01 概述：

**①** 搜索及修改方法不局限于教程，不同游戏汇编可能有所不同，如三国战纪1是68k汇编，

而三国战纪3是ARM汇编，若不懂什么是汇编，建议自行百度或谷歌搜索了解，

理论上只要Arcade或MAME能运行和调试的游戏都能修改

**②** 若有不懂的地方可回帖或私信问我

**③** 若有英文基础或不嫌麻烦手动翻译，可在调试器输入框内输入 help 后回车，

所有的调试器命令相关信息都能在这里浏览到

------------------------------------------------------------------------------------------------------------

02 准备：

**①** Arcade / MAME模拟器及欲修改的游戏rom

因本篇教程基础部分采用三国战纪3举例，

思路通用，但若是完全初学者可先跟随教程做一遍，

若已有模拟器及rom则跳过此处，若是没有，于此贴下载，

[https://www.ppxclub.com/forum.php?mod=viewthread&tid=684109](https://www.ppxclub.com/forum.php?mod=viewthread&tid=684109&highlight=PGM2)

或是在奶妈及论坛其他坛友的帖子里下载

**②** MAME Debugger命令

若想了解更多，此贴有中文注解，虽然不全面

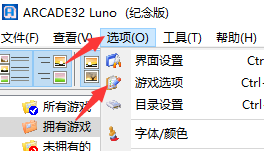
(附件了修订过的版本 命令及解释集.txt ，基于下方链接帖子里前辈所写的注解，添加了部分没提到的命令，剔除了少部分基本用不到的命令)

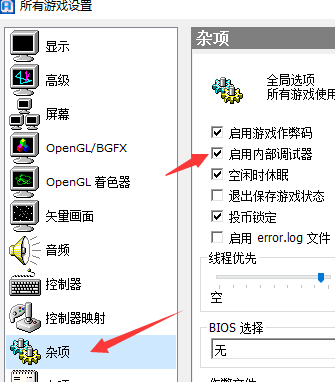
<https://www.ppxclub.com/forum.php?mod=viewthread&tid=669492>

------------------------------------------------------------------------------------------------------------

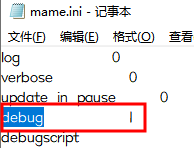
03 如何启用调试器：

**①** 若是Arcade / MAME模拟器，则按此步骤启用游戏作弊码和内部调试器





**②** 若是没有GUI的MAME模拟器，则需要在模拟器根目录找到mame.ini，即模拟器配置文件，打开后搜索debug，将右侧的0改成1 ，之后保存，若默认1则无需变更



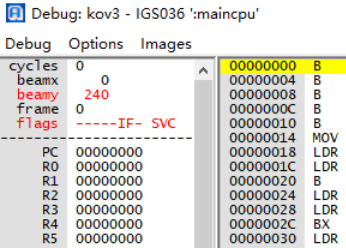
若没有这个文件，则在模拟器根目录空白处按住shift后按右键，

选择在此处打开CMD或PowerShell，之后输入mame.exe -createconfig ，

便会创建配置文件

或是在mamep图形界面里开启debug

**③** 之后进游戏，以三国战纪3举例，



进游戏后会弹出调试器，且游戏持续黑屏，

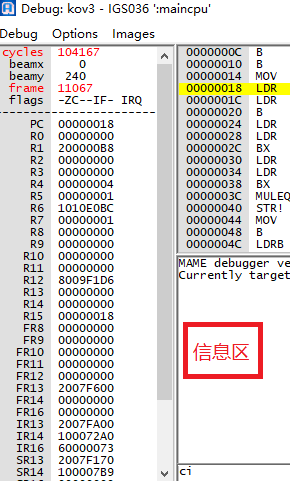
这时候点一下调试器，并按下F5即可运行游戏，

注意不要关闭调试器，然后游戏里正常投币选角色进图

------------------------------------------------------------------------------------------------------------

04 如何通过精确搜索找到并修改无限气：

 可以看到当前有5格气，



暂停游戏 (暂停可有可无，仅为锁定数据搜索) ，然后在调试器的输入框里输入 ci

(ci全称cheat initial ，即初始化作弊搜索，每次搜索新的作弊码前都要先输入ci，

输入后看不到任何变化很正常，因为暂停了游戏，此时在信息区滚轮一下，或解除游戏暂停，

就会看到信息区的变化)



再在输入框输入cn eq,#5

(cn全称 cheat next，即搜索作弊变化，搜索作弊码就是不断筛选的过程，

eq全称 equal，意为等于，

#表示其右侧跟着的数据类型为10进制，若是不添加#则默认为16进制，

当然，若只是0-9的数据变化区间可不用加#，

十进制为 0 1 2 3 4 5 6 7 8 9

十六进制为 0 1 2 3 4 5 6 7 8 9 A B C D E F

数字5是因为当前有5格气，所以搜索10进制的5)

回到游戏AB施放技能用掉一格气，暂停游戏



这时在调试器输入 cn eq,#4

(若是手抖搜索了错误的值，可以输入cu以撤销刚才的搜索，返回到上次结果)

数据会剩下两三个，

再次游戏内AB用掉一格气，输入 cn eq,#3

还是剩下两条，不用继续以此种方式筛选，直接测试哪条才是存储气值的地址

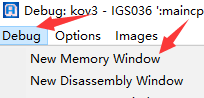


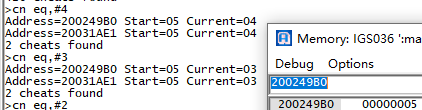
(address表示地址，start表示起始值，如初次 eq,#5时start就是5，current表示当前值)

点一下调试器，

按下Ctrl+M，或用调试器Debug菜单的New Memory Window打开内存浏览区域，

此处可输入地址以查看对应地址所存储的值





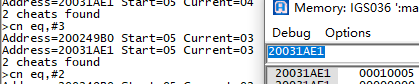
在内存区域输入刚找到的第一条地址 200249B0，并回车两次，

有时只回车一次可能无法精确定位到地址对应的值，可以看到其值为00000005，

因为刚没暂停，站了下街气已经恢复到5了，所以这里的5可能就是存储气的值，

先回游戏把5个气都用掉，会发现原来的5变成了0，将原来5位置的0改为5，

再回游戏AB施放技能，施放不能，那这个就不是存储气的地址，



再输入第二条的地址 20031AE1，站街满气显示5，

以测试第一条地址的方式回到游戏把气用完，再将原来5变0的数字改成5，

可以看到虽然气条不满1格但仍可继续施放技能，那这个就是对的地址

------------------------------------------------------------------------------------------------------------

05 如何将找到的地址保存到作弊菜单：

① 可用记事本或任何方式记录正确地址

② 亦可在调试器输入cl 名字 <.可选文件后缀>

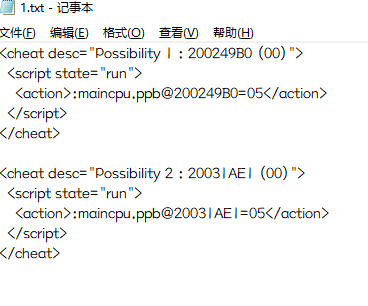
(cl 全称 cheat list，输入cl等效于cheatlist，

即把当前搜索到的作弊码条目以MAME作弊表的形式保存到文件，

名字可以任意，亦可自行添加后缀，此处以1.txt举例)

以后者举例，输入cl 1.txt ，

之前搜索到的两条地址就会被以名字为1.txt的文件保存到**模拟器根目录**，

 打开后内容如图，科普下：

① cheat desc=”” ，双引号内容为显示在作弊菜单的作弊项文字，可任意更改

② script state=”” ，双引号内容为切换或运行的方式，其值可为run、change、on、off



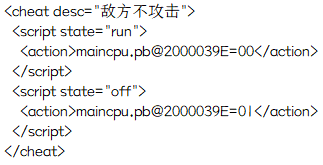
run在作弊菜单里往右切换就能开启并锁定

change一般用于paramer自定义列表，具体用法参考另一篇书写作弊表的教程

on在作弊菜单里是显示set，回车就能生效但不锁定，可与run和change共存



off一般用于还原，如图，用作开关，当开启时执行run的内容，当关闭时执行off的内容



③ <action></action> 标签里的内容为执行的操作

maincpu代表cpu类型，亦是一个地址，暂时不用管就这样写，扩展篇会讲到另一个名为prot的类型，也就是说调试器找到的只是偏移地址，要用cpu类型+偏移才能指向对应地址

pb为数据类型：

p是ram也就是内存地址，也可以是r，r为rom地址，改汇编要将p改为r

b为数据类型，有b、w、d、p，b为字节也就是xx，w为二字节也就是xxxx，d为四字节也就是xxxxxxxx，p为八字节)

@xxxxxx 即为引用地址：

=后内容为值，视@前的数据类型而定，若为b则此处为两位，w则为四位，以此类推

简言之，直接从别的作弊表里复制要的这一大段，然后自己改说明文字改地址改值即可，

亦可用cl保存作弊表的方式复制粘贴到这里，然后自己修改

其次，不同的游戏有与之版本对应的作弊表文件，存储在模拟器根目录的cheat文件夹里，

以三国战纪3为例，104版三国战纪3的作弊表文件名为kov3.xml ，

之前提到过的cl保存作弊表只是保存在模拟器根目录，

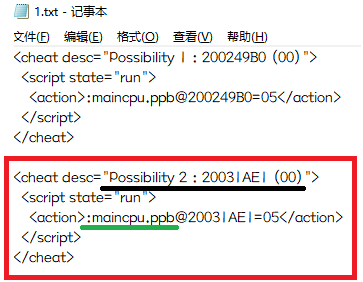
若是不把内容复制粘贴到对应游戏版本的作弊表里，是不会在作弊菜单里看到的，

因为作弊菜单加载的cheat文件夹里的作弊表文件



版本名即是rom名，进游戏后模拟器标题栏右侧能看到

回到之前的步骤，打开cl保存的1.txt是这样的

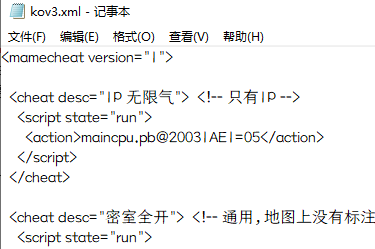


已知正确的作弊码地址是第二条也就是20031AE1，

划黑线的地方可以任意更改，划绿线的地方可以去掉冒号和两个p中的一个，

把这一整段复制，然后打开cheat目录的kov3.xml作弊表文件，

粘贴到非<mamecheat>标签外的任意地方，如这样

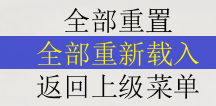


可以自己写注释，xml文件的注释格式为 <!-- -->，

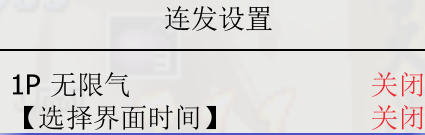
在其中间空白的部分可以写任意文字而不会影响作弊菜单

之后重进游戏或是在游戏里按Tab键调出菜单列表切换到作弊菜单，

手动或是按End键跳到最下面，



选择全部重新载入，再回到最上面就能看到刚添加到作弊菜单的无限气项，



将1P 无限气切换到开启状态回到游戏即可无限释放技能

------------------------------------------------------------------------------------------------------------

06 如何通过共用指令找地址：

之前只找到了1P的无限气地址，但2P呢

**①** 换2P手动重复搜索及添加过程

**②** 或用更高级的方法，下断点

不论是街机游戏还是PC游戏，都会有一些共用指令，同时处理多个地址，如一条指令同时处理1-4P的气值减少或增加，相当于编程语言传参数调用函数，只是传进去处理的参数不一样，而处理的过程基本是一样的

以找2P无限气作弊码为例，复制刚才找到的1P无限气作弊码地址，

游戏里依然用1P，因为要用1P触发改写断点以获取共用指令地址，

在调试器输入框里输入 wp 20031AE1,1,w

(wp 全称 watch point 监视断点，后接地址，1为监视字节长度，不用管，照抄，

w为write 写入数据，也可以是r，read 读取数据，这里用w监视写入数据，

当地址20031AE1存储的值被改写时游戏就会中断在改写值的指令处)

回到游戏AB施放技能，会发现游戏立刻卡住，回到调试器滚轮会刷新出如下内容，

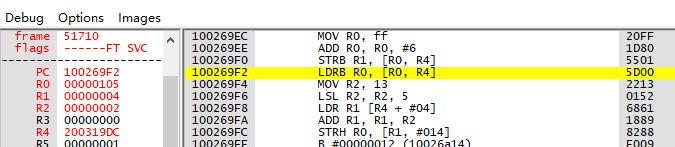


翻译一下：

断点1已设置

在断点1中断并往地址20031AE1写入4 (PC=100269F0)

此处的PC即共用指令的地址，也叫汇编指令的地址



观察上方的地址，之前指令地址显示的是100269F0，但为什么会停在100269F2？

因为100269F0已经执行完了，这个不用深究，然后看269F0的指令说明，

STRB就是赋值的意思，R1、R0、R4都是寄存器，在左边那一排可以看到寄存器的值，

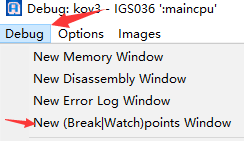
[]里的基本就是寄存器加上寄存器或者一个值=地址，

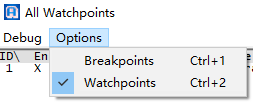
而68K汇编指令也就是这里的街机汇编指令，赋值是从左往右的，

也就是说这里的R1, [R0, R4]是把R1 的值2赋给地址 (105+200319DC) ，

用计算器十六进制把105+200319DC会发现刚好等于20031AE1，也就是1P的无限气地址，

记下100269F0的地址，然后按下Ctrl+B，或菜单指令打开断点列表





默认打开显示断点列表，菜单或快捷键切换到监视断点列表，

点一下刚才wp地址的En那一列的X，就关闭了对应地址的断点，

亦可在调试器输入框输入 wpc (watch point clear 监视断点清除)，即清除所有监视断点，

或是输入wpc ID，ID可在监视断点列表里看到，如此就只会清除对应的断点，

确认这个断点不会影响游戏了之后，点一下调试器任意窗口，按下F5即可恢复游戏运行，

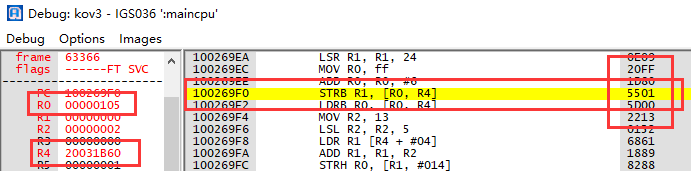
回到游戏，切换到2P，在调试器输入框输入 bp 100269F0

(bp 全称 breakpoint 断点，wp是用来监视内存地址的，而bp是用来监视指令地址的，

100269F0是之前找到的共用处理指令地址，

也就是说当程序执行到或是调用100269F0时游戏就会断下来)

用2P AB释放技能，游戏立即断下，



观察指令里的寄存器，再观察左侧寄存器的值，对号入座用计算器加起来并测试就会发现，

R0+R4就是2P的气值地址，把得到的地址添加到作弊表就行

不局限于此，像是找多玩家相关的地址之类都可以这样

------------------------------------------------------------------------------------------------------------

07 如何修改汇编指令：

其实还有另一种方式可实现通用无限气，即直接把这句共用指令无效化，

也就是不会再改变本应处理的地址的值，依然拿无限气举栗

气减少的处理指令是 100269F0，观察上图会发现在 100269F0指令的右侧有个5501，

这里的5501是操作码，也就是汇编指令的机器码或是字节码，

将其改成4E71或0000 (4E71即68K汇编的nop，但三国战纪3等几个PGM2游戏是并不是68K汇编，而是ARM汇编，简单说这里的4E71并不是nop，而是将其替换成了无用代码，也就是说写0000也能达到相同效果) 就能让这句指令无效，

在调试器输入框里输入 maincpu.rw@100269F0=0000

(框架直接照抄，r意为rom修改的是ROM地址，w为二字节，

因为操作码有4位也就是2个字节，而b的只有2位也就是1字节，所以这里用w，

@指令地址=0000，这样就行了)

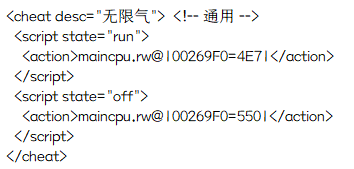
现在回游戏就能无限放技能了，而且1P也能无限放技能

其它用途如道具不减，时间不减，血量不减 blahblah

但若是重上游戏或是用F7读个档会发现又失效了，

重上游戏无需解释，读档是因为PGM2的F7会重置指令地址，

也就是把改成4E71的5501还原成5501，这样也很好解决，将地址添加到作弊菜单就行了



如这样，无需过多解释，

第二个script的off一整段是当这条作弊项在作弊菜单往左切换至关闭的时候还原字节码

------------------------------------------------------------------------------------------------------------

08 如何通过模糊搜索找到并修改无限时间：

三国战纪3的时间初始为999秒，但若是直接ci初始化再搜索是搜索不到的，

因为ci默认是初始化搜索字节型数据，数据类型我之前提到过，

这里提一下 有符号(signed) 和 无符号(unsigned) 数据类型，

不用了解太多，百度就有，无符号数据类型一般用不到，

有符号字节型byte数据范围是0-255，所以搜不到999，除非时间减少到255以下，

而有符号二字节型word数据范围是0-65535，这里搜索时间完全够用，

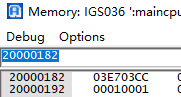
所以初始化的时候用 ci sw，即初始化有符号二字节，这样搜索出来的数据都是二字节的

(虽然用不到，但提一下，若搜索无符号数，则初始化要写为 ci ub/uw/ud/.. )

比如现在时间是973秒，输入 cn eq,#973，一般只有一个，

若有几个就变化时间再次搜索变化后的，我这里找到的时间地址为20000182，

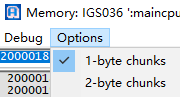
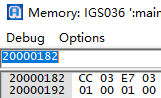
Ctrl+M打开内存浏览区域，输入地址会看到，



若看不懂正常，因为是16进制的，

前面的03E7为时间上限，转化为10进制为999，

后面的03CC为当前时间，转化为10进制为972，

将其显示方式改为1字节会发现显示是倒过来的，具体自己科普，不影响修改和使用作弊码，

把显示方式改回四字节然后把03CC改成03E7时间就变成了999秒，

添加作弊码并不需要反着写值，直接把999转化为十六进制用0补全四位，

如这样写就行了，maincpu.pw@20000182=03E7 (w和用0补位很重要)

再就是模糊搜索，有些东西没有实际显示值，如血量，这里依然拿时间举栗，

血量也可以这么搜索，依然ci sw初始化，回游戏让时间减少，再输入cn -

(意为值减少，还有

cn + 值增加，

cn eq 值未变化，

cn ne 值已变化，

cnf 和初始化时的值比较，如和初始化值的值相比未变化就这么写 cnf eq)

多重复几次时间减少和cn -就能得出唯一的值

若是血量或是其它不论怎样搜索都有几个地址可用排除法，

以血量举例，依次在内存浏览区域里输入地址把值都改0，

然后给敌方打一下，若直接狗带那就是正确的地址

------------------------------------------------------------------------------------------------------------

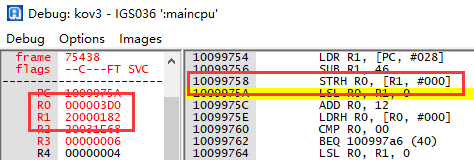
09 如何通过断点修改寄存器的值：

断点前面了解过了，但作弊码或是作弊菜单项无法直接修改寄存器的值，

除非是找到改写寄存器的地址或值加以操作，

这一段提供一种以断点方式修改寄存器值的方法，常用于调试

依然以三国战纪3的时间举例，先wp 20000182,1,w找改写时间的指令地址，



看得到是把R0的值3D0赋给(R1+0)也就是时间地址，

关闭wp断点，然后输入bp 10099758,r0=3E7,g

(在修改时间值的指令10099758处下断点，

r0=3E7即把值十六进制的999赋值给r0寄存器，g代表不中断继续运行，

也就是说只要这个断点还在，每次运行到这句指令的时候都会把3E7赋值给时间地址，并且不会中断)

------------------------------------------------------------------------------------------------------------

10 如何自定义条件断点：

有时候下断点会遇到很多次连续中断，按F5按得手累那种，如kof2002角色血量，当

对玩家血量下访问断点时，会持续的中断，包括几种已知的情况，是否被击中以判断角色应该做什么动作blahblah，但若是只想要检测角色血量是否少到可以施放隐藏超必杀的指令，

这时候就可以自定义条件，让其在达成定义的条件时才会中断，

如1P血量地址为12345，下访问断点 wp 12345,1,r后会持续中断，但可以观察到左侧的不同寄存器里的值很明显是不一样的，但相同的指令对应的寄存器其值又始终不变，

68k的游戏我比较喜欢用a6以区分

**①** 若只有一条指令持续访问，那就好办，

记录下a6的值，假设a6的值等于80ffa0，wpc清除所有监视断点，

然后再次输入 wp 12345,1,r,a6!=80ffa0 ，这时就不会持续中断了，就可以尝试施放隐藏超必杀以获取判断血量能否方隐藏超必杀的地址

**②** 若有好几个不同的地址轮流访问，分别记录其a6的值，wpc清除所有监视断点，

然后再次输入 wp 12345,1,r,a6!=80ffa0&&a6!=........ ，其关键就是a6与a6之间的&&，

若学过编程应该知道这是要同时达成条件才能触发语句

若a6寄存器里的值也有重复，那就用别的寄存器以区分

另一种自定义条件断点，依然拿改写时间断点举栗，

在改写时间指令下了断点后会发现只要时间减少就会断点一次，

但如果想让其在时间刚好到500的时候中断该如何实现？

依然 bp 10099758,r0==1F4

(1F4即16进制的500，此处意为当r0也就是时间剩余500秒的时候中断，

==为条件运算符，意为等于，不同于赋值的=，

这里可用的条件运算符还有

!=不等于

<=小于等于

>=大于等于 等)

改写寄存器和g也能用在wp断点上

------------------------------------------------------------------------------------------------------------

补充：

1  当光标在在调试器输入框里时按↑↓方向键可以浏览之前的输入历史

2 当断点在某条汇编指令地址时，可以输入 寄存器名=值 来改变当前命令对应寄存器的值，如 R0=1，这样做可以让之后单步执行的相关指令R0寄存器的值继承当前R0的值，

方便某些时候调试

3 所谓hack rom即修改rom的静态地址里的内容，ips亦是这样的原理，

也就是说hack rom亦可以通过作弊码实现，实现自由开关，相当于自由加载ips