

基于 MFC 的游戏修改器的设计与实现

谈沛良 白俊鸽

成都锦城学院计算机与软件学院 四川 成都 611731

【摘要】相信我们每个人平时都玩过小游戏，大多数小游戏是有得分的。所以我们想要得高分的话，可以通过修改游戏配置来达到我们的目的。笔者认为，对游戏的修改未尝不可，比如可以缩短无聊的练功时间，或者克服凶悍的 BOSS，有的时候，通过修改还可以发现一些隐藏的道具或情节，为玩游戏增添了几分新的乐趣。^[1] 本文主要介绍了游戏修改器的设计思想、界面布局、功能实现，以及如何使用 MFC 环境来开发一个游戏修改器。

【关键词】MFC；算法；游戏修改器

1 引言

如今，市面上有很多各种各样的小游戏。大多数以积分为通过条件或者进行排名的游戏都不容易得分。很多小游戏会因为得分不够而不能解锁或者进行下一关。本文主要介绍了游戏修改器的设计思想，以及如何使用 MFC 环境来开发一个游戏修改器。游戏修改，一个为很多玩家所不屑却为另一部分玩家所热衷的行为，在电脑游戏发展的漫长历程中，它扮演了举足轻重的角色。^[2]

2 设计思想

首先打开小程序，游戏运行后，点击刷新按钮，进入读取操作。玩家在进程列表装置找到所打开的游戏，然后选中它，点击打开按钮。点击打开按钮后，若打开成功，则会弹出“打开进程成功”，反之则未打开失败。接着开始玩游戏，得到一个初始分数，在输入框中输入这个分数，点击查找按钮，地址列表中就会显示出对应的地址。之后再一次玩游戏，得到另外一个分数。再次在输入框中输入这个新得到的分数，点击累计查找按钮。这个时候地址列表中就会出现一个唯一的地址，而这个地址就是最终的修改得分的地址。最后在下一个输入框中填上你想要修改的分数，点击修改按钮就完成了（见图 1）。

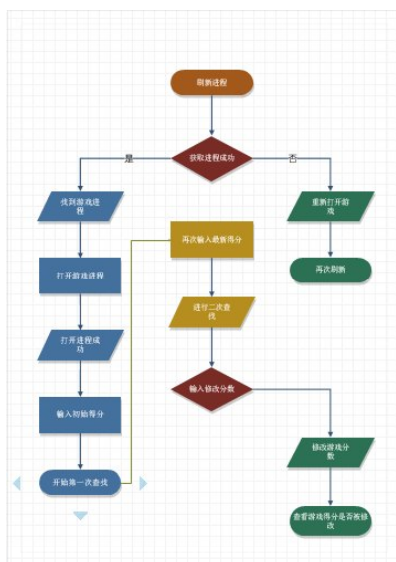


图 1 游戏修改器设计流程图

3 主要功能描述

本游戏修改器主要分为五个模块，也就是五个核心按钮。分别是刷新、打开、查找、累计查找和修改。此游戏修改器目的是为了通过修改游戏配置，对游戏的得分进行修改。所以首先找到一款适合的游戏，刷新得到游戏的进程号和进程名称，打开游戏进程，对其配置进行修改操作。先玩一会游戏，得到一个初始得分，然后在游戏修改器中的输入这个分数进行第一次查找，得到与此相关的地址。因为与这个相关的地址肯定不止一个，所以我们还需要累计查找一下，直到出现只有一个目标地址为止。再玩一会儿游戏后，得到另一个分数，接着在刚才的输入框中把初始分数改成现在的分数，点击累计查找进行再次查找。当地址列表中出现唯一地址时就说明查找成功，此地址就是我们要修改的得分地址。最终在输入框中输入你想要修改的分数，游戏中的得分就变成了你修改的分数。

4 界面设计

本游戏修改器主要有五个核心按钮，三个贴上标签控件，三个编辑控件，两个列表框控件和一个工艺条控制控件。五个按钮分别是刷新按钮、打开按钮、查找按钮、累计查找按钮和修改按钮。刷新按钮用来获取电脑上所有已打开的进程。要先打开游戏程序，再点击刷新按钮，否则第一次的进程列表中是没有该游戏进程的。打开按钮就是打开你要打开的目的进程。查找按钮是用来查找原始分数的，累计查按钮找是用来找寻最新得分的，修改按钮就是修改分数的。三个贴上标签控件分别用来区分一下两个列表框控件和一个编辑控件，工艺条控制控件是进度条，显示刷新的进度的。布局排版可以根据自己的喜好进行任意分布（见图 2）。

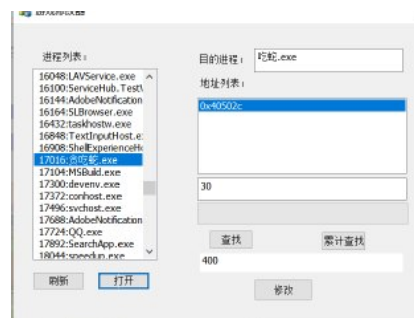


图 2 游戏修改器界面效果图

5 功能实现

5.1 刷新按钮

获取进程是整个修改器的第一步,也是最为关键的一步。先从后台调取所有的正在运行的进程并显示出来,这里用到了读取内存,使用的是阅读处理器内存语句。点击刷新按钮可以进行更新进程,起到实时同步的效果。得到进程就必须使用一个C++中特有的函数。记得每次添加特定函数时要加入头文件。先设计一个列表框控件,添加一个变量,再以字符串的方式显示在列表框控件中。我们要获取进程名称和id号,将它写入一个while循环,以便得到所有正在运行的进程。前面加一个贴上标签控件,取名为进程列表,然后再定义一个刷新按钮。

5.2 打开按钮

打开进程就相对简单一些,找出你要打开的进程名称,对其进行if判断,设计一个弹窗,查看是否打开进程。如果打开成功就弹出“打开进程成功”,没有的话就弹出“打开进程失败”。设计一个编辑控件,再在前面加一个贴上标签控件,取名为目标进程。给编辑控件加一个变量,用设置窗口文本语句使点击打开按钮后,将打开成功的进程的进程号显示在它上面。最后设置一个打开按钮。

5.3 查找按钮

查找按钮是对游戏的得分进行查找,找寻与分数相关的所有地址。所以只需要在整个游戏进程中找出得分地址即可,然后初始化在地址列表中显示出来。设计一个列表框控件,添加一个变量,前面加一个贴上标签控件取名为地址列表,定义一个字符串,然后设计一个按钮,也就是这个查找按钮,调用查询第一轮函数,初始化后将结果显示在地址列表中。查询第一轮会用调用到两个函数,一个是第一轮查询函数,另一个是每一页比较函数。具体来说是查找按钮调用第一轮查询函数,第一轮查询函数中调用每一页比较函数。在第一轮查询函数中先设置用户程序区页的总数,然后再来一个for循环,一页一页地比较,这里就调用每一页比较函数了。每一页比较函数中会读取内存,用到阅读处理器内存语句,将数据读取下来。

5.4 累计查找按钮

累计查找实现的功能是精确地找出哪一个才是我们真正需要的地址,查找按钮进行的是第一轮查找,已经帮我们找出了所有与分数有关地址,所以我们再更新一下分数,对其进行二次查找就能知道到底哪一个才是得分的地址。累计查找和查找按钮的逻辑是相似的,也是通过遍历。设计一个累计查找按钮,调用二轮查找的函数,将满足条件的地址显示出来,最终会出现一个唯一地址,这个地址就是我们要找的。累计查找的逻辑和查找按钮的逻辑是相似的,也是通过遍历得到结果。这里用到的是第二轮查询函数和显示地址函数。第二轮查询函数里面也是使用了阅读处理器内存语句读取了内存。显示地址函数中使用了特殊输出语句进行格式化输出。和第一次查找不同就是累计查找通过数据更新,一遍一遍地查询,最终确定了我们想要的地址。

5.5 修改按钮

首先设计一个编辑控件,用来输入我们需要改的分

数,在这个控件上添加一个变量。然后再添加一个按钮,取名为修改按钮。我们要对游戏配置进行修改,会用到改写程序的内存,使用写入内存的语句,然后,我们添加一个if判断语句,看是否修改内存成功,如果成功就弹出“修改成功”,反之则弹出“修改失败”。

6 功能测试及后期改进

项目完成后,对游戏修改器的主要功能进行了测试。在点击刷新按钮后打开贪吃蛇小游戏进行测试时,发现有时会出现两个贪吃蛇进程,这是因为打开进程后没有及时关闭,导致点击第二次刷新时还保留了上一次的结果。所以,在刷新按钮功能最后面要记得添加上关闭进程函数关闭每一次的进程。还有就是有时进程列表显示出来是乱码,是因为没有把CString转换成DWORD类型。经过测试和修改,游戏的主要功能均能正常运行。

后期对游戏修改器进行改进,准备加入一些新功能适应更多类型的小游戏。现在市面上不断出现更多更新的游戏,玩法新奇别致,玩家的要求也越来越多,只是修改得分并不能满足玩家的需要。所以,我们要紧跟时代的步伐,对游戏修改器加入更多的功能,注入更多的活力。比如对于没有得分的闯关游戏增加跳过关卡的功能,修改角色外貌特征等等。将游戏修改器做到多样化,功能更加强大一点,不止是单机游戏,还可以修改一些联网的游戏。

7 结束语

本文介绍了如何使用MFC环境开发一个游戏修改器,所设计的游戏修改器实现了获取进程,打开进程,显示进程,修改进程等功能。实现了从获取游戏的内存到打开和修改的操作,适合所有得分的小游戏。如今的修改器通常分为内存修改器和存档修改器两种。^[3]游戏修改器属于前者,是内存修改器,还存在着许多的不足之处。例如,游戏修改器的界面不够美观,排列不太整齐规范。该游戏修改器目前只能修改一些小游戏的分数,对于其它地方还不能修改。这些都是下一步游戏修改器需要改进的地方。总体来说,该游戏修改器的逻辑清晰简单,容易上手,功能较为完善,适合初学者学习使用。

【参考文献】

- [1] maxZ. 学会使用游戏修改工具[J]. 软件, 2001(09): 19-20.
- [2] 冯烈. 成为超人并不难——闯关乎? 修改乎?[J]. 电子计算机与外部设备, 2001(01): 182-183.
- [3] 小狼. 开外挂 玩大作[J]. 电脑迷, 2009(22): 14-15.