中科院计算所
INSTITUTE OF COMPUTING TECHNOLOGY

龙芯QEMU模拟器的使用介绍

卢天越

2019.9.2

目录

- 什么是QEMU
- 需要的工具
- 使用方法

目录

- 什么是QEMU
- 需要的工具
- 使用方法

什么是QEMU

- QEMU模拟器：通过软件的方法模拟一个硬件平台
  - 硬件寄存器->软件变量，硬件运算->软件运算
  - 将同学们写的操作系统运行在模拟器上，与运行在开发板上功能基本相同
- 优点：
  - 1、硬件平台的输出有限，使用软件模拟加快调试速度
    - 可以接入GDB：单步调试，查看系统状态
  - 2、硬件平台无法修改，通过在软件模拟器上修改的方式来做研究

学习使用模拟器

- 磨刀不误砍柴工
  - 学习使用QEMU和GDB会花一点时间，但是会大大降低解决代码bug的难度
- 对未来的研究工作有很大帮助
  - 1、使用模拟器是计算机体系结构研究中的常用工具
    - 现有硬件平台无法直接修改，硬件流片太贵，FPGA调试起来也比软件代码要复杂许多
  - 2、学习使用gdb：Linux环境下的调试利器

目录

- 什么是QEMU
- 需要的工具
- 使用方法

需要的工具

- 提供的工具：
  - 1、QEMU模拟器
    - 龙芯的QEMU模拟器不开源，但网上有其他架构的开源QEMU
  - 2、和开发板上相同功能的PMON
    - bios文件夹下的文件
- 需要安装的工具
  - gdb-multiarch：

```
apt-get install gdb-multiarch
```

目录

- 什么是QEMU
- 需要的工具
- 使用方法

使用方法

- 制作USB镜像盘
  - 由于QEMU模拟器的限制，这里制作USB盘镜像来代替开发板的SD卡
  - 制作一个较大的空USB盘镜像（这里为512MB）

```
dd if=/dev/zero of=disk bs=512 count=1M
```

  - 将操作系统代码制作成USB镜像
    - 制作方法与P1中介绍的制作镜像的方法类似

```
./createimage --extended bootblock kernel
```

```
dd if=image of=disk conv=notrunc
```

使用方法

- 启动QEMU模拟器
  - 使用提供的启动脚本：run_pmon.sh
  - 给QEMU程序执行权限 `chmod +x qemu/bin/qemu-system-mipsel`
  - 检查脚本中是否正确调用了提供的PMON
    - 启动脚本中的参数包含：-kernel ./bios/gzram
  - 检查脚本中是否正确调用了USB盘镜像文件
    - 启动脚本中的参数包含：-usb -drive file=disk,id=a,if=none
  - 运行启动脚本，进入PMON界面

```
sh run_pmon.sh
```

使用方法

- 连接gdb工具
  - 安装gdb工具

```
apt-get install gdb-multiarch
```

  - 在启动脚本中设置gdb连接端口
    - 启动脚本中包含 -gdb tcp::50010
  - 启动gdb，设置mips架构，连接该端口

```
gdb-multiarch
```

```
set arch mips
```

```
target remote localhost:50010
```

  - 载入符号表（编译代码时加上-g选项）

```
symbol-file kernel
```

使用方法

- gdb工具调试技巧
- 在gdb界面中可以使用以下命令：
  - 设置断点：b，例：b *0xa0800000
  - 继续运行：c
  - 单步运行：si
  - 查看寄存器内容：i r
  - 查看内存：x，命令格式：x/nfu [addr]
    - n是内存单元个数，f是显示格式，u是内存单元大小
  - 显示指定地址之后的10条汇编指令：x/10i addr
  - 显示指定地址之后的10条数据单元：x/10x addr
  - 退出：q

总结

- 使用QEMU模拟器进行调试
  - 无需修改同学们自己写的操作系统代码
  - 可以通过gdb调试
  - 输出和开发板平台基本一样
- 在过程中
  - 熟悉模拟器的使用
  - 学习gdb工具的调试
  - 协助完成本课程的projects