编译qemu

一、安装所需要的一些包

`libglib2.0-dev`

`libpixman-1-dev`

`libfdt-dev`

安装的时候直接`sudo apt-get install package_name`就行

对于第三个包， 实验室的电脑上按上述的安装方式安装的版本比所需要的版本更低

解决办法是按照stackoverflow上的做法(`https://stackoverflow.com/questions/54838295/error-dtc-libfdt-version-1-4-2-not-present-please-install-the-dtc-libfdt`)，将网页链接上的包下载并解压，将文件放至`qemu-6.828-2.9.0/dtc/`

二、编译

1、`cd qemu-6.828-2.9.0` 首先进入qemu文件夹

2、`mkdir build` 新建一个文件夹来存放安装文件

3、a. 可选择编译所有系统（x86_64、i386、arm等）， 通过`./configure --prefix=build`，大概需要半小时时间即可完成，--prefix指定安装文件存放在哪，便于日后管理;

b. 由于本课程只涉及i386, 也可只编译i386，方法是

`./configure --target-list=i386-softmmu --enable-debug --enable-kvm --prefix=build`

注：a、b任选其一，但在实验室电脑上，无法编译所有系统，因此只能选择b方法

4、编译操作, 执行`make`

注：执行make在当前目录下能运行qemu，通过`qemu-system-i386`即可。但在其他目录下找不到，因此需要修改xv6的makefile,具体做法见下文。

运行xv6

1、`cd xv6/` 进入xv6文件夹

2、修改Makefile文件，找到下面这行

`If the makefile can't find QEMU, specify its path here`

`QEMU := qemu-system-i386`

修改路径便于查找，例如在我的电脑上，修改为

`QEMU := /home/yfliu/文档/oslab/qemu-6.828-2.9.0/i386-softmmu/qemu-system-i386/qemu-system-i386`

3、`make` 编译

4、运行xv6

`make qemu-nox` 运行， -nox表示不开启另一个窗口

先按ctrl+a后按x 退出