生成汇编文件

- xcrun --sdk iphoneos clang -S -arch arm64 main.c -o main.s

寄存器

- 通用寄存器
  - 64bit的：x0 ~ x28
  - 32bit的：w0 ~ w28（属于x0 ~ x28的低32bit）
  - x0 ~ x7通常拿来存放函数的参数，更多的参数使用堆栈来传递
  - x0通常拿来存放函数的返回值
- 程序计数器
  - pc（Program Counter）
  - 记录CPU当前指令的是哪一条指令
  - 存储着当前CPU正在执行的指令的地址
  - 类似于8086汇编的ip寄存器
- 堆栈指针
  - sp（Stack Pointer）
  - fp（Frame Pointer），也就是x29
- 链接寄存器
  - lr（Link Register），也就是x30
  - 存储着函数的返回地址
- 程序状态寄存器
  - cpsr（Current Program Status Register）
  - spsr（Saved Program Status Register），异常状态下使用

指令

- mov
- ret
  - 函数返回
  - 将**lr（x30）**寄存器的值赋值给**pc**寄存器
- add
- sub
- cmp
  - 将2个寄存器相减

    - 相减的结果会影响cpsr寄存器的标志位
- b
    - 跳转指令
    - 可以带条件跳转，一般跟cmp配合使用
- bl
    - 带返回的跳转指令
    - 执行的操作
        - 将下一条指令的地址存储到**lr（x30）**寄存器中
        - 跳转到标记处开始执行代码
- 条件域
    - EQ：equal，相等
    - NE：not equal，不相等
    - GT：great than，大于
    - GE：greate equal，大于等于
    - LT：less than，小于
    - LE：less equal，小于等于
- 内存操作
    - load，从内存中读取数据
        - ldr、ldur
        - ldp（p是pair的简称）
    - store，往内存中写入数据
        - str、stur
        - stp
        - 零寄存器，里面存储的值是0
            - wzr（32bit，Word Zero Register）
            - xzr（64bit）

iOS汇编

- 真机：arm64汇编
    - 寄存器
    - 指令
    - 堆栈
- 模拟器：x86汇编

函数的堆栈

- 函数的类型

- 叶子函数
- 非叶子函数