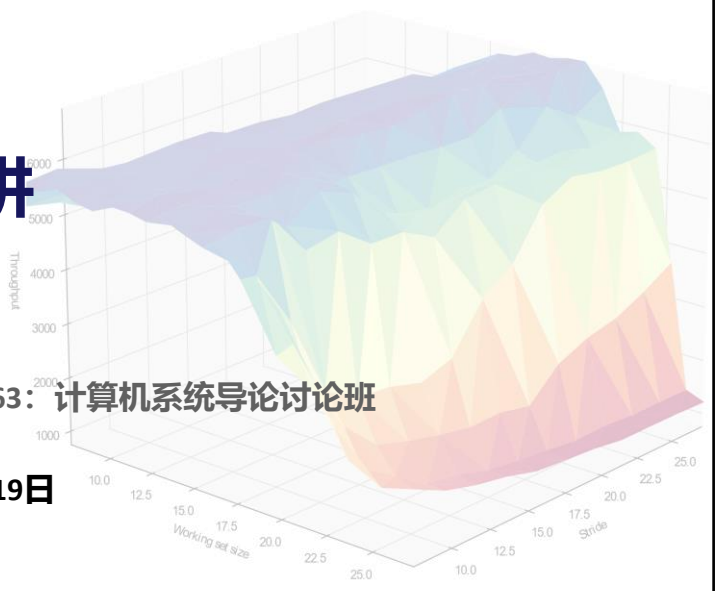
第三讲



PKU 04832363：计算机系统导论讨论班

王畅

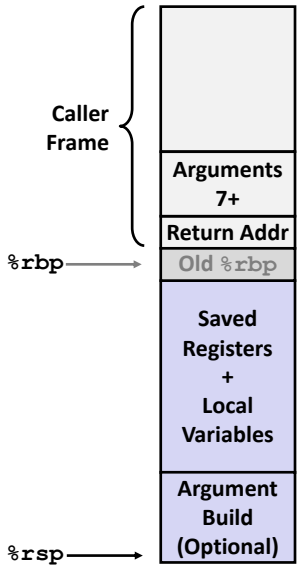
2021年10月19日

ABI

- a processor instruction set (with details like register file structure, stack organization, memory access types, ...)
- the sizes, layouts, and alignments of basic data types that the processor can directly access
- the calling convention, which controls how the arguments of functions are passed, and return values retrieved.
- how an application should make system calls to the operating system, and if the ABI specifies direct system calls rather than procedure calls to system call stubs, the system call numbers.
- and in the case of a complete operating system ABI, the binary format of object files, program libraries, and so on.

x86-64 Calling

- Push the current value of the frame pointer (`ebp/rbp`). This saves it so we can restore it later.
- Move the current stack pointer to the frame pointer. This defines the start of the frame.
- Subtract the space needed for the function's data from the stack pointer. This puts the stack pointer past the space that will be used by the function so that anything pushed onto the stack now will not overwrite useful values.

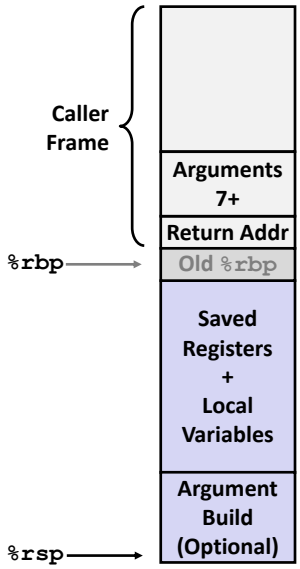


3

在IA32中，参数都用栈传递，所以rbp比较重要（用rbp+偏移访问参数）。要非常清楚整个调用过程以便做题。

x86-64 Calling

- Execute the code for the function. References to local variables will be negative offsets to the frame pointer (e.g., "`movl $123, -8(%rbp)`").
- On exit, copy the value from the frame pointer to the stack pointer (clearing up the space allocated to the stack) and pop the old frame pointer. This is accomplished by the "`leave`" instruction.
- Return from the procedure via a "`ret`" instruction. This pops the return value from the stack and transfers execution to that address.



4

注意一下指令`leave`的意思，虽然考试中不常见。

Activity 1

轮流回答问题

Question 1

- **下列描述更符合（早期）RISC还是CISC?**
  - 指令机器码长度固定。
  - 指令类型多、功能丰富。
  - 不采用条件码。
  - 实现同一功能，需要的汇编代码较多。
  - 译码电路复杂。
  - 访存模式多样。
  - 参数、返回地址都使用寄存器进行保存。
  - 广泛用于嵌入式系统。
  - 已知某个体系结构使用add R1, R2, R3来完成加法运算。当要将数据从寄存器S移动至寄存器D时，需要使用add S, #ZR, D进行操作（#ZR是一个恒为0的寄存器）。
  - 已知某个体系结构提供了xlat指令，它以一个固定的寄存器A为基地址，以另一个固定的寄存器B为偏移量，在A对应的数组中取出下标为B的项的内容，放回寄存器A中。

6

RISC，固定长的指令译码电路简单；通常CISC有变长指令，例如x86中清零用xor，因为这样可以节省指令长度。

CISC

RISC

RISC

CISC

CISC

RISC

RISC，嵌入式系统是指可穿戴设备、物联网之类的小设备，需要省电，因此处理器不能太复杂。

RISC，说明提供的基本操作很少。

CISC

Activity 2

问题求解

考点1：综合汇编阅读（难点！）

- 期中考试两大区分点之一
- 先通读题目再分析
- 掌握基本技巧，熟练：作对应、画栈帧、推断
- 注意字节序和对齐要求！！！
- 历年试题：section 5 练习26、27、28、29、30、31

any questions?

Thanks & 感谢观看