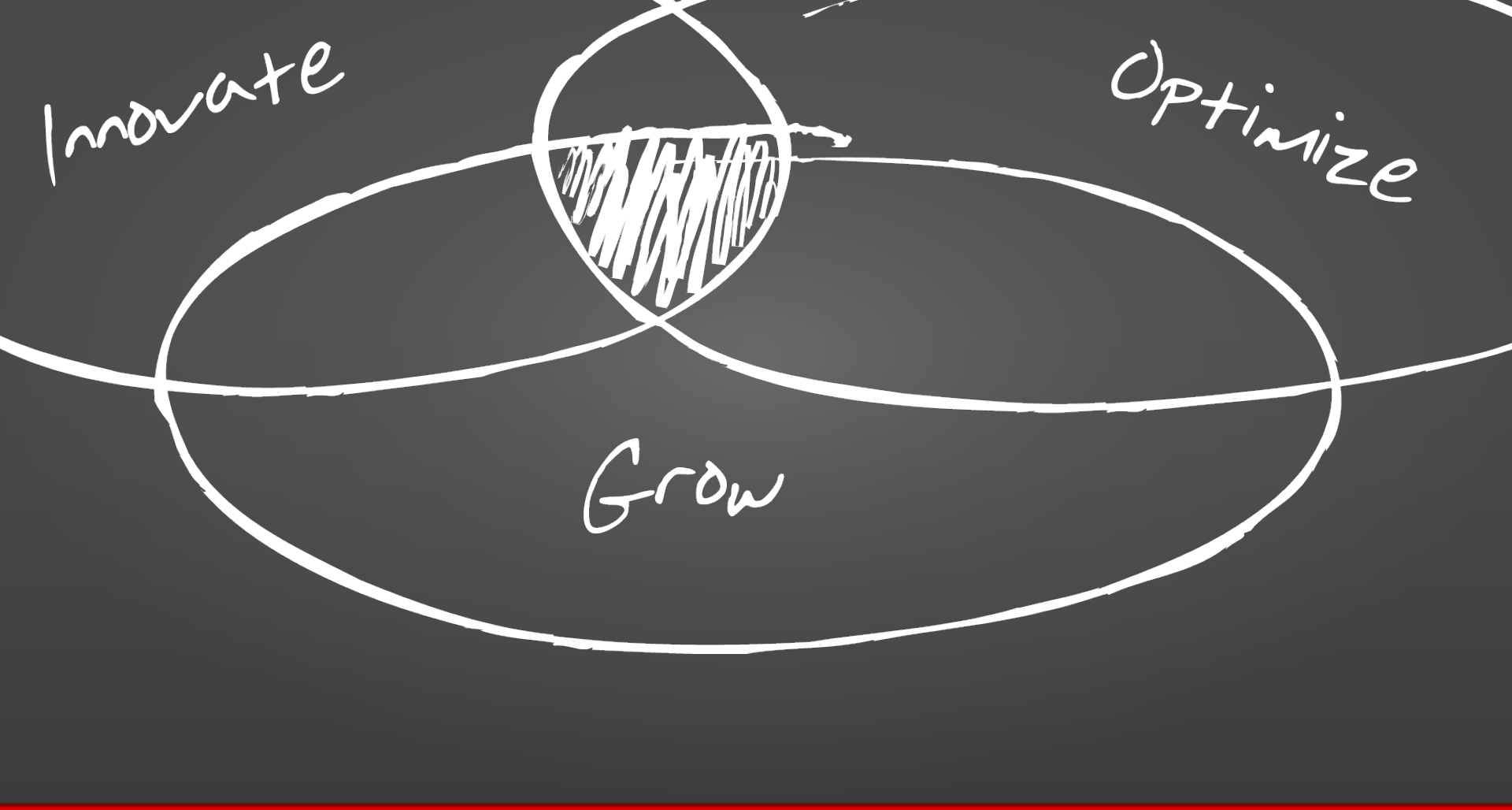
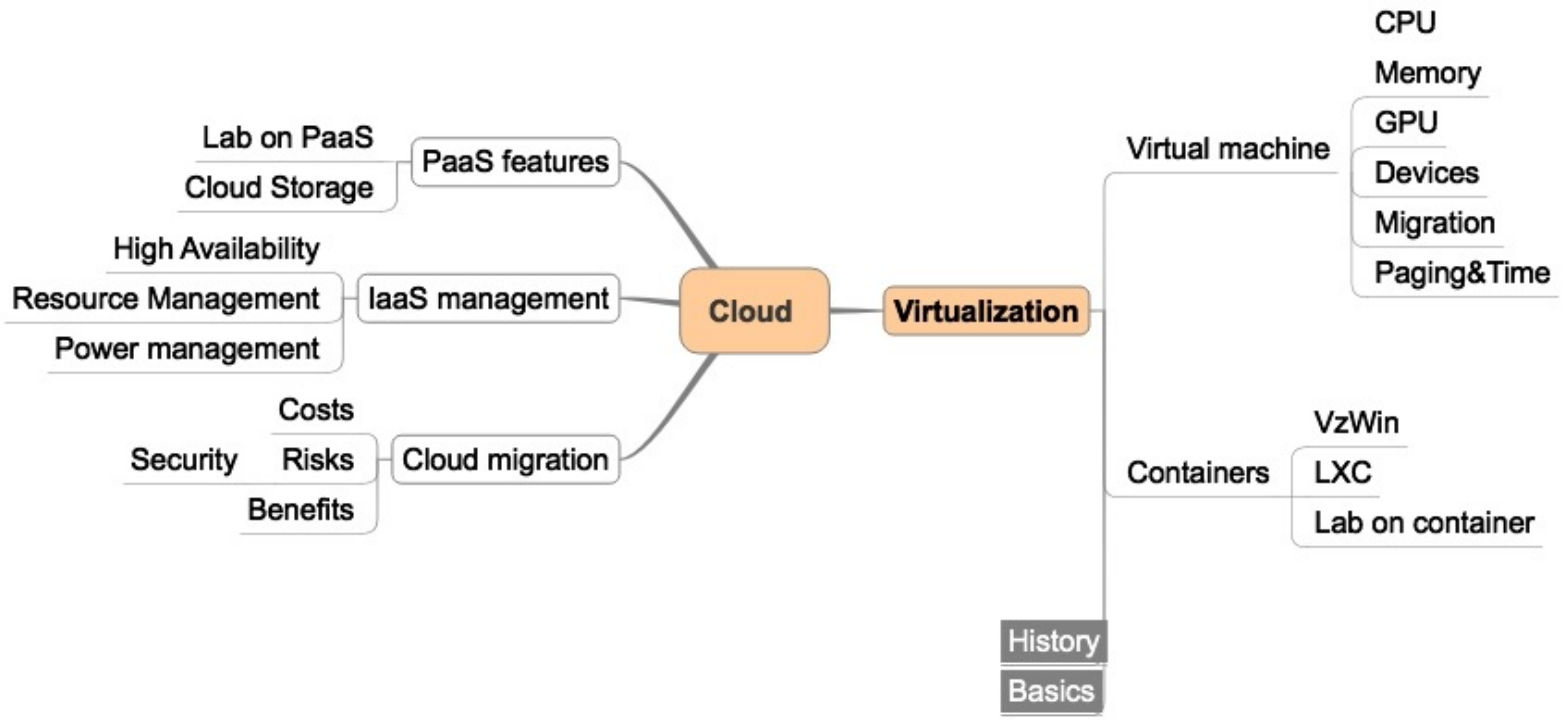


The total virtualization

Virtualization approaches

Lecture #3

Course overview

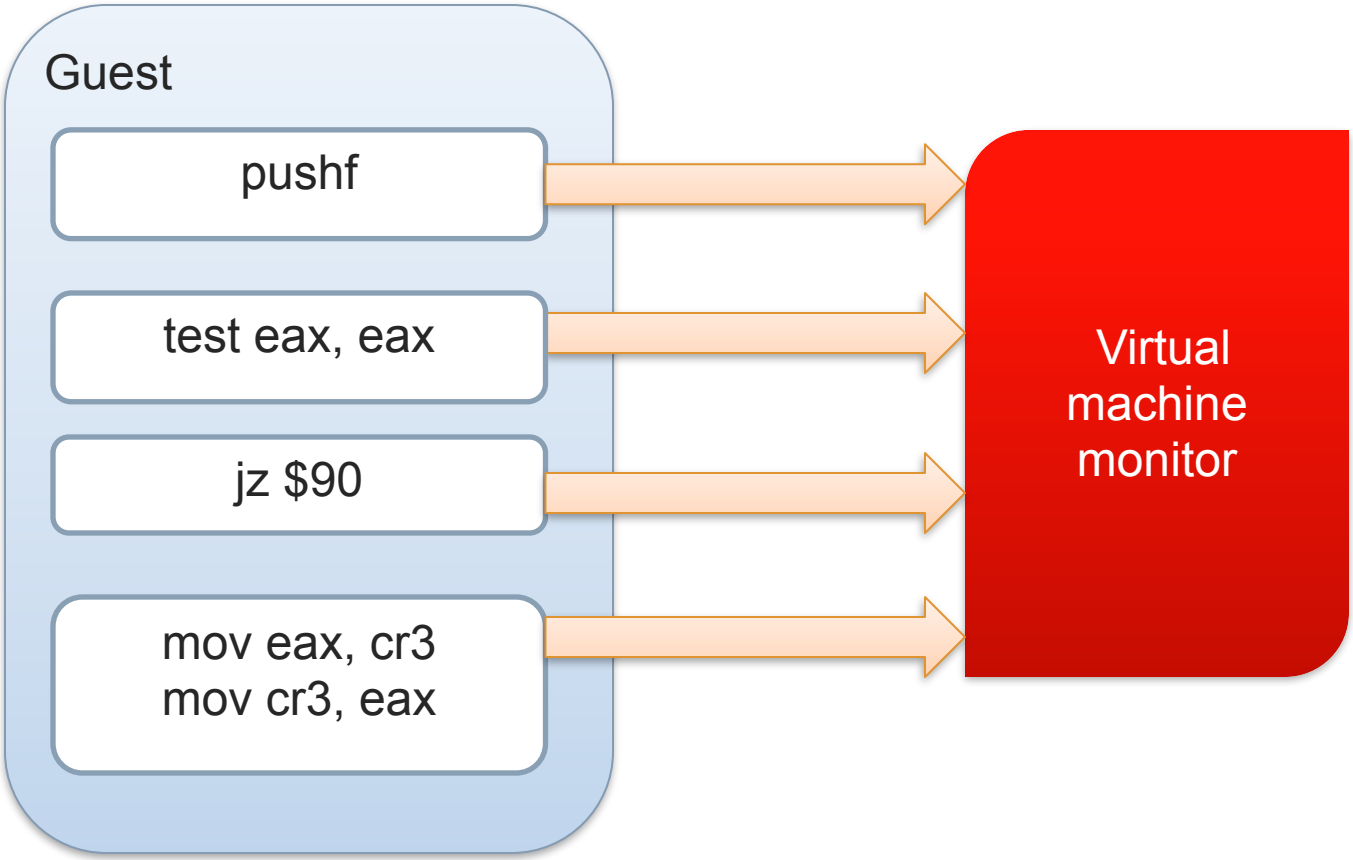


Content

- ✓ Emulation
- ✓ Binary translation
- ✓ Stubbing
- ✓ Paravirtualization
- ✓ Hardware-assisted

Virtualization is one of classic CS tasks. Understand its possible solutions to apply them in the future

Virtualization technologies: emulation



Virtualization technologies: emulation

PROS:

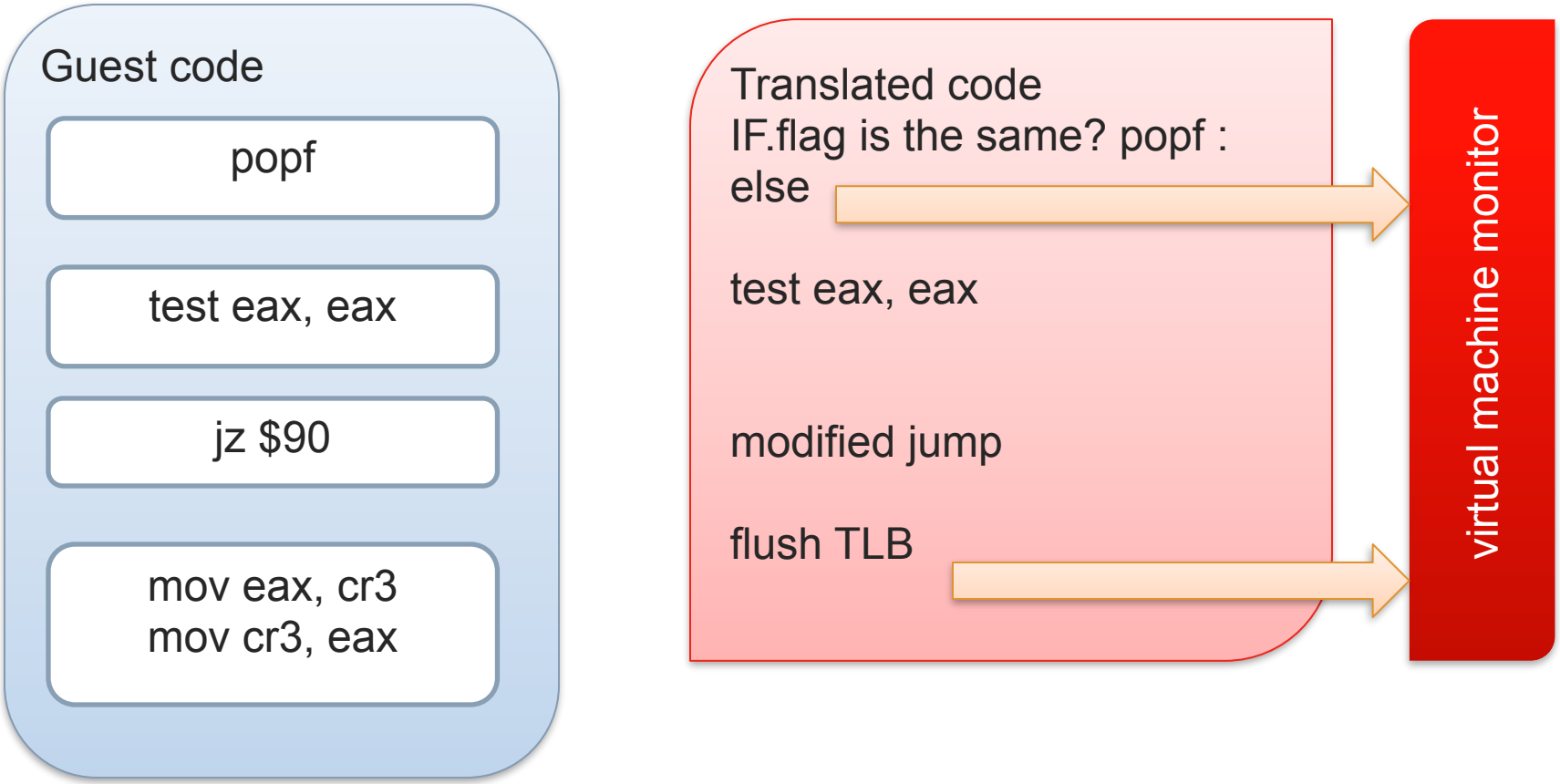
✓ Stability

✓ Universality

CONS:

✓ Low performance

Virtualization technologies: binary translation



Virtualization technologies: binary translation

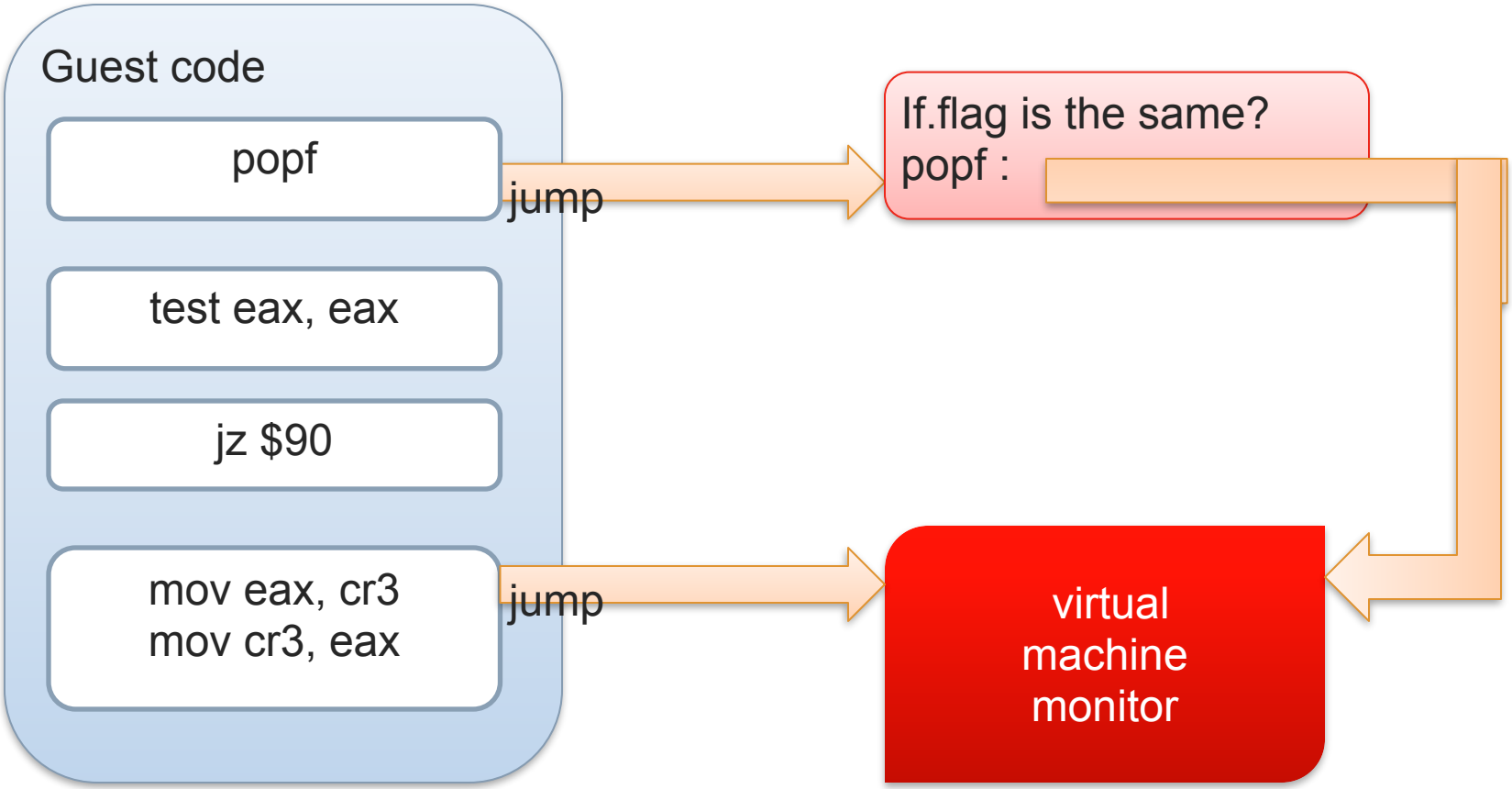
PROS:

- ✓ Performance
- ✓ Universality
- ✓ Optimizations of translated code

CONS:

- ✓ Overhead for translation
- ✓ Linear address complexity

Virtualization technologies: stubbing



Virtualization technologies: stubbing

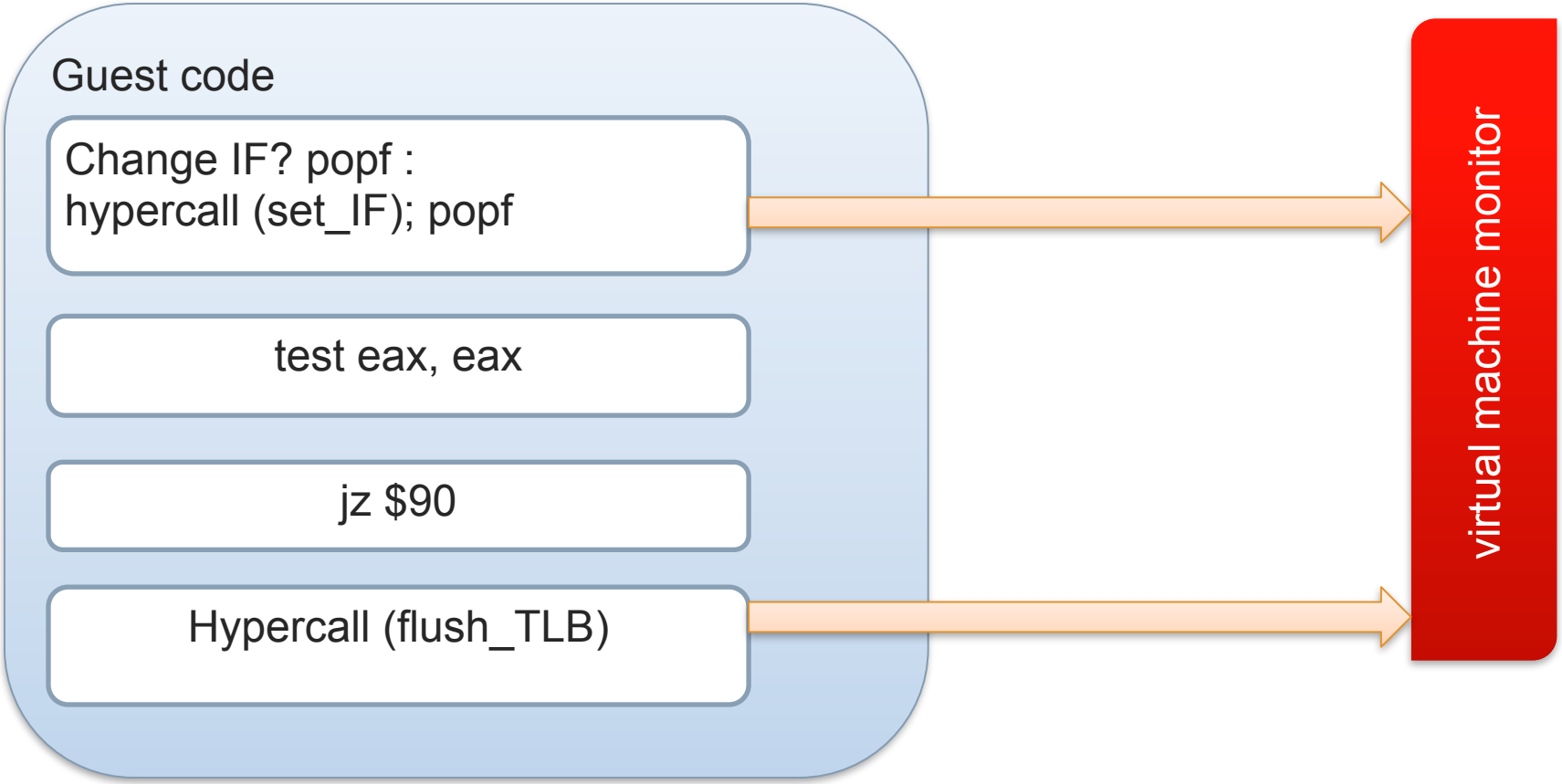
PROS:

- ✓ performance
- ✓ No complexity of linear address recalculation

CONS:

- ✓ Virtualize only the same platform
- ✓ Complex cases with instructions longer then jmp, pairing instructions, cross-page instructions

Virtualization technologies: paravirtualization



Virtualization technologies: paravirtualization

PROS:

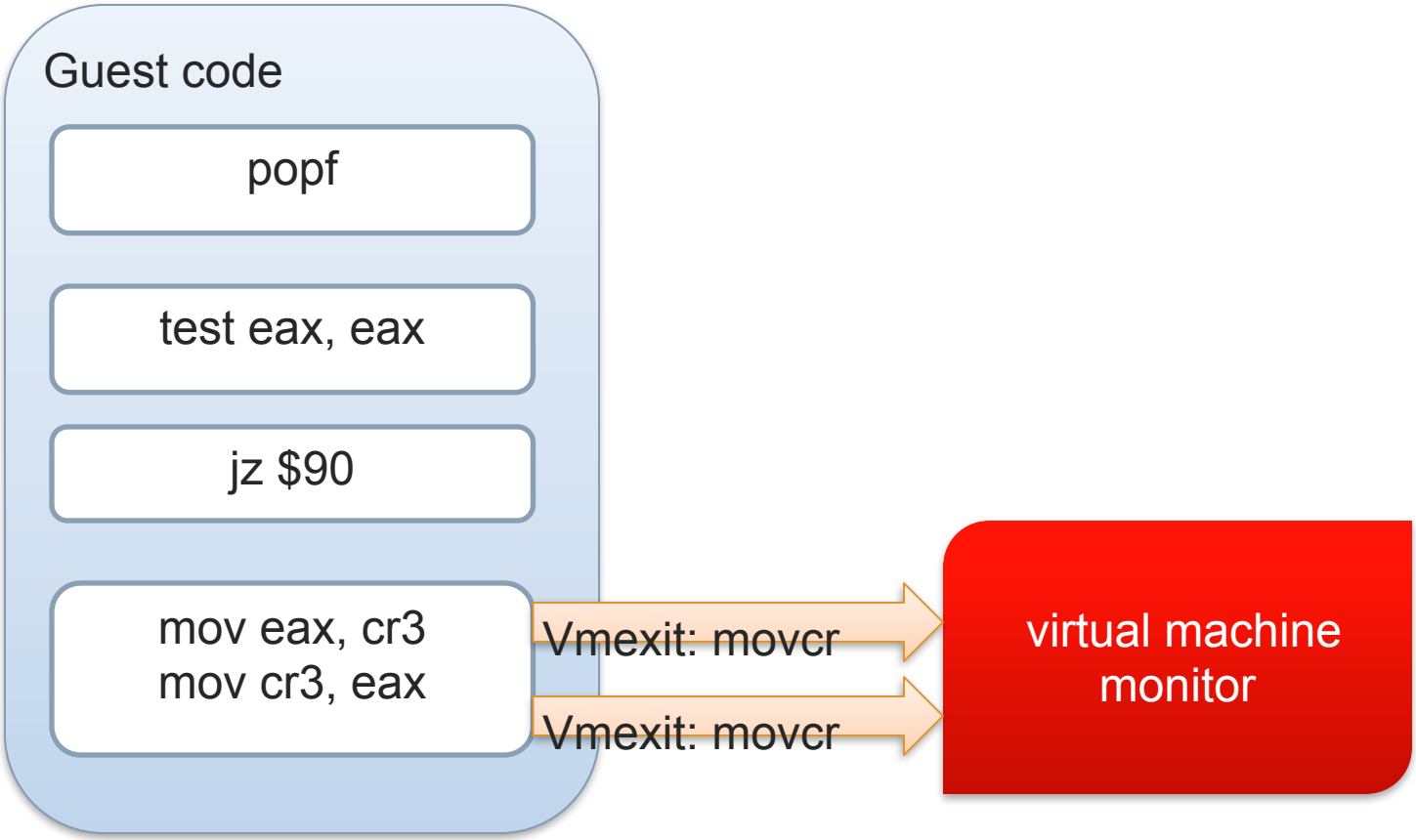
✓ near native performance

CONS:

✓ No standard for VMM API

✓ No easy solutions for system with proprietary source code

Virtualization technologies: hardware virtualization



Virtualization technologies: hardware assisted

PROS:

✓ Constantly improving performance

✓ Easy

CONS:

✓ Non-universality of the platform

✓ Unexpected performance problems

✓ Bugs in hardware

✓ Not all models supported

Hardware virtualization

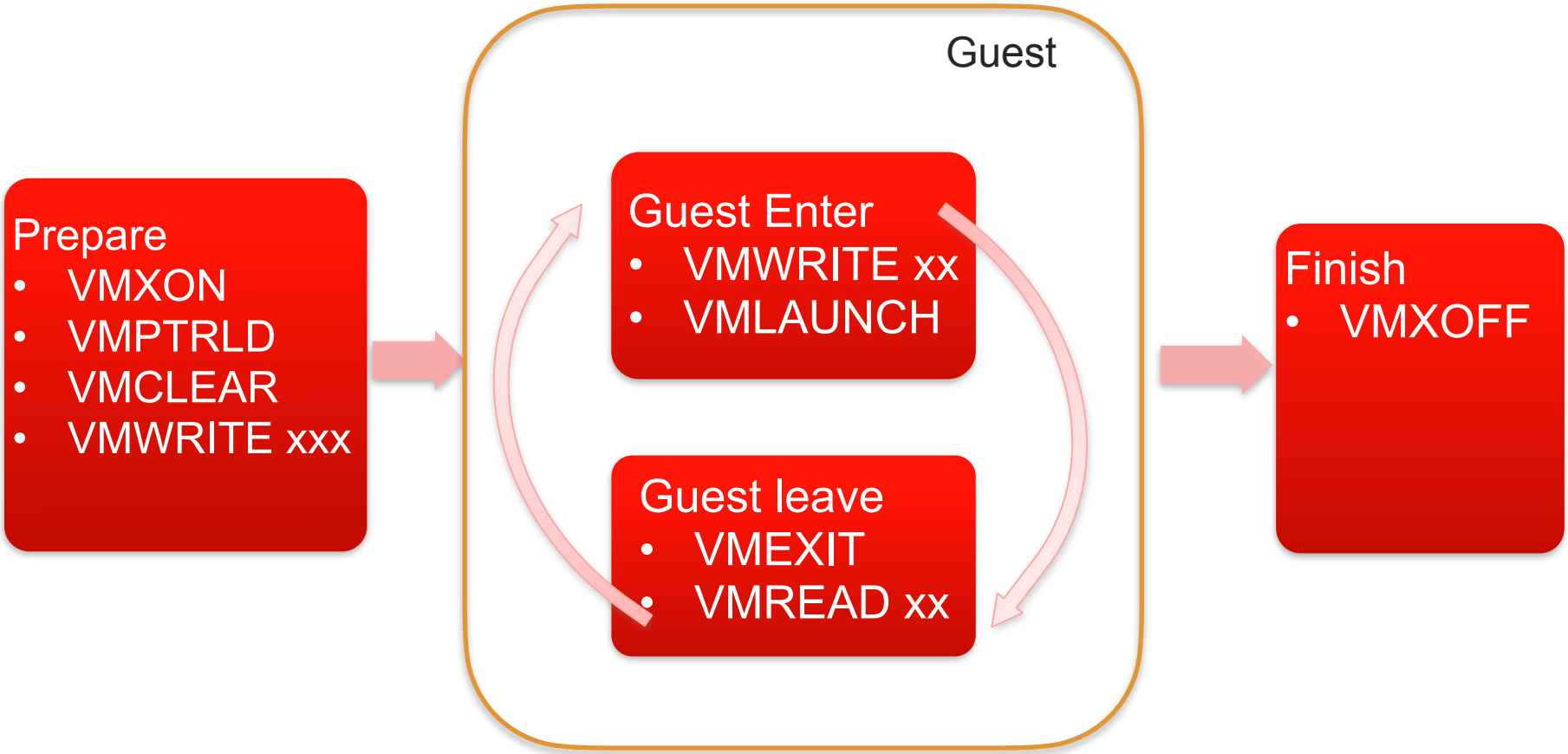
Hardware-virtualization x86

- Fix architecture to meet Popek-Goldberg requirements
- Make a machine context switchable + create a new privilege level

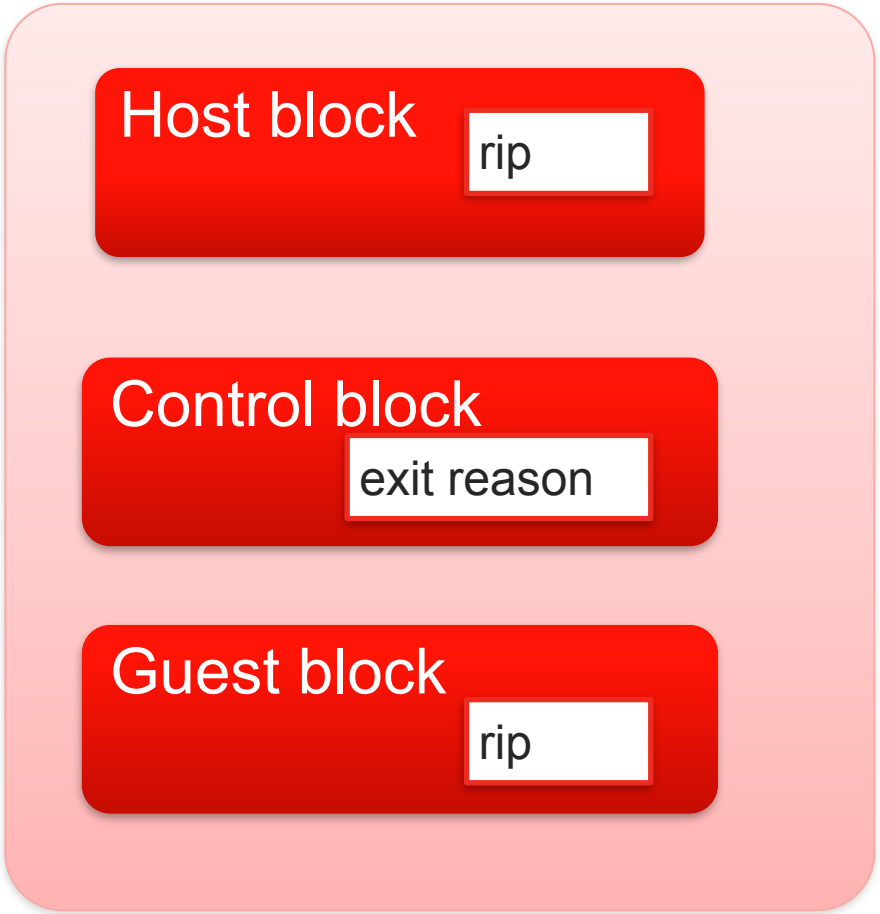
Hardware-virtualization

- ✓ VMM is executed as vmroot
- ✓ Guest ring0 == non-root ring0, guest ring3 == non-root ring3.
- ✓ CPU state is present in VMCS
  - ✓ CPU state.safe is available from non-root natively
  - ✓ CPU state.unsafe causes vmexits to vmroot mode

Hardware virtualisation



Hardware virtualization: VMCS



Conclusions

A few approaches to CPU virtualization: emulation, recompilation/translation, paravirtualization, hardware-assisted solutions

Questions?