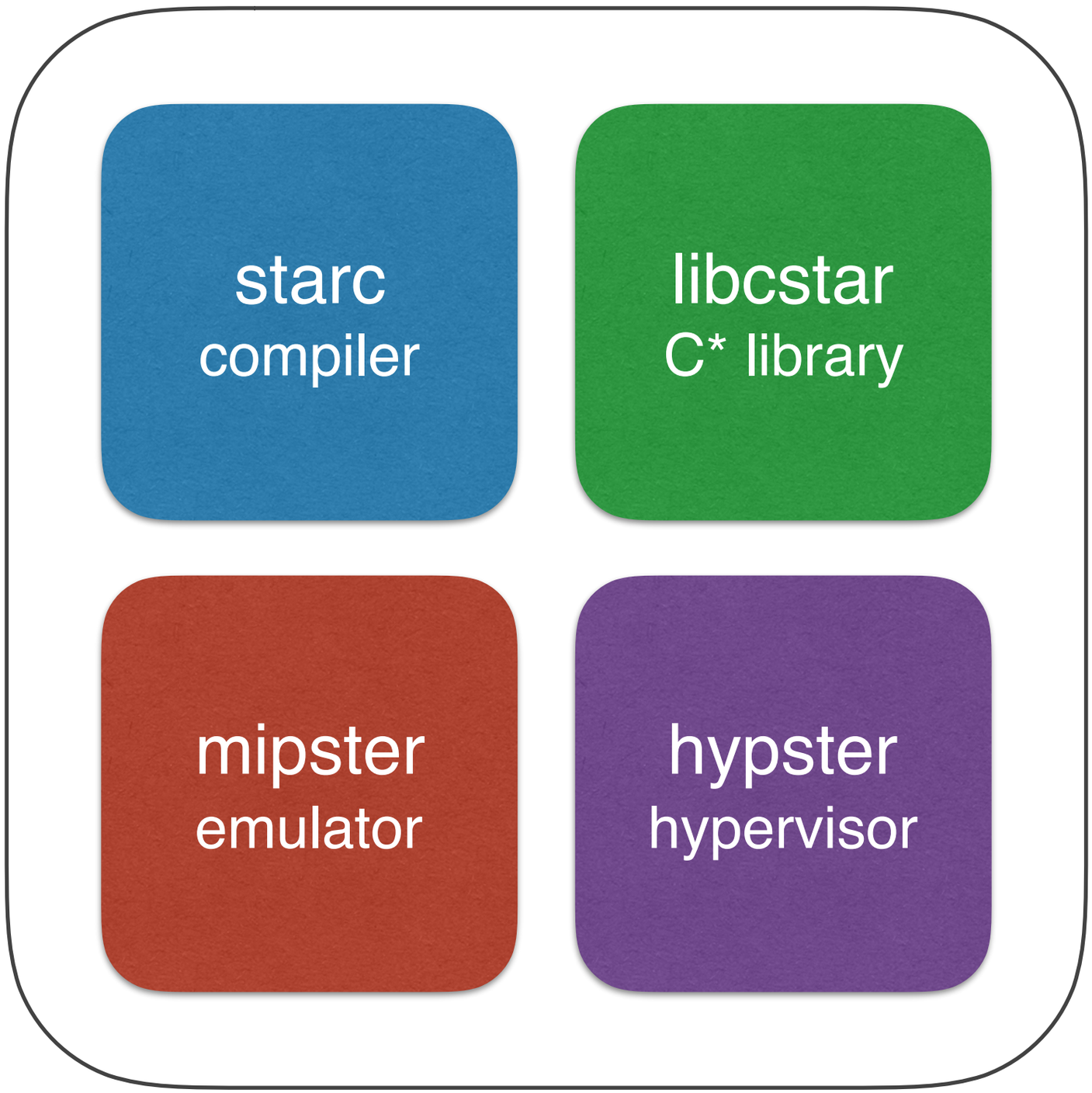
Mixter: Towards Simultaneous Emulation and Virtualization

Master's thesis by Thomas Hütter
Supervised by Univ.-Prof. Dr. Christoph Kirsch

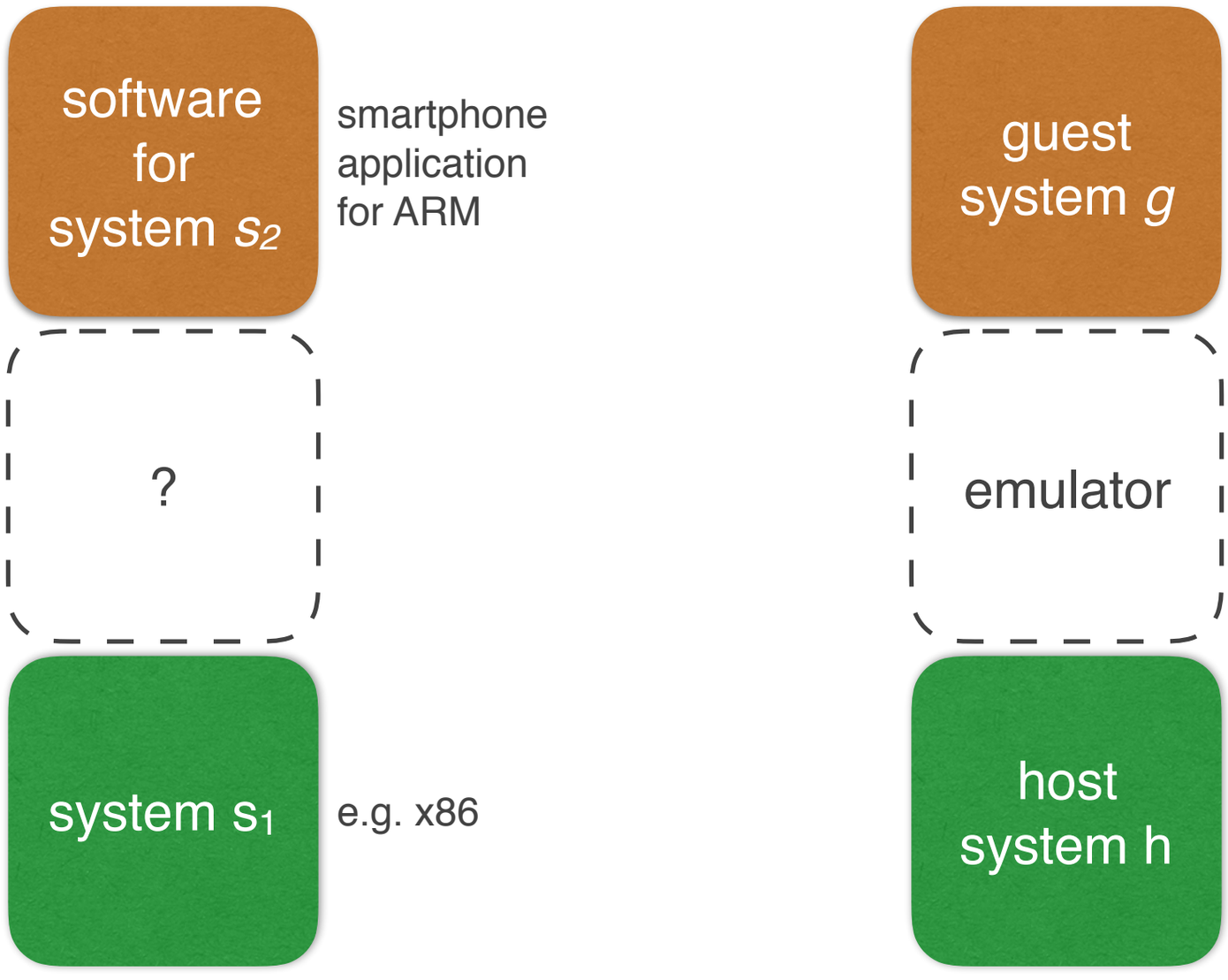
Department of Computer Sciences
Faculty of Natural Sciences
University of Salzburg

Selfie[1]

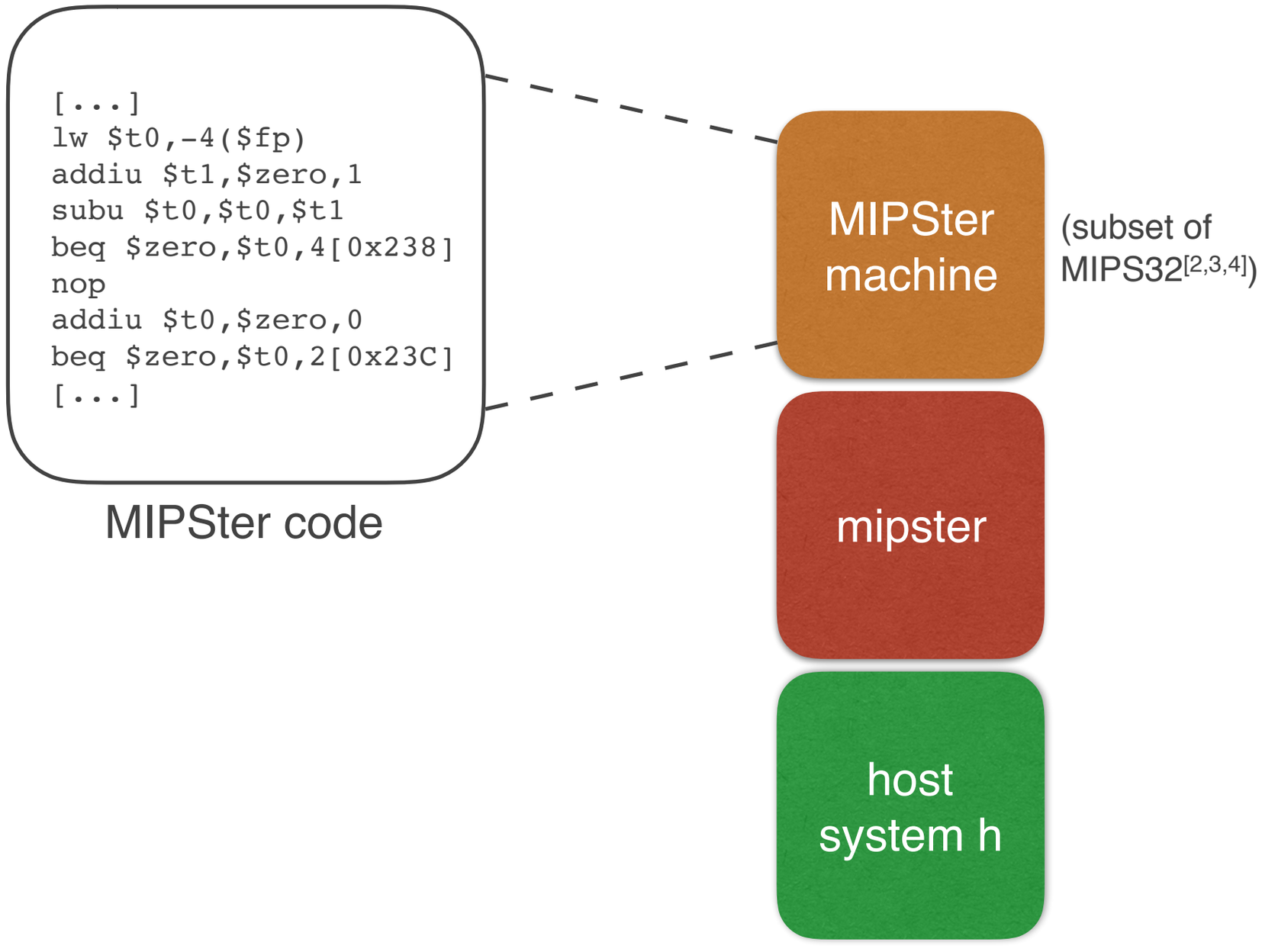


http://selfie.cs.uni-salzburg.at

Emulation

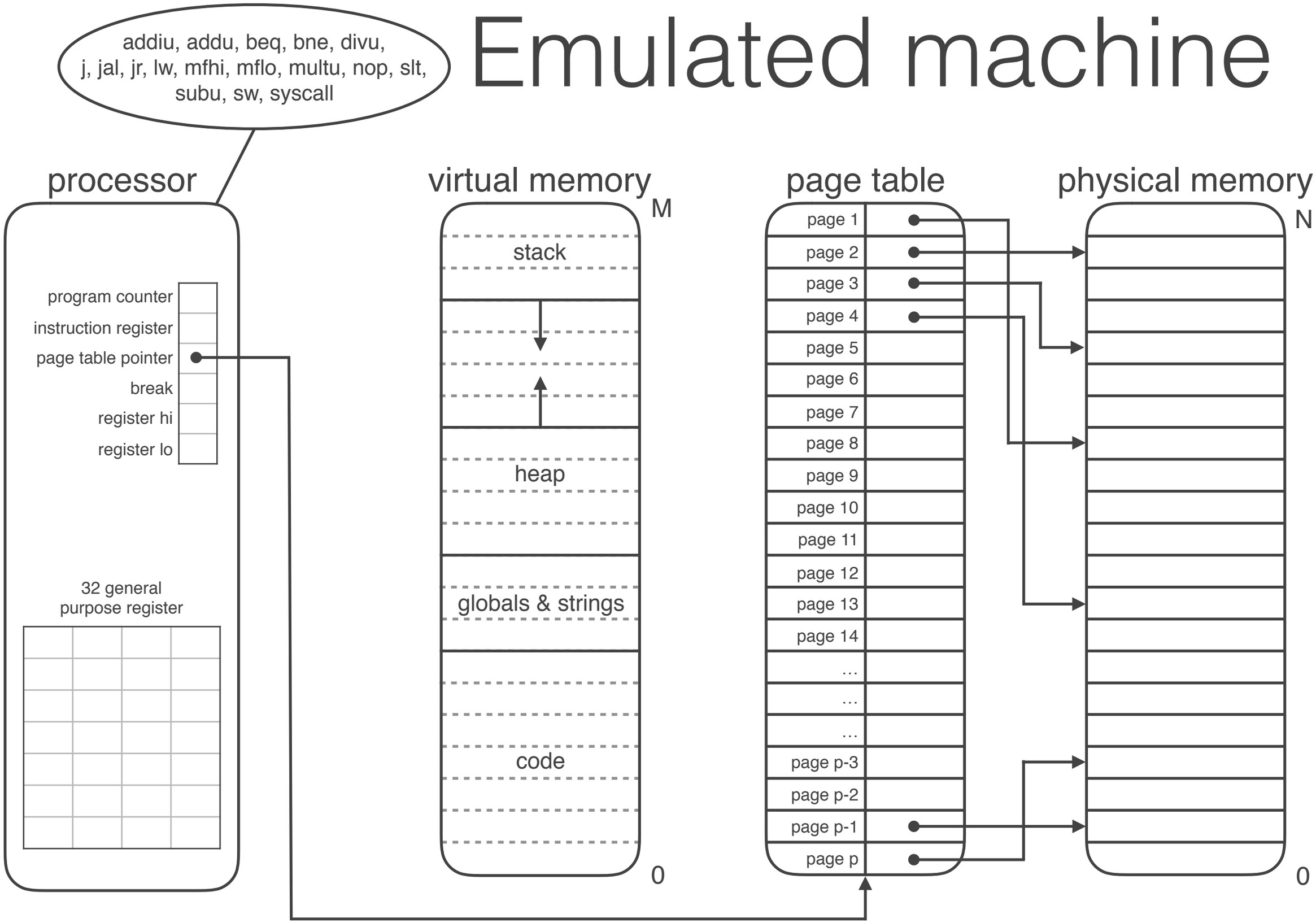

software for system s_2
smartphone application for ARM
guest system g
?
emulator
system s_1
e.g. x86
host system h

mipster


[...]
lw $t0,-4($fp)
addiu $t1,$zero,1
subu $t0,$t0,$t1
beq $zero,$t0,4[0x238]
nop
addiu $t0,$zero,0
beq $zero,$t0,2[0x23C]
[...]
MIPSter code
MIPSter machine
(subset of MIPS32[2,3,4])
mipster
host system h

Emulated machine

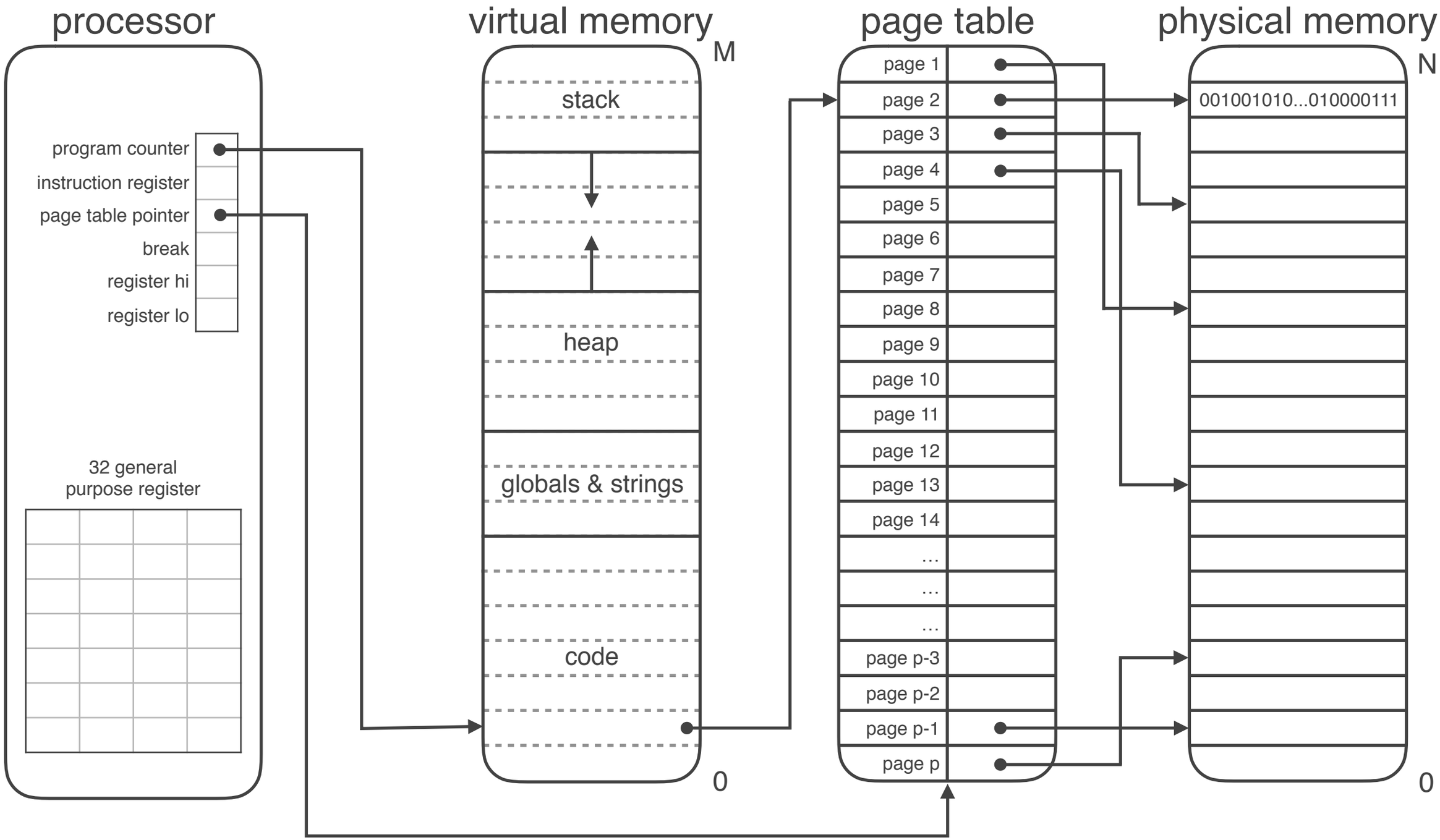
addiu, addu, beq, bne, divu,
j, jal, jr, lw, mfhi, mflo, multu, nop, slt,
subu, sw, syscall



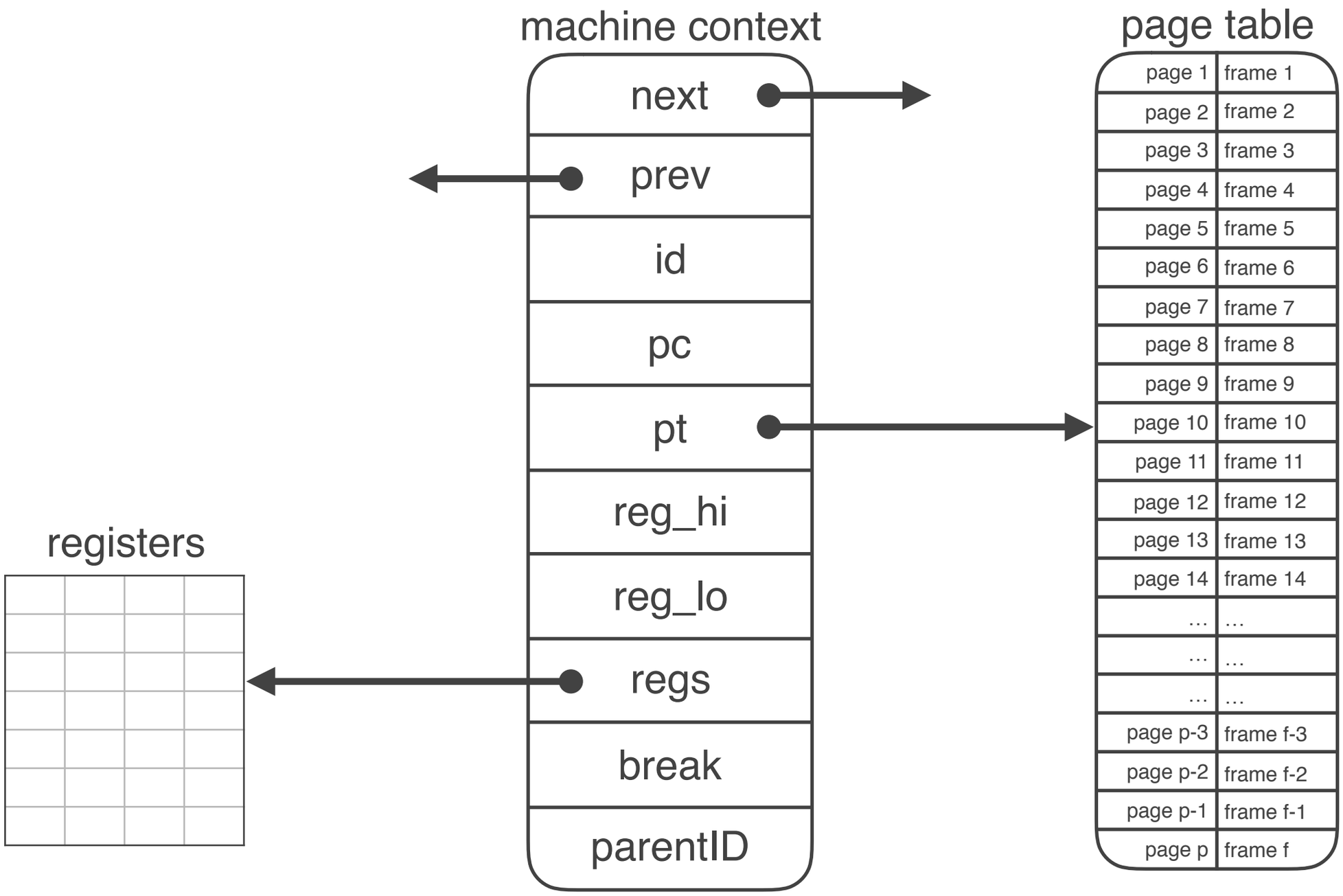
Code interpretation

- **Fetching**: Read an instruction from memory
- **Decoding**: Decode an instruction by a given format
- **Executing**: Perform an instruction

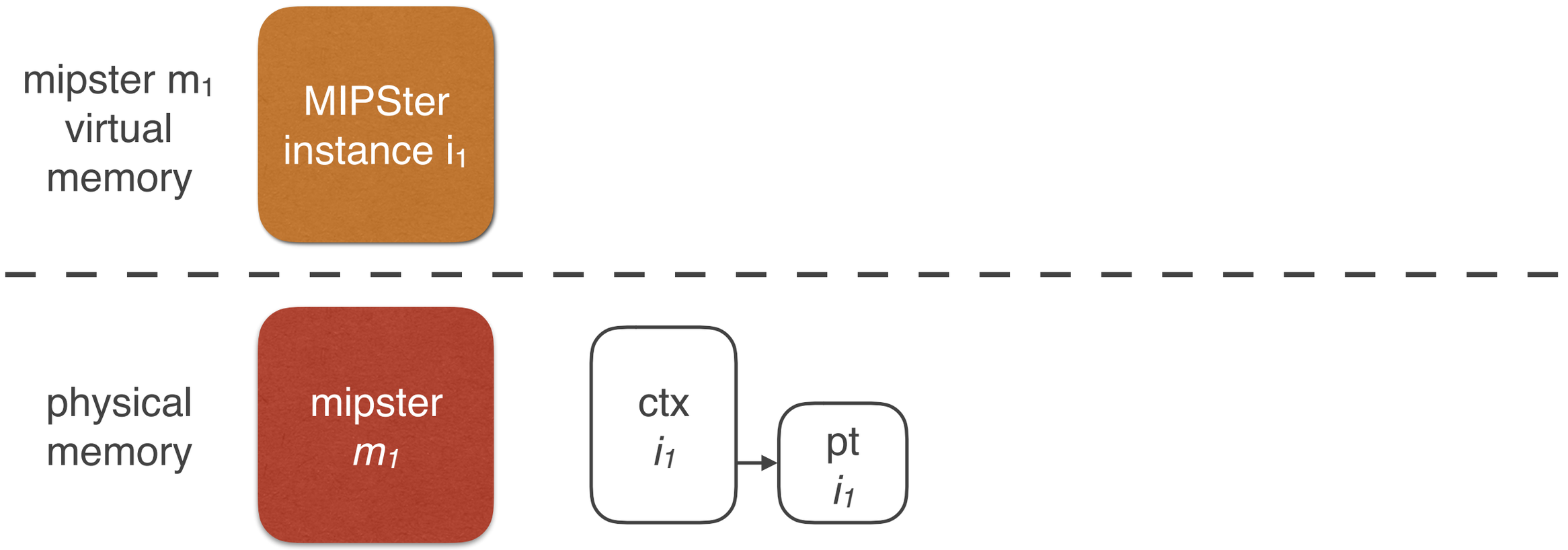
Fetching


processor
program counter
instruction register
page table pointer
break
register hi
register lo
32 general
purpose register
virtual memory
M
stack
heap
globals & strings
code
0
page table
page 1
page 2
page 3
page 4
page 5
page 6
page 7
page 8
page 9
page 10
page 11
page 12
page 13
page 14
…
…
…
page p-3
page p-2
page p-1
page p
physical memory
N
001001010...010000111
0

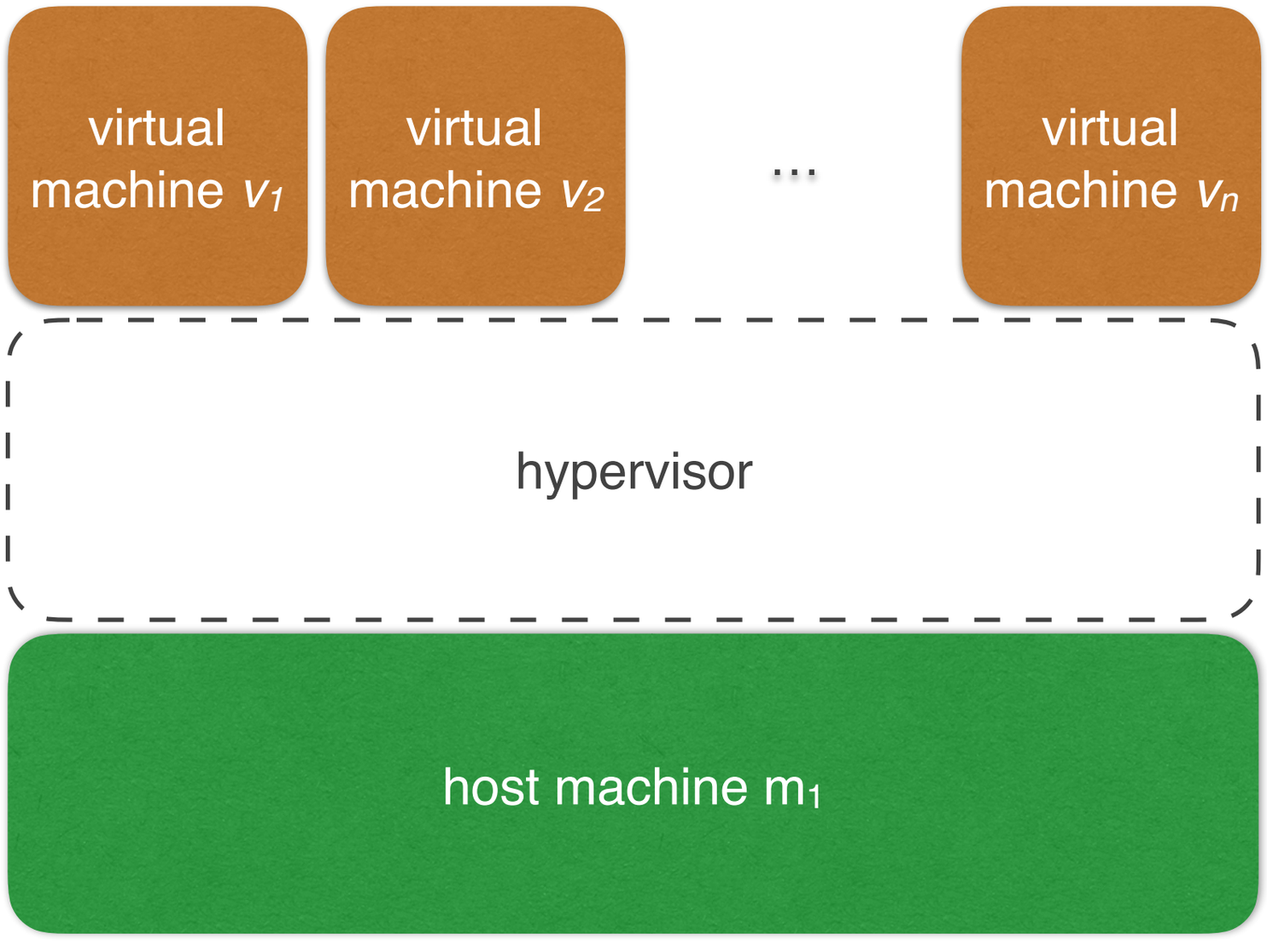
Machine context



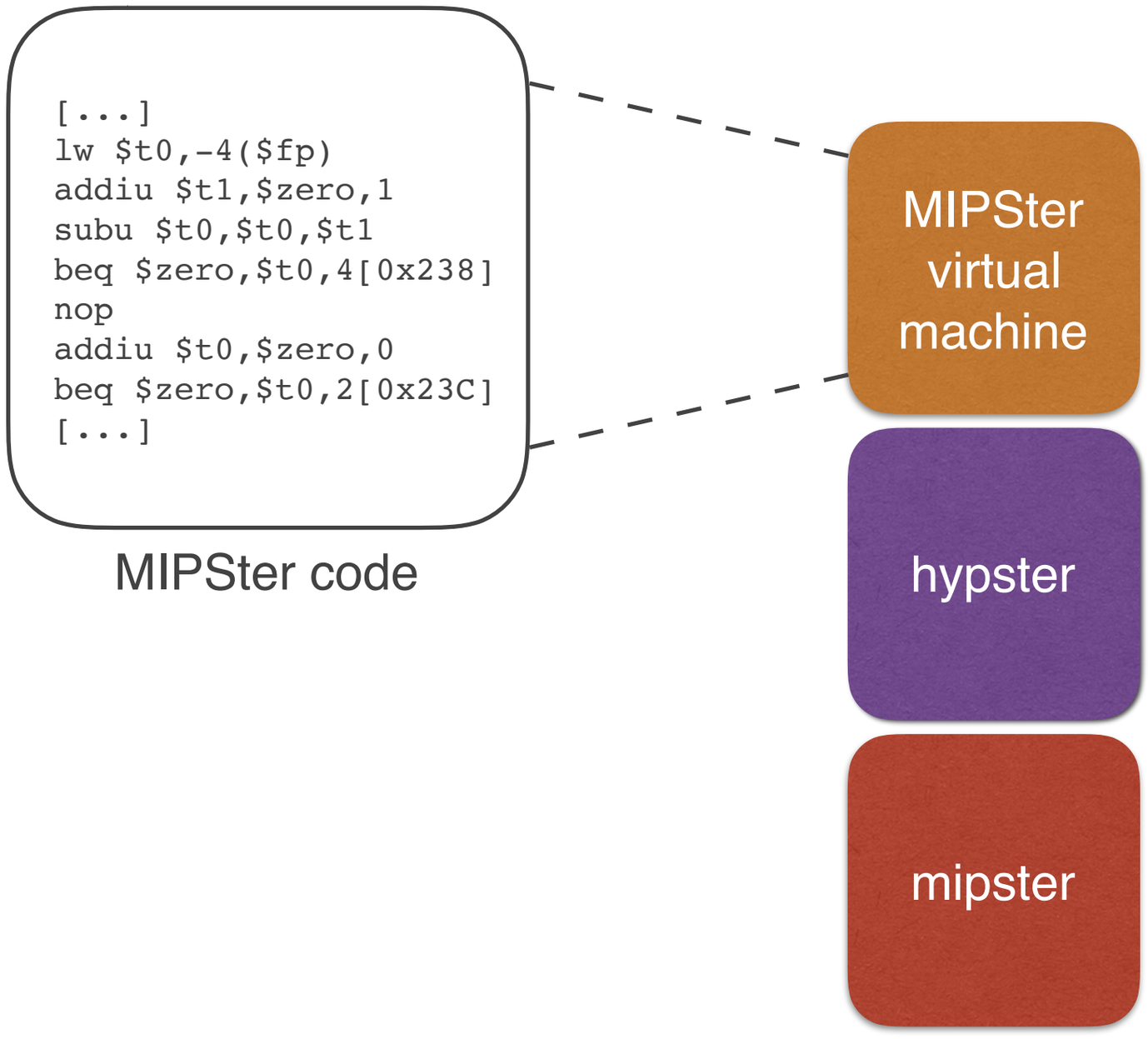
Address spaces and machine contexts



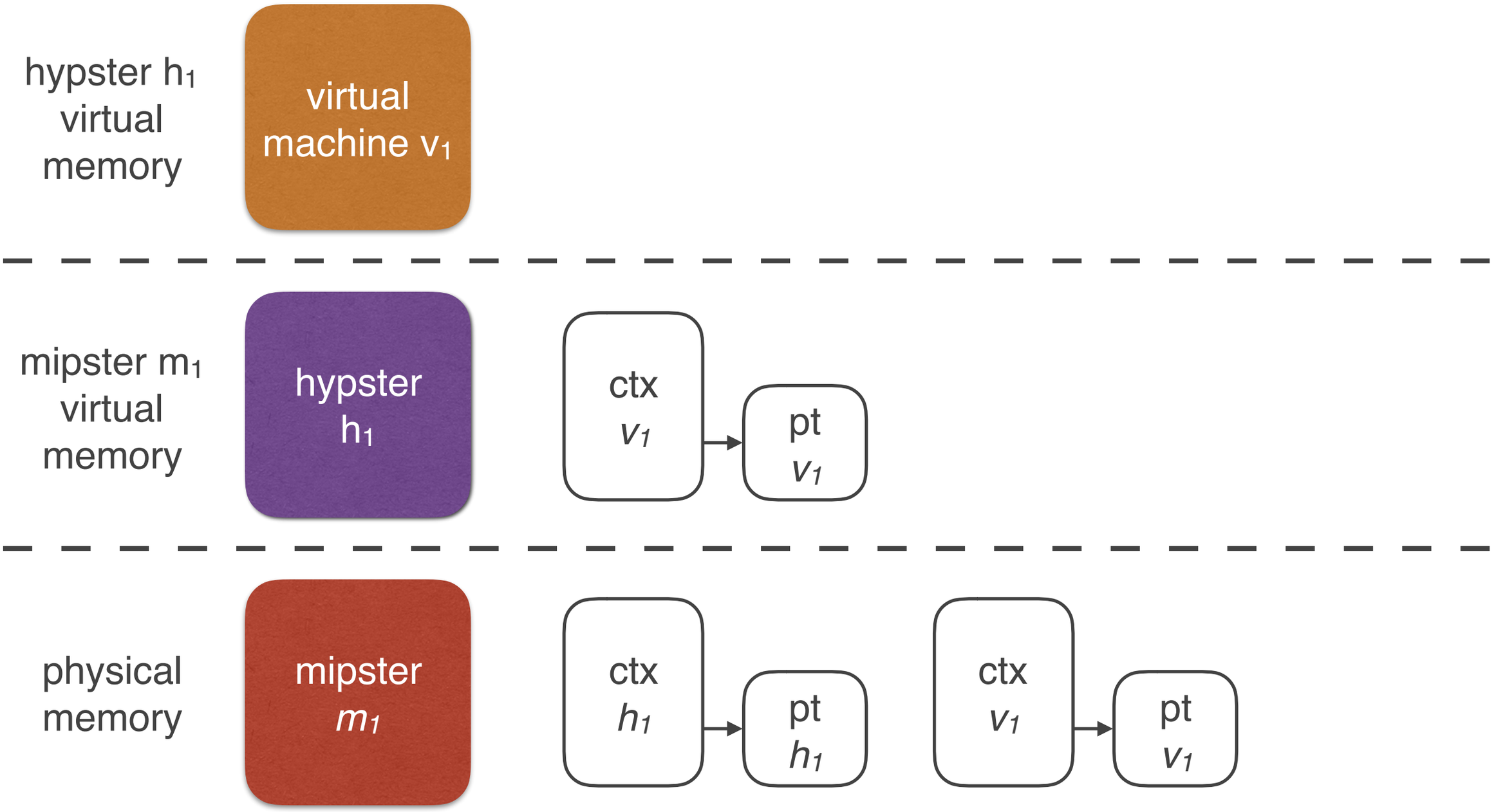
Virtualization



hypster


[...]
lw $t0,-4($fp)
addiu $t1,$zero,1
subu $t0,$t0,$t1
beq $zero,$t0,4[0x238]
nop
addiu $t0,$zero,0
beq $zero,$t0,2[0x23C]
[...]
MIPSter code
MIPSter virtual machine
hypster
mipster

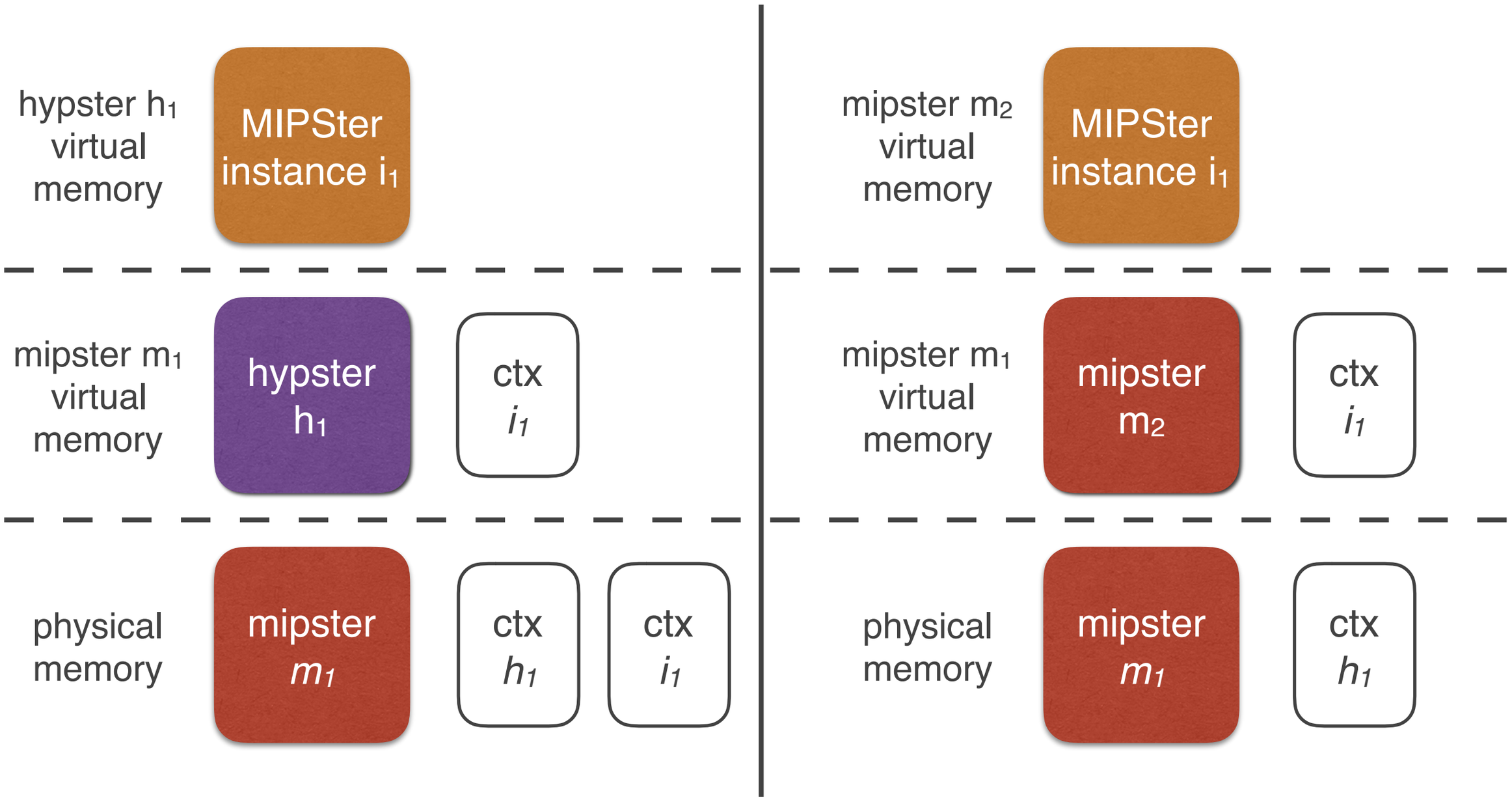
Address spaces and machine contexts



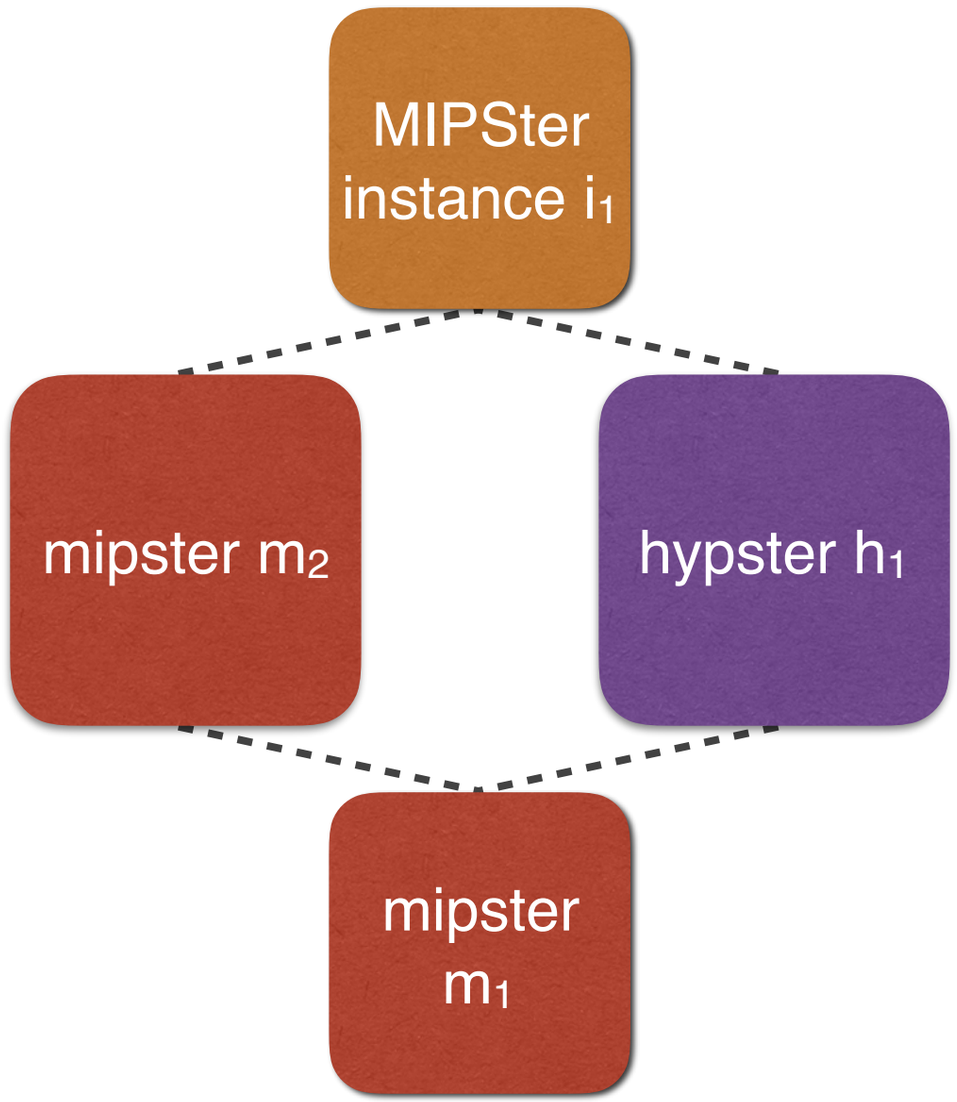
Problem

- Find methods to verify the functional equivalence of emulation and virtualization of the same hardware.

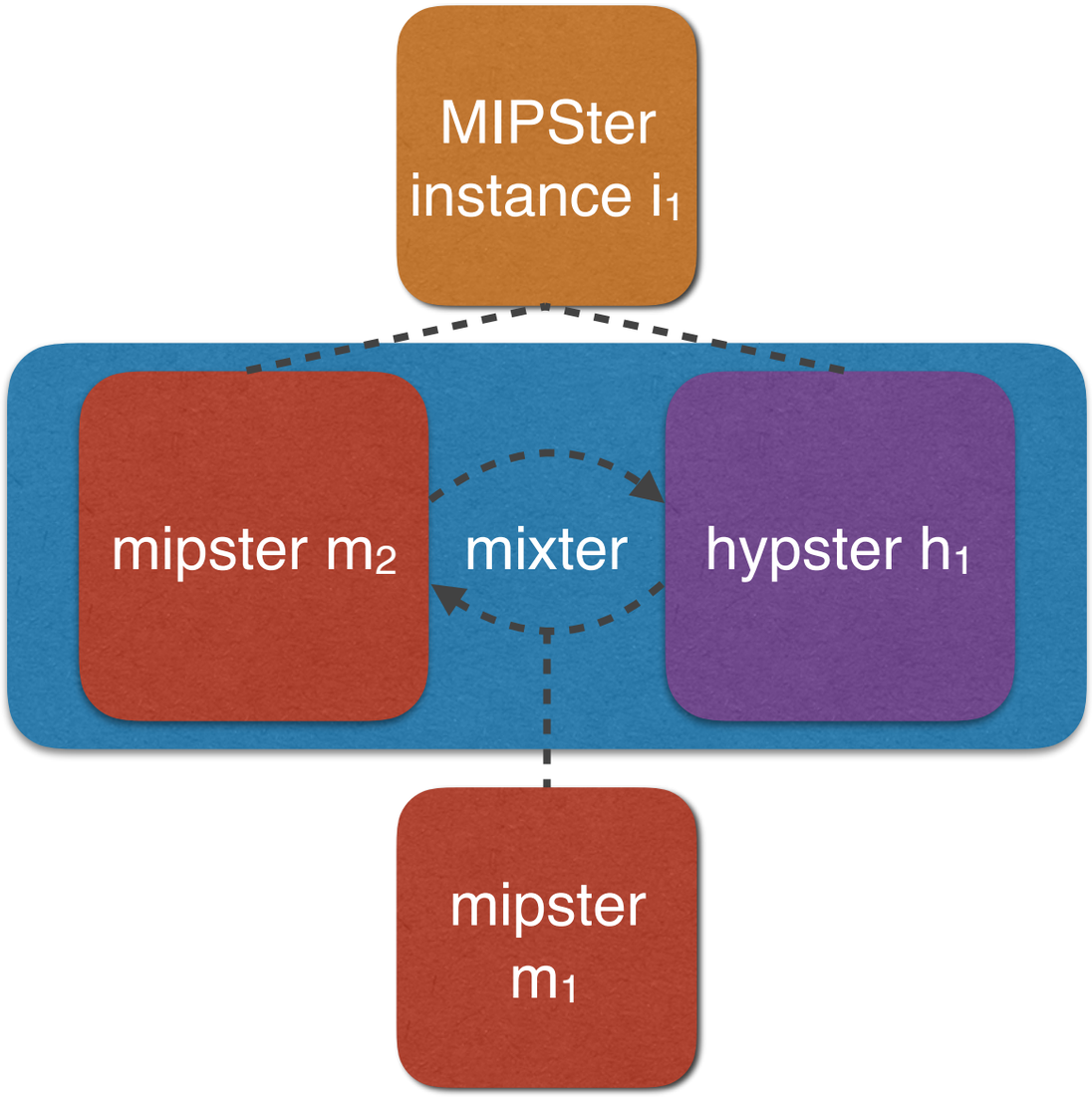
Virtualization and emulation of the same hardware



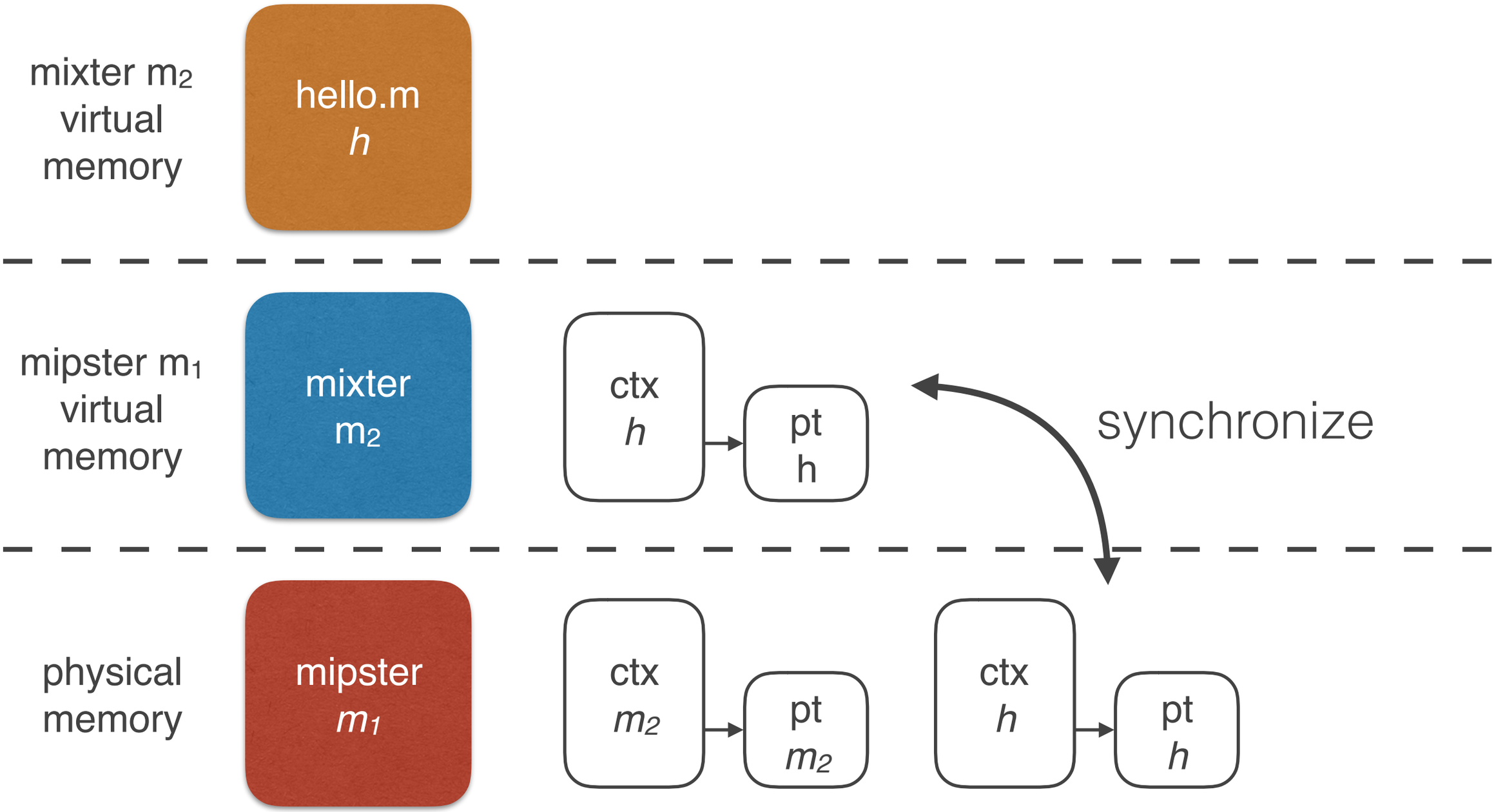
Idea



mixter


MIPSter
instance i_1
mipster m_2
mixter
hypster h_1
mipster
m_1

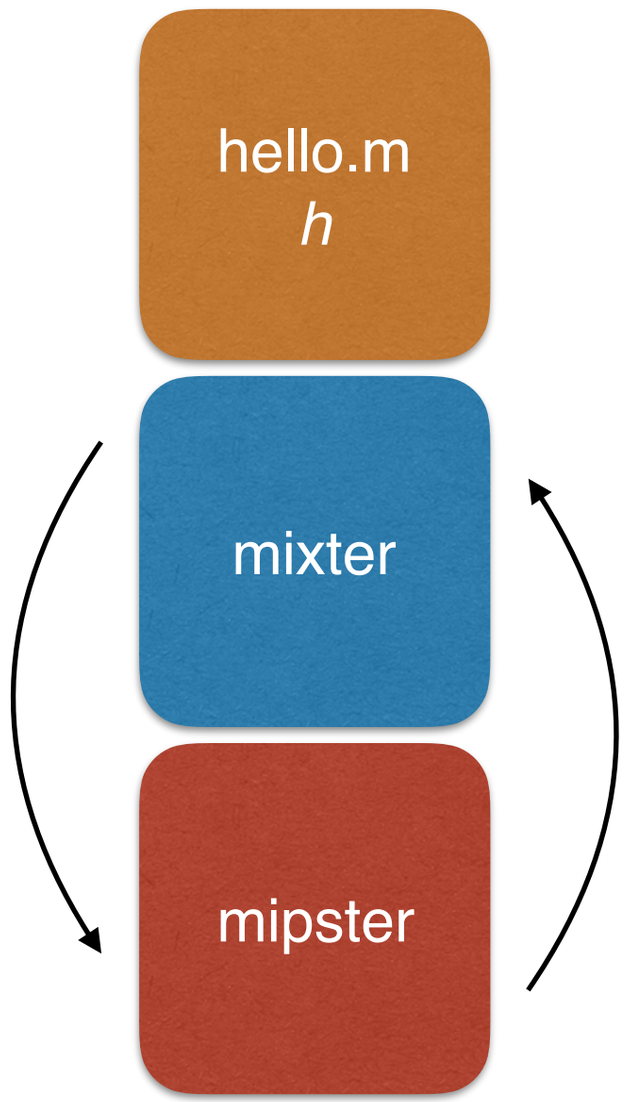
Emulation and Virtualization



Context caching

restoreContext:

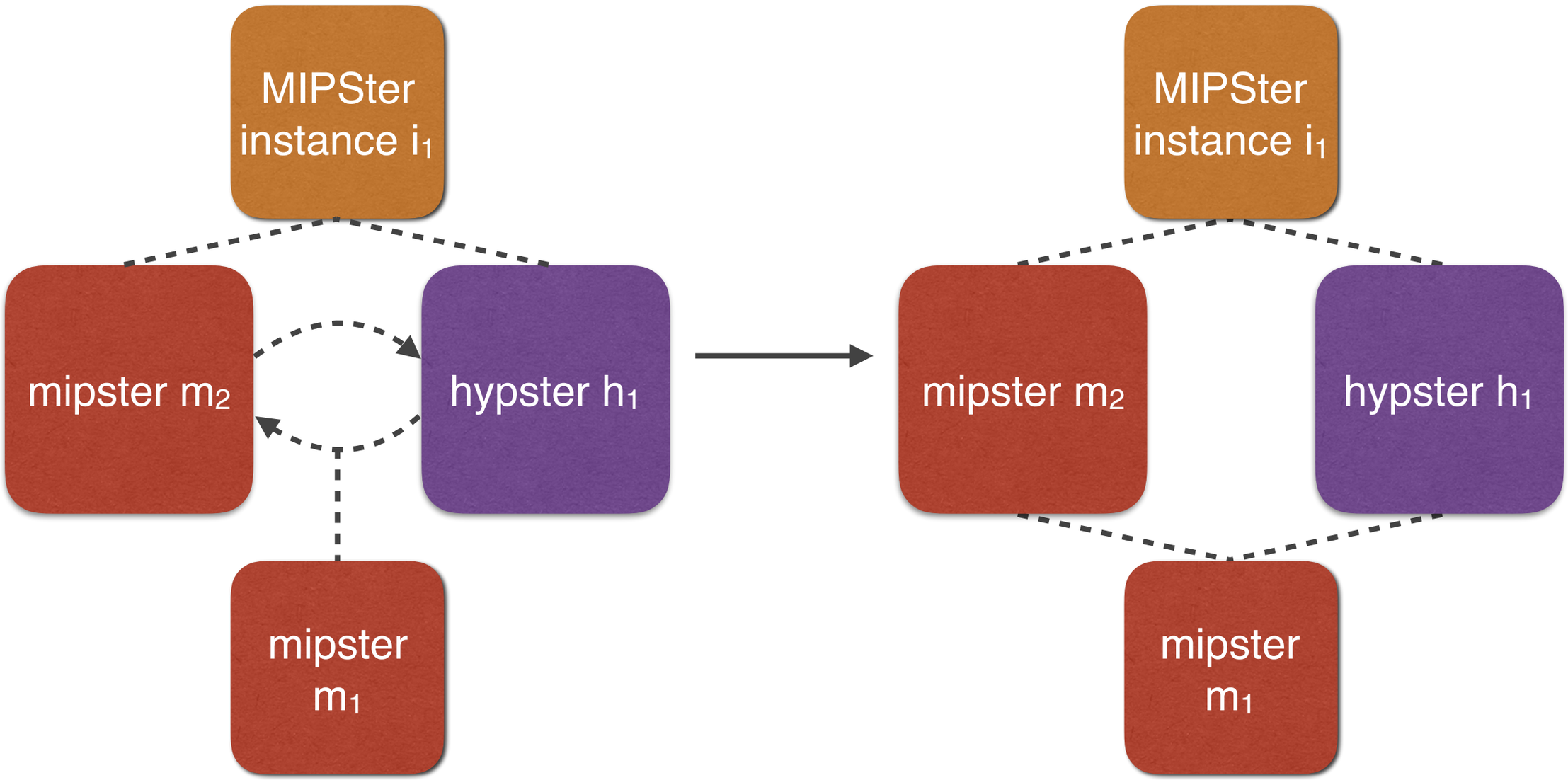
- restore machine state in physical context
  - pc
  - all registers
  - all newly allocated pages



saveContext:

- save machine state in virtual context
  - pc
  - all registers

Future work


MIPSter instance i_1
mipster m_2
hypster h_1
mipster m_1
MIPSter instance i_1
mipster m_2
hypster h_1
mipster m_1

References

[1] Christoph M. Kirsch. Selfie and the basics. In Proceedings of the 2017 ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software, Onward! 2017. ACM, 2017.

[2] MIPS Technologies, 1225 Charleston Road, Mountain View, CA. MIPS32 Architecture for Programmers Volume I: Introduction to the MIPS32 Architecture, 0.95 edition, March 2001.

[3] MIPS Technologies, 1225 Charleston Road, Mountain View, CA. MIPS32 Architecture for Programmers Volume II: The MIPS32 Instruction Set, 0.95 edition, March 2001.

[4] MIPS Technologies, 1225 Charleston Road, Mountain View, CA. MIPS32 Architecture for Programmers Volume III: The MIPS32 Privileged Resource Architecture, 0.95 edition, March 2001.

Thanks for your attention!

Any questions?