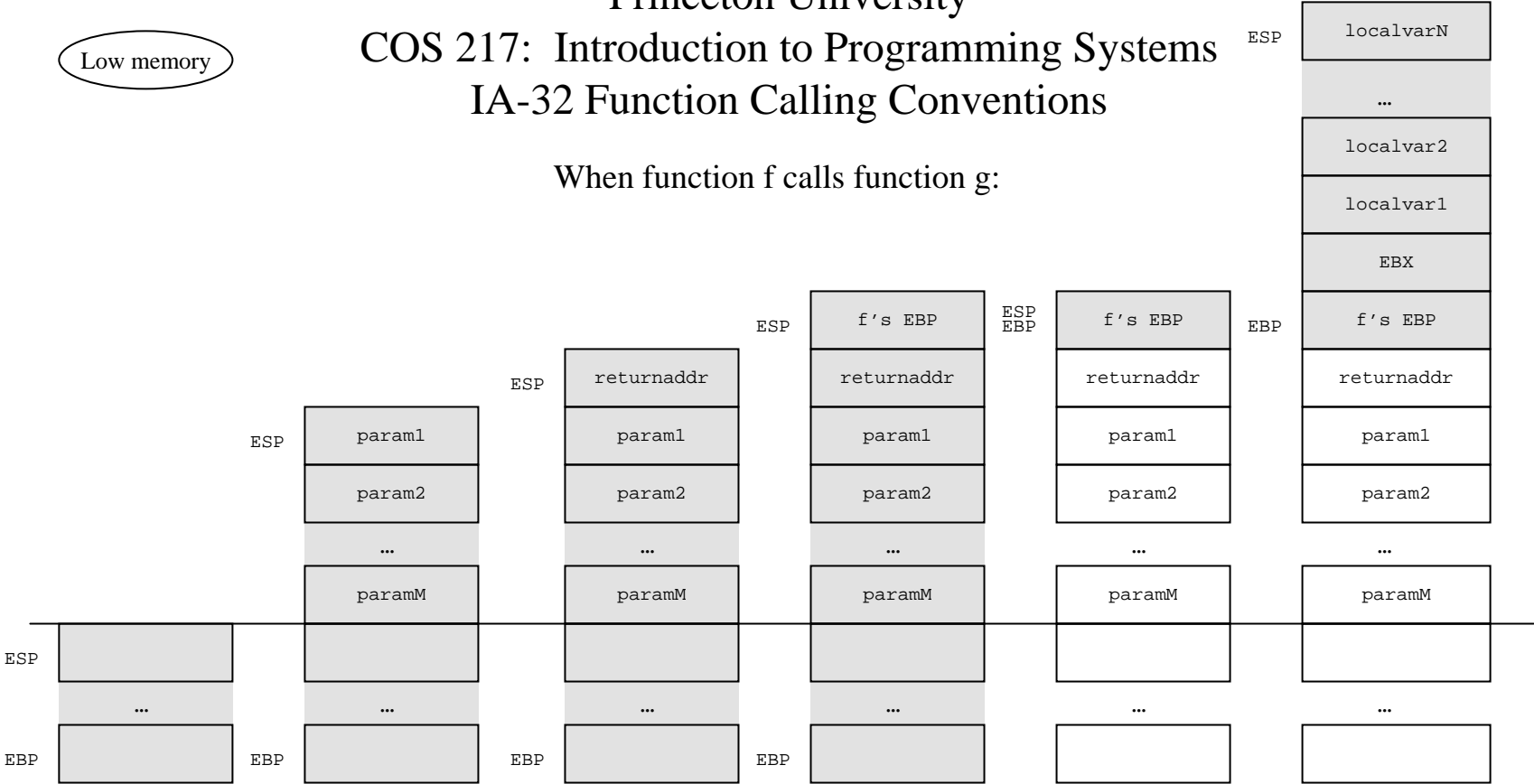


Low memory

Princeton University COS 217: Introduction to Programming Systems IA-32 Function Calling Conventions

When function f calls function g:



(1) f pushes parameters:
`pushl paramM`
`...`
`pushl param2`
`pushl param1`

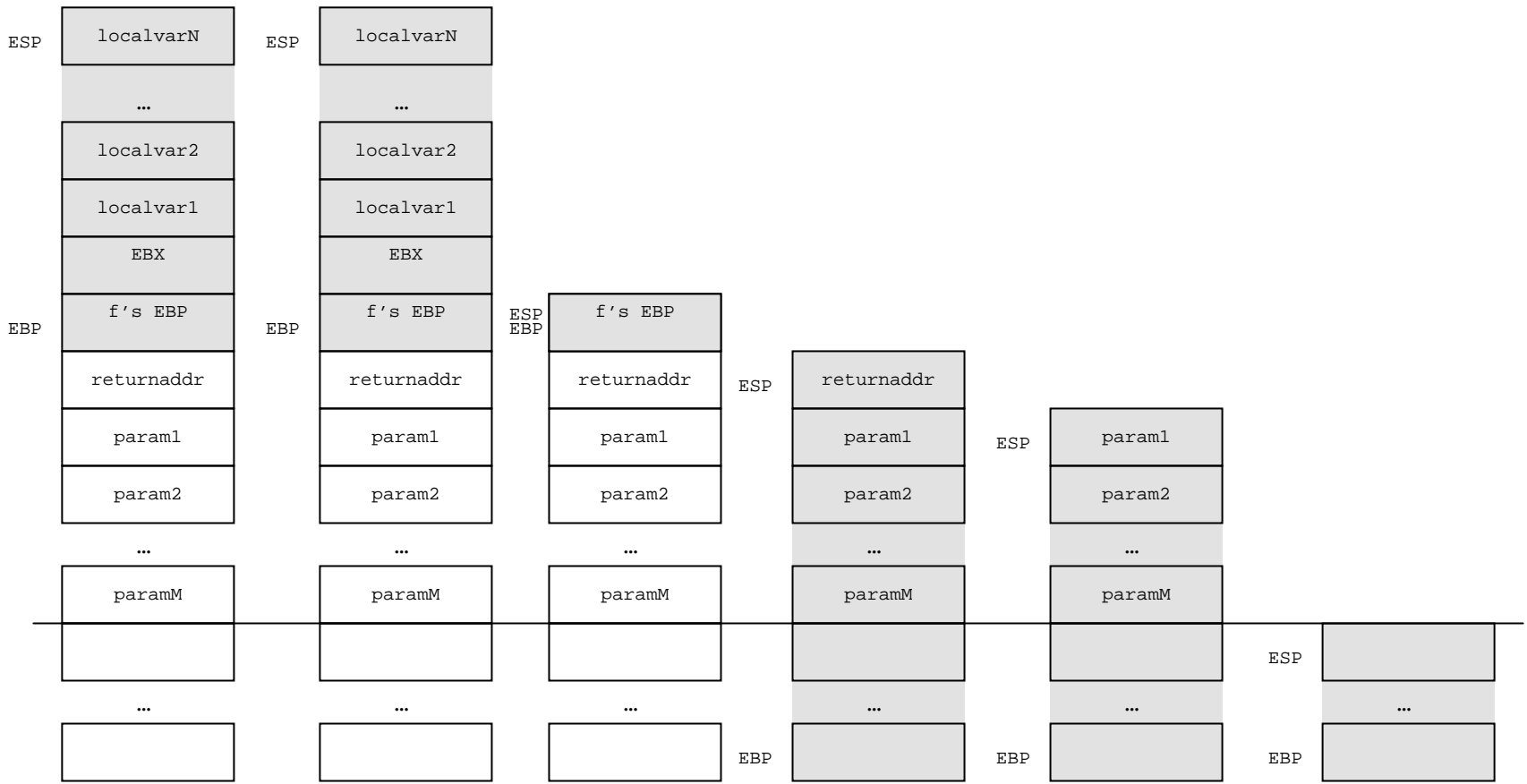
(2) f executes call instruction:
`call g`

(3) g pushes f's EBP:
`pushl %ebp`

(4) g moves ESP to EBP:
`movl %esp,%ebp`

(5) If necessary, g pushes EBX, ESI, or EDI and local variables:
`pushl %ebx`
`pushl localvar1`
`pushl localvar2`
`...`
`pushl localvarN`

High memory



(6) g uses parameters and local variables to compute a return value, and moves that value to EAX:

```
movl 8(%ebp), ???
movl 12(%ebp), ???
...
movl -8(%ebp), ???
movl -12(%ebp), ???
...
movl ???, %eax
```

(7) If necessary, g restores EDI, ESI, or EBX

```
movl -4(%ebp), %ebx
```

(8) g moves EBP to ESP:

```
movl %ebp, %esp
```

(9) g pops from stack into EBP:

```
popl %ebp
```

(10) g executes ret instruction:

```
ret
```

(11) f pops actual parameters from stack, and uses return value in EAX:

```
addl $4*M, %esp
movl %eax, ???
```