

Heap Allocation

C++

Example: dynamically allocate all non-primitive values

```
Foo foo; // static allocation
Foo* foo; // dynamic allocation
```

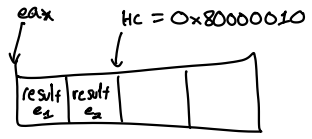
At program start: call malloc and allocate slab of memory

Global variable tracking next free byte of heap

(4, 5)

bird pointers end in 01 machine pointers and in 00 heap_cursor is a machine ptr

```
mov eax, 8
mov [ebp-4], eax
mov eax, 10
mov [ebp-8], eax
mov ecx, [heap_cursor]
mov eax, [ebp-4]:
mov [ecx], eax
mov eax, [ebp-8]
mov [ecx+4], eax
mov ecx, ecx
add ecx, 8
mov [heap_cursor], ecx
or eax, 1
```



0x80000008
 0x8000001000
 0x8000001001
 0x8000001009

let $x = (4, 5)$ in eax

first(x)

all the stuff from above

```
mov [ebp-4], eax
mov eax, [ebp-4]
and eax, 0xFFFFF0C xor eax, 1 dec eax
mov eax, [eax]
```

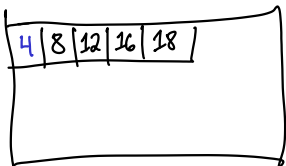
Eagle

(4, 6, 8, 9)[8]

$\langle \text{expr} \rangle ::= \dots$

| ($\langle \text{expr} \rangle, \dots, \langle \text{expr} \rangle$)

| $\langle \text{expr} \rangle [\langle \text{expr} \rangle]$



expected a tuple 4[3] : err code 4

index oob : (1,2)[-1] : err code 5