Virtual Memory:
malloc, method 1: implicit lists

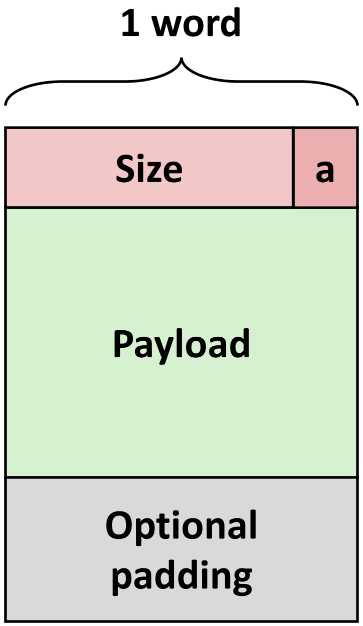
Method 1: Implicit List

- **For each block we need both size and allocation status**
  - Could store this information in two words: wasteful!

Method 1: Implicit List

- **For each block we need both size and allocation status**
  - Could store this information in two words: wasteful!
- **Standard trick**
  - If blocks are aligned, some low-order bits of size are always 0
  - Instead of storing an always-0 bit, use it as a allocated/free flag
  - When reading size word, must mask out this bit

Format of allocated and free blocks

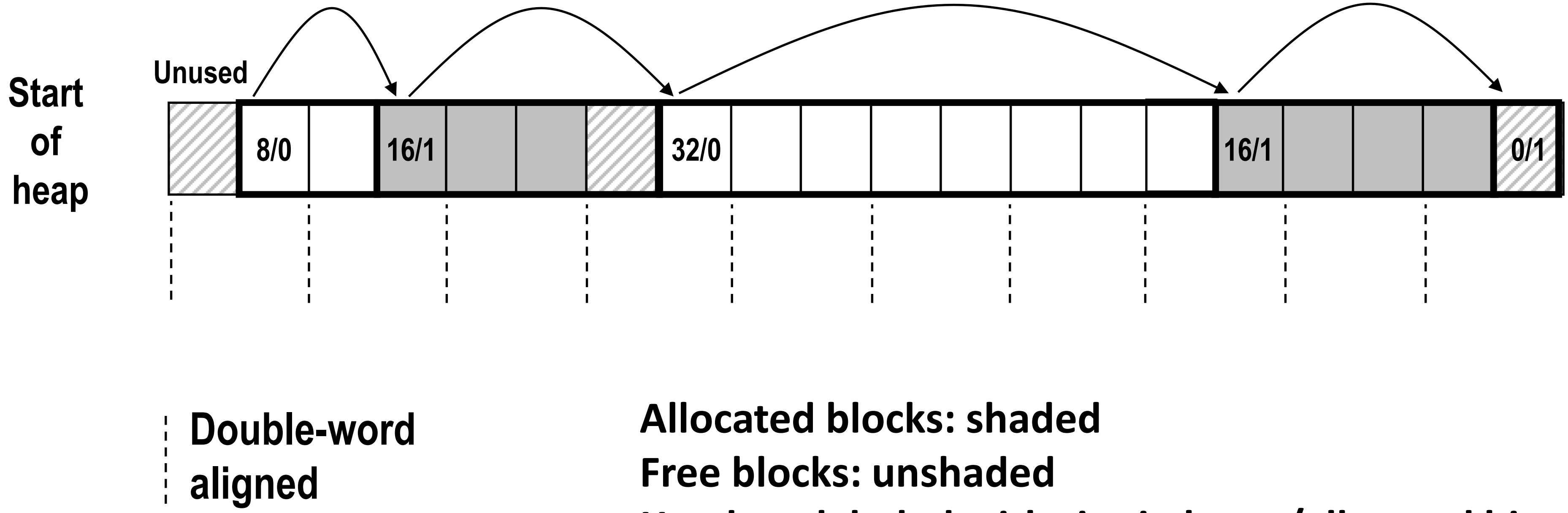


a = 1: Allocated block
a = 0: Free block

Size: block size

Payload: application data (allocated blocks only)

Detailed Implicit Free List Example



Allocated blocks: shaded

Free blocks: unshaded

Headers: labeled with size in bytes/allocated bit

Implicit List: Finding a Free Block

- ***First fit:***
  - Search list from beginning, choose ***first*** free block that fits:

```
p = start;
while ((p < end) &&     \\ not passed end
       ((*p & 1) ||     \\ already allocated
       (*p  <= len)))   \\ too small
  p = p + (*p & -2);    \\ goto next block (word addressed)
```

  - Can take linear time in total number of blocks (allocated and free)
  - In practice it can cause “splinters” at beginning of list

Implicit List: Finding a Free Block

- ***First fit:***
  - Search list from beginning, choose ***first*** free block that fits:

```
p = start;
while ((p < end) &&    \\ not passed end
       ((*p & 1) ||    \\ already allocated
       (*p  <= len)))  \\ too small
  p = p + (*p & -2);   \\ goto next block (word addressed)
```

  - Can take linear time in total number of blocks (allocated and free)
  - In practice it can cause "splinters" at beginning of list
- ***Next fit:***
  - Like first fit, but search list starting where previous search finished
  - Should often be faster than first fit: avoids re-scanning unhelpful blocks
  - Some research suggests that fragmentation is worse

Implicit List: Finding a Free Block

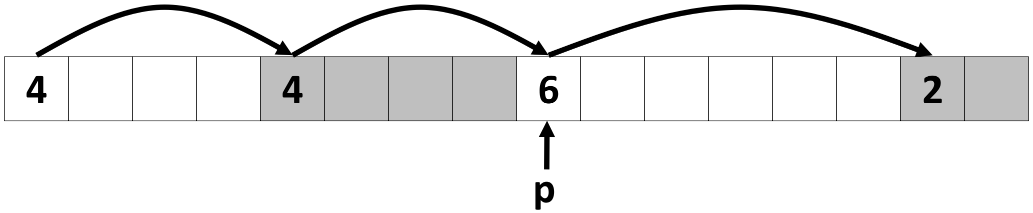
- ***First fit:***
  - Search list from beginning, choose ***first*** free block that fits:

```
p = start;
while ((p < end) &&      \\ not passed end
       ((*p & 1) ||      \\ already allocated
       (*p  <= len)))    \\ too small
  p = p + (*p & -2);     \\ goto next block (word addressed)
```

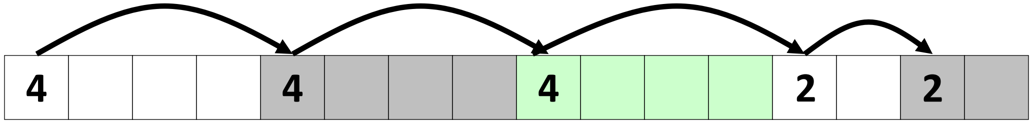
  - Can take linear time in total number of blocks (allocated and free)
  - In practice it can cause “splinters” at beginning of list
- ***Next fit:***
  - Like first fit, but search list starting where previous search finished
  - Should often be faster than first fit: avoids re-scanning unhelpful blocks
  - Some research suggests that fragmentation is worse
- ***Best fit:***
  - Search the list, choose the ***best*** free block: fits, with fewest bytes left over
  - Keeps fragments small—usually improves memory utilization
  - Will typically run slower than first fit

Implicit List: Allocating in Free Block

- **Allocating in a free block: *splitting***
  - Since allocated space might be smaller than free space, we might want to split the block



```
addblock(p, 4)
```



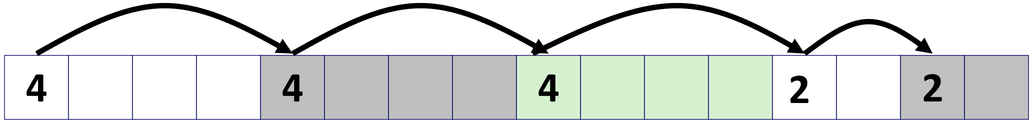
```
void addblock(ptr p, int len) {
  int newsize = ((len + 1) >> 1) << 1;  // round up to even
  int oldsize = *p & -2;                // mask out low bit
  *p = newsize | 1;                     // set new length
  if (newsize < oldsize)
    *(p+newsize) = oldsize - newsize;   // set length in remaining
}                                       //   part of block
```

Implicit List: Freeing a Block

- **Simplest implementation:**
  - Need only clear the "allocated" flag

```
void free_block(ptr p) { *p = *p & -2 }
```

  - But can lead to "false fragmentation"

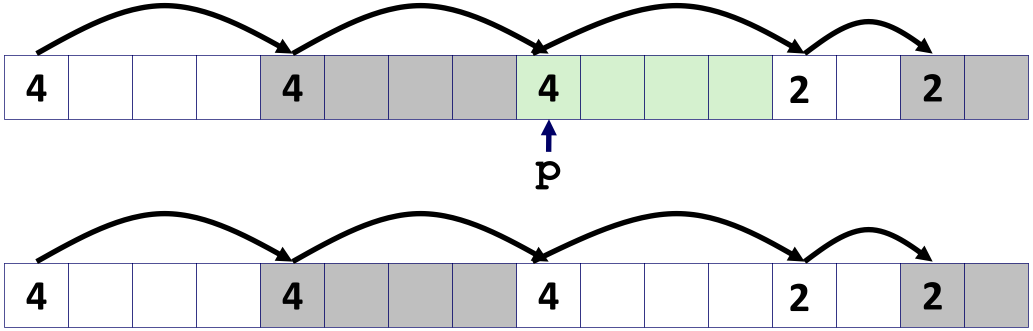


Implicit List: Freeing a Block

- **Simplest implementation:**
  - Need only clear the “allocated” flag

```
void free_block(ptr p) { *p = *p & -2 }
```

  - But can lead to “false fragmentation”

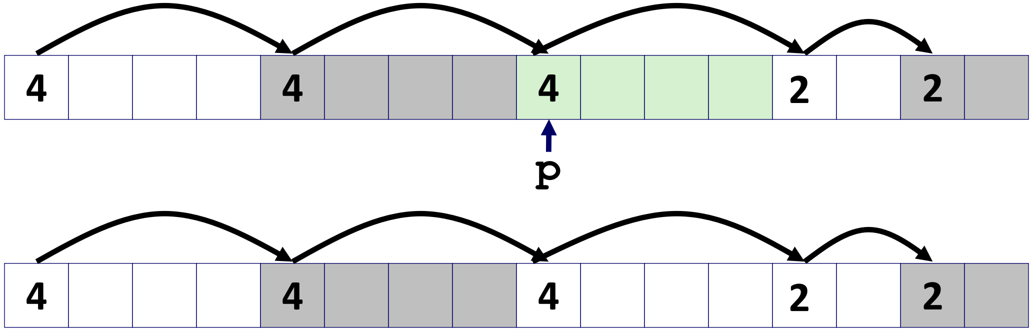


Implicit List: Freeing a Block

- **Simplest implementation:**
  - Need only clear the “allocated” flag

```
void free_block(ptr p) { *p = *p & -2 }
```

  - But can lead to “false fragmentation”



`free(p)`

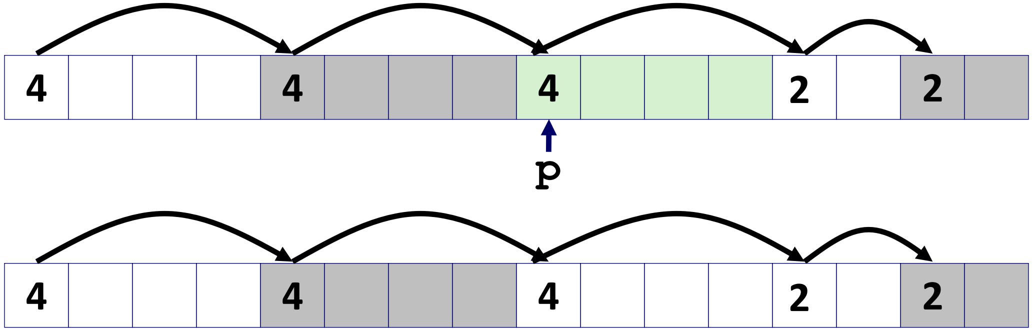
`malloc(5)` ***Oops!***

Implicit List: Freeing a Block

- **Simplest implementation:**
  - Need only clear the “allocated” flag

```
void free_block(ptr p) { *p = *p & -2 }
```

  - But can lead to “false fragmentation”



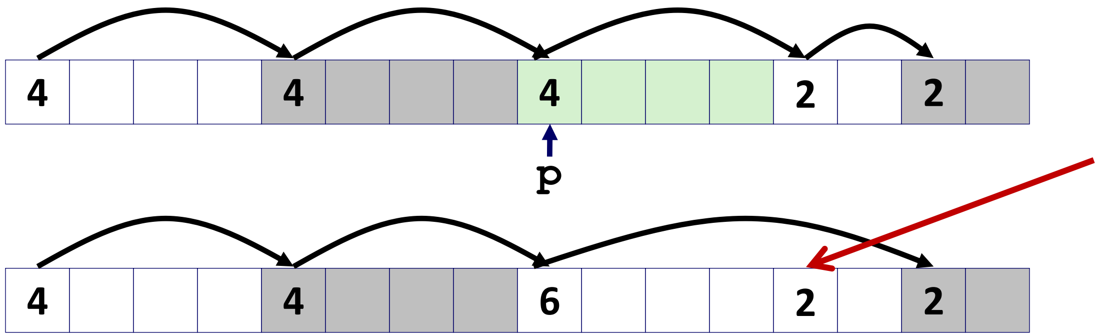
`free(p)`

`malloc(5)` *Oops!*

There is enough free space, but the allocator won’t be able to find it

Implicit List: Coalescing

- **Join *(coalesce)* with next/previous blocks, if they are free**
  - Coalescing with next block



`free(p)`

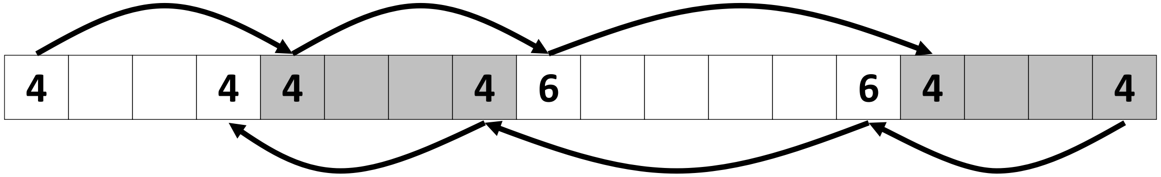
logically gone

```
void free_block(ptr p) {
    *p = *p & -2;           // clear allocated flag
    next = p + *p;          // find next block
    if ((*next & 1) == 0)
      *p = *p + *next;      // add to this block if
}                           //    not allocated
```

- But how do we coalesce with *previous* block?

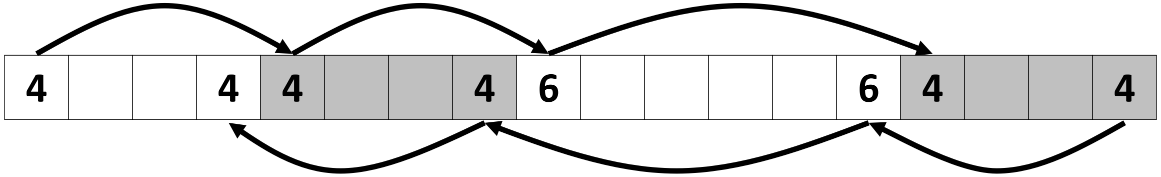
Implicit List: Bidirectional Coalescing

- ***Boundary tags*** [Knuth73]
  - Replicate size/allocated word at “bottom” (end) of free blocks
  - Allows us to traverse the “list” backwards, but requires extra space
  - Important and general technique!

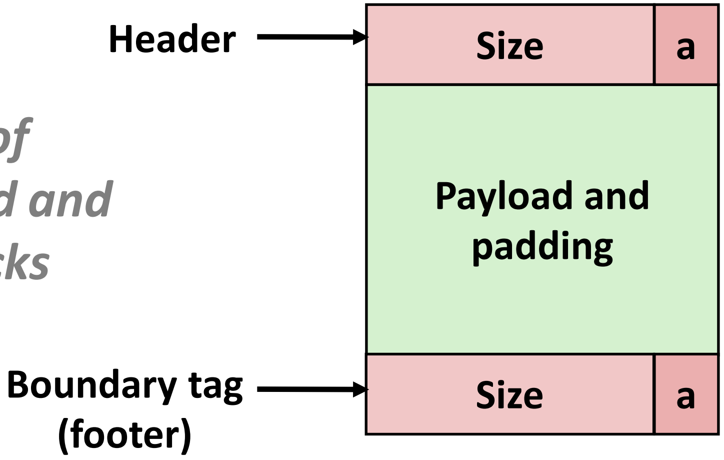


Implicit List: Bidirectional Coalescing

- ***Boundary tags*** [Knuth73]
  - Replicate size/allocated word at “bottom” (end) of free blocks
  - Allows us to traverse the “list” backwards, but requires extra space
  - Important and general technique!



4			4	4			4	6					6	4			4



Header

Size | a

Payload and padding

Boundary tag (footer)

Size | a

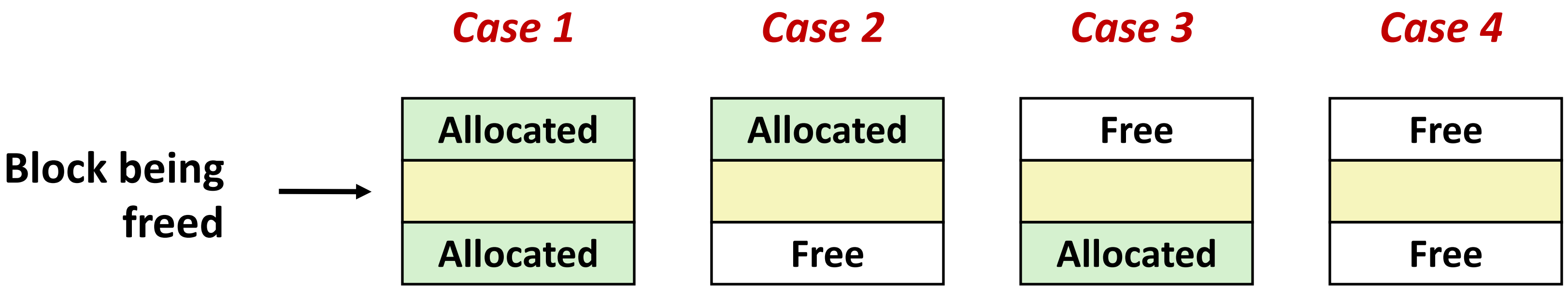
Format of allocated and free blocks

a = 1: Allocated block
a = 0: Free block

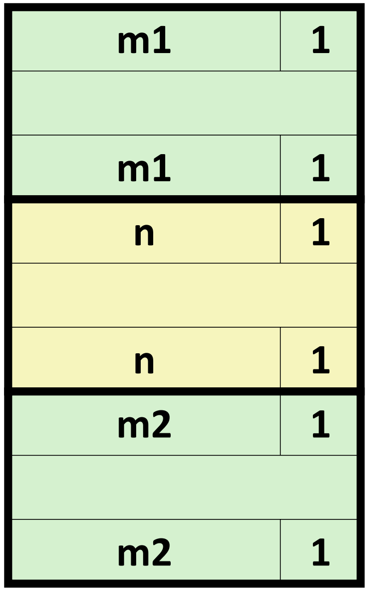
Size: Total block size

Payload: Application data (allocated blocks only)

Constant Time Coalescing



Constant Time Coalescing (Case 1)



m1 1

m1 1

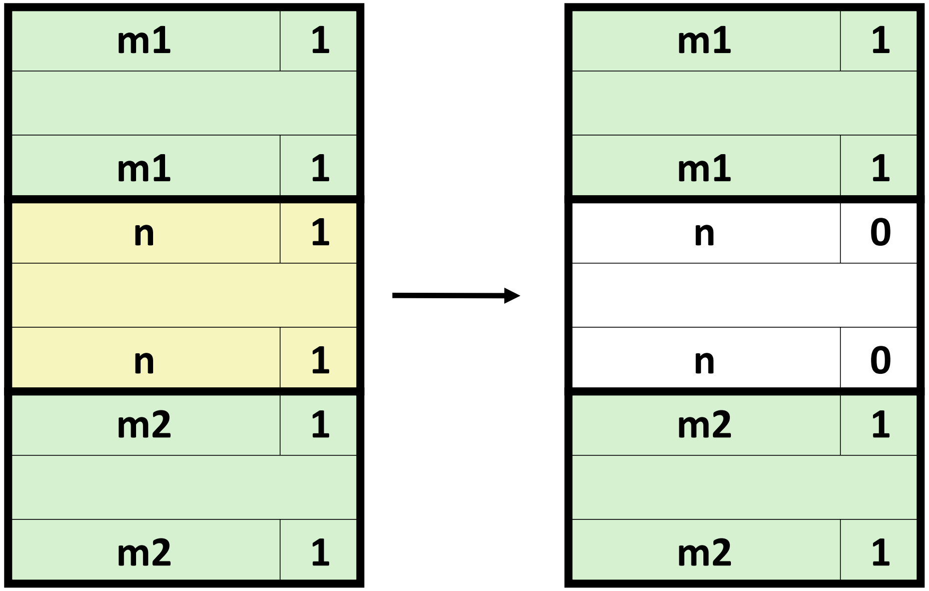
n 1

n 1

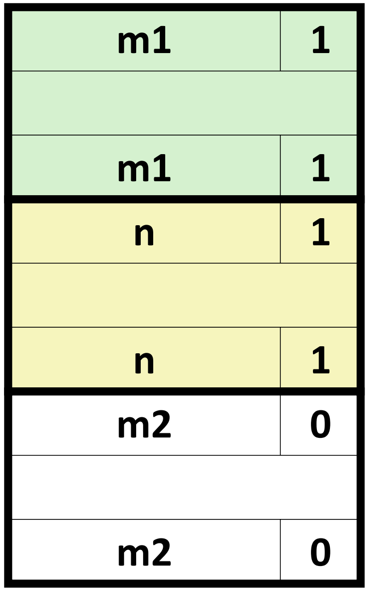
m2 1

m2 1

Constant Time Coalescing (Case 1)



Constant Time Coalescing (Case 2)



m1 1

m1 1

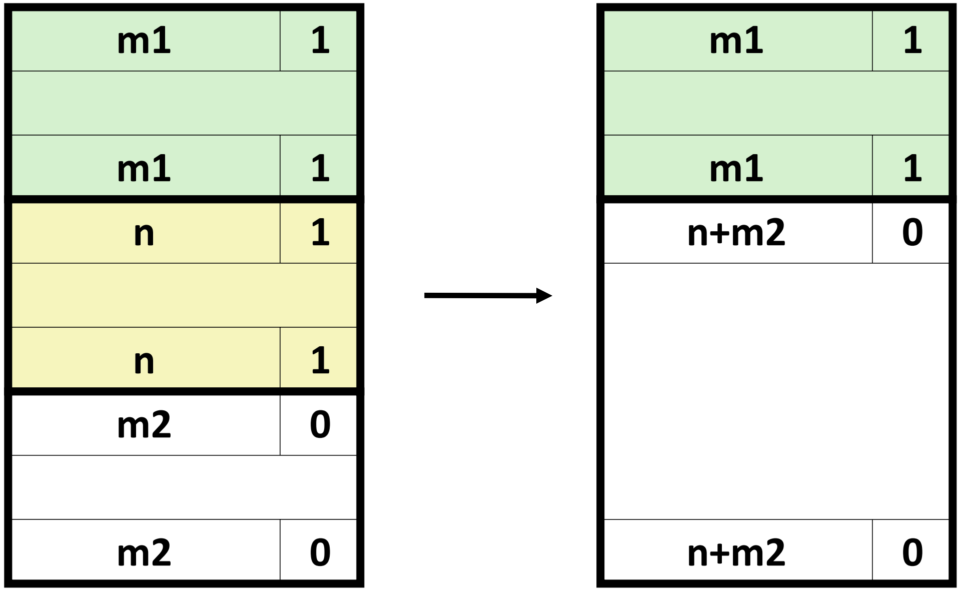
n 1

n 1

m2 0

m2 0

Constant Time Coalescing (Case 2)



m1 1

m1 1

n 1

n 1

m2 0

m2 0

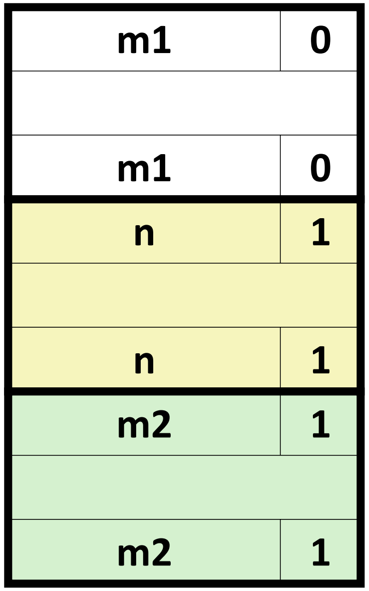
m1 1

m1 1

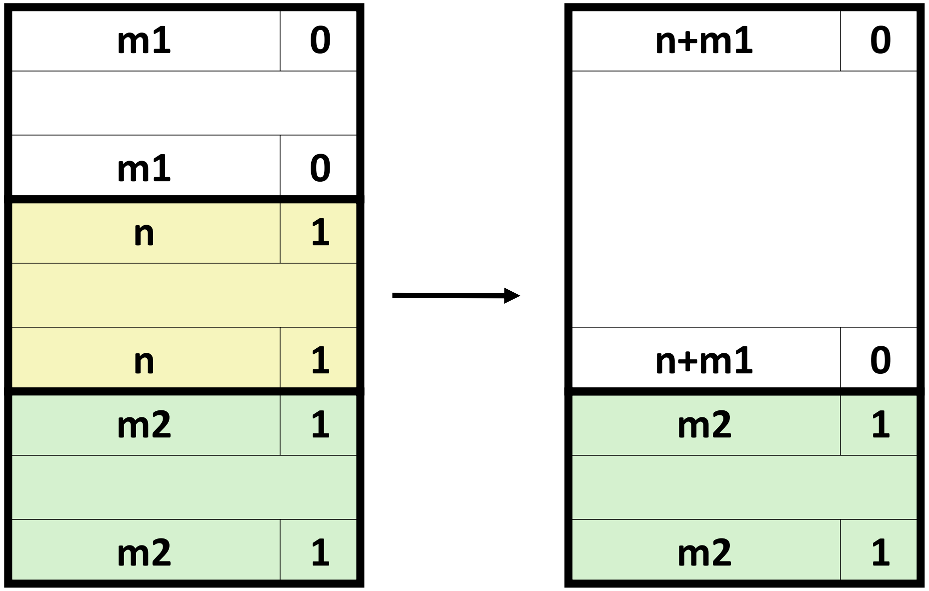
n+m2 0

n+m2 0

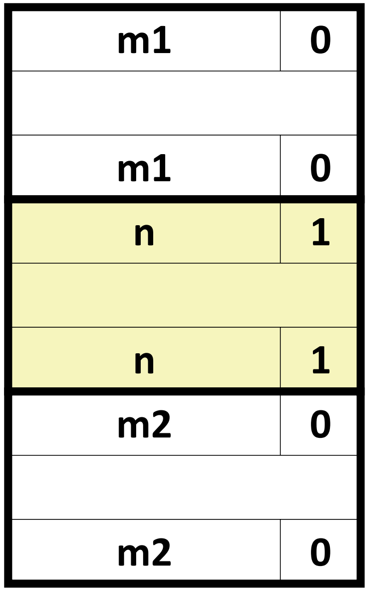
Constant Time Coalescing (Case 3)



Constant Time Coalescing (Case 3)



Constant Time Coalescing (Case 4)



m1 0

m1 0

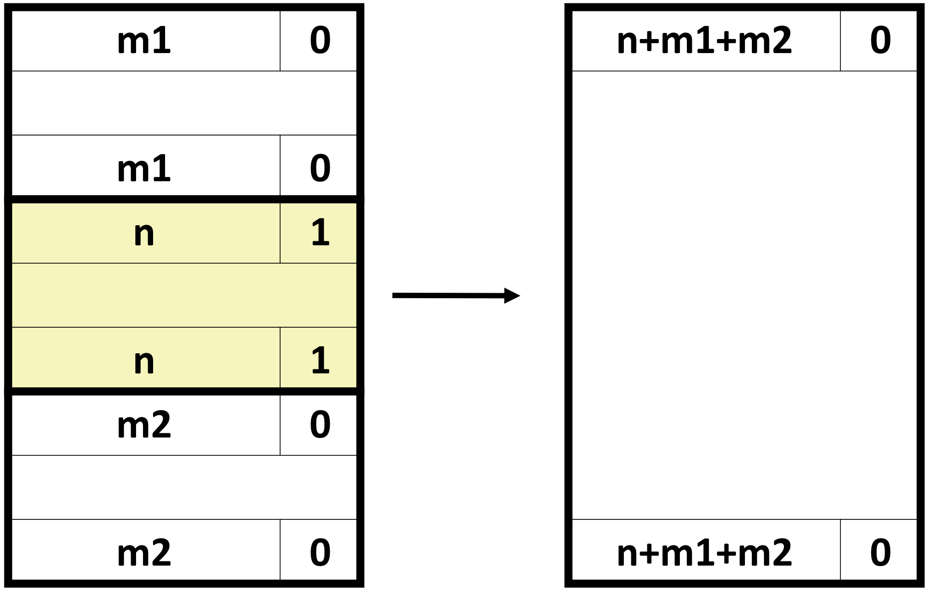
n 1

n 1

m2 0

m2 0

Constant Time Coalescing (Case 4)



m1	0
m1	0
n	1
n	1
m2	0
m2	0

n+m1+m2	0
n+m1+m2	0

Disadvantages of Boundary Tags

- **Internal fragmentation**
  - Not part of payload, hence overhead!

- **Can it be optimized?**
  - Which blocks need the footer tag?

Disadvantages of Boundary Tags

- **Internal fragmentation**
  - Not part of payload, hence overhead!

- **Can it be optimized?**
  - Which blocks need the footer tag?
    Do we need it for allocated blocks?

Disadvantages of Boundary Tags

- **Internal fragmentation**
  - Not part of payload, hence overhead!

- **Can it be optimized?**
  - Which blocks need the footer tag?
    Do we need it for allocated blocks?
    …Can we use *more* of the header free/allocated trick?

Summary of Key Allocator Policies

- **Placement policy:**
  - First-fit, next-fit, best-fit, etc.
  - Trades off lower throughput for less fragmentation
  - ***Interesting observation*****:** segregated free lists (next lecture) approximate a best fit placement policy without having to search entire free list

Summary of Key Allocator Policies

- **Placement policy:**
  - First-fit, next-fit, best-fit, etc.
  - Trades off lower throughput for less fragmentation
  - ***Interesting observation***: segregated free lists (next lecture) approximate a best fit placement policy without having to search entire free list

- **Splitting policy:**
  - When do we go ahead and split free blocks?
  - How much internal fragmentation are we willing to tolerate?

Summary of Key Allocator Policies

- **Placement policy:**
  - First-fit, next-fit, best-fit, etc.
  - Trades off lower throughput for less fragmentation
  - ***Interesting observation***: segregated free lists (next lecture) approximate a best fit placement policy without having to search entire free list
- **Splitting policy:**
  - When do we go ahead and split free blocks?
  - How much internal fragmentation are we willing to tolerate?
- **Coalescing policy:**
  - ***Immediate coalescing:*** coalesce each time **`free`** is called
  - ***Deferred coalescing:*** try to improve performance of **`free`** by deferring coalescing until needed. Examples:
    - Coalesce as you scan the free list for **`malloc`**
    - Coalesce when the amount of external fragmentation reaches some threshold (but how do you measure that?)

Implicit Lists: Summary

- **Implementation: very simple**
- **Allocate cost:**
  - linear time worst case
- **Free cost:**
  - constant time worst case
  - even with coalescing
- **Memory usage:**
  - will depend on placement policy
  - First-fit, next-fit or best-fit

- **Not used in practice for `malloc/free` because of linear-time allocation**
  - used in many special purpose applications

- **However, the concepts of splitting and boundary tag coalescing are general to *all* allocators**