Лекция 0xE

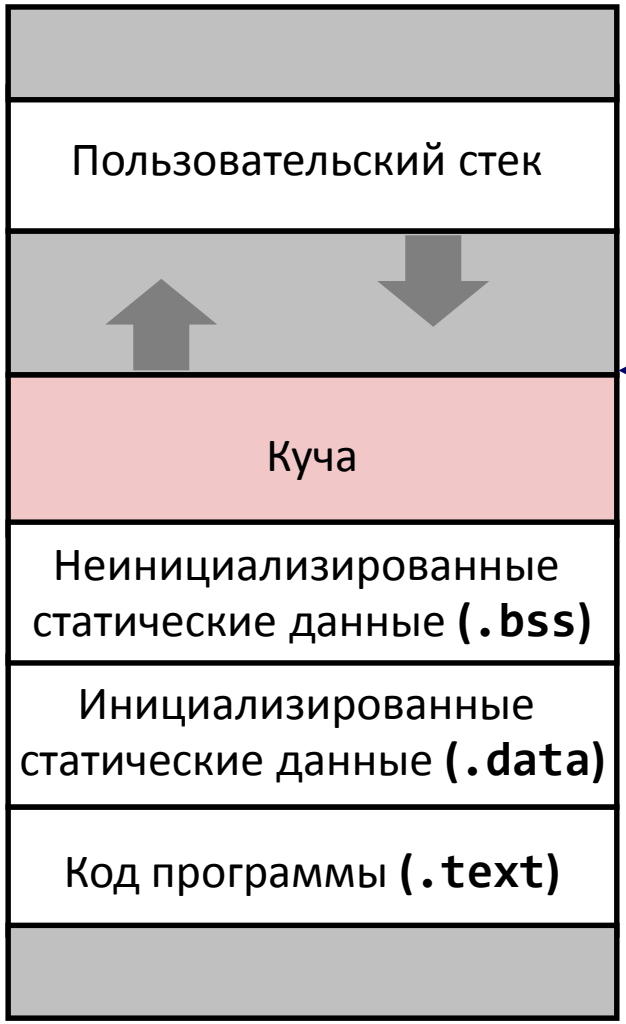
25 марта

Управление динамической памятью

```
#include <stdlib.h>

void *calloc(size_t nmemb, size_t size);
void *malloc(size_t size);
void free(void *ptr);
void *realloc(void *ptr, size_t size);
```

- Программисты используют *функции выделения динамической памяти* (например, `malloc`) для того, чтобы получить память под переменные во время выполнения.
  - Для структур данных, размер которых известен только во время выполнения.
- Эти функции управляют пространством памяти программы, называемой *куча*.

Интерфейсные функции



Верхушка кучи

```
#include <unistd.h>

int brk(void *addr);
void *sbrk(intptr_t increment);
```

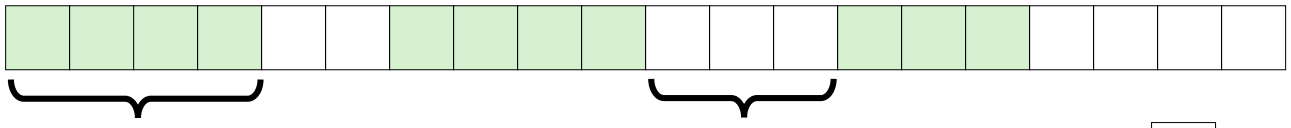
```
sbrk(0);
```

Выделение динамической памяти

- Менеджер памяти рассматривает пространство кучи как множество *блоков* различного размера, которые либо *выделены*, либо *свободны*
- Различные способы управления динамической памятью
  - ***Явное управление*:** разработчик сам выделяет и освобождает пространство в памяти
    - Например, `malloc` и `free` в языке Си
  - ***Неявное управление*:** разработчик выделяет память но не освобождает
    - Сборщик мусора в языках Java, ML, Lisp, в платформе .NET
    - Умные указатели (smart pointers) – подсчет «живых» ссылок на выделенную память. Освобождает память библиотека (boost, `std::unique_ptr` в языке Си++11) или компилятор (язык Rust).

```
void foo(int n, int m) {
    int i, *p;

/* Выделяем блок из n целых чисел */

    p = (int *) malloc(n * sizeof(int));
    if (p == NULL) {
        perror("malloc");
        exit(0);
    }

    ...

/* Возвращаем пространство в кучу */
    free(p);
}
```

- В дальнейшем материале предполагается, что выделение и освобождение памяти происходит с блоками машинных слов
- Машинное слово вмещает указатель, т.е. 4 байта



Выделенный блок (4 слова)

Свободный блок (3 слова)

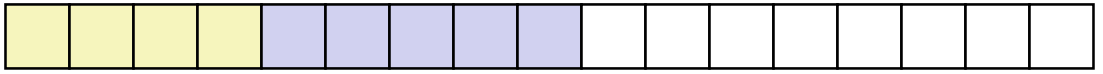
Свободное слово

Занятое слово

Пример: выделение и освобождение памяти в произвольном порядке

```
p1 = malloc(16)
```

```
p2 = malloc(20)
```



```
p3 = malloc(24)
```

```
free(p2)
```

```
p4 = malloc(8)
```

Ограничения

- Пользовательская программа
  - Произвольная последовательность вызовов функций `malloc` и `free`
  - Вызовы `free` получают в качестве параметра указатель полученный из функции `malloc`
- Менеджер памяти
  - Никак не может повлиять на запрашиваемый размер блоков или число этих запросов
  - Обязан предоставлять запрошенную память незамедлительно
    - *нет возможности буферизировать запросы (переупорядочить)*
  - Блоки выделяются в свободной памяти
  - Выделяемые блоки должны быть выровнены
    - выравнивание 8 байт для GNU `malloc` (`libc malloc`) в ОС Linux
  - Нет возможности перемещать уже выделенные блоки
    - *нельзя собрать вместе выделенную память*

Производительность
Пропускная способность

- Имеется некоторая последовательность вызовов `malloc` и `free`:
  - $R_0, R_1, ..., R_k, ..., R_{n-1}$

- Цели: максимально увеличить пропускную способность менеджера и пиковое использование памяти
  - Эти цели часто конфликтуют

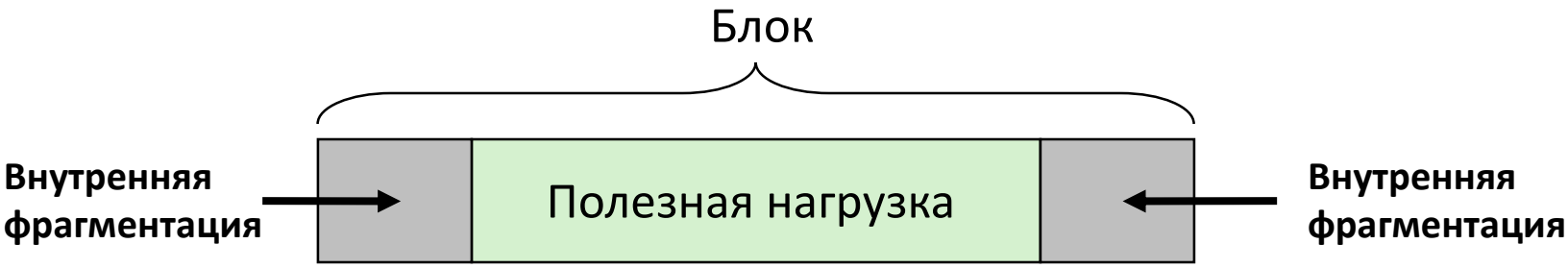
- Пропускная способность
  - Число выполненных запросов за единицу времени
  - Пример
    - 5 000 вызовов `malloc` и 5 000 вызовов `free` в течение 10 секунд
    - Пропускная способность 1 000 операций в секунду

Производительность
Пиковое использование

- Дана последовательность вызовов функций `malloc` и `free`
  - $R_0, R_1, ..., R_k, ... , R_{n-1}$
- *Суммарная полезная нагрузка* P_k
  - `malloc(p)` возвращает блок с полезной нагрузкой в p байт
  - После завершения вызова R_k, *суммарная полезная нагрузка* P_k - сумма всех выделенных, но еще не освобожденных блоков памяти
- *Текущий размер кучи* H_k
  - Предполагается H_k монотонно не убывает
    - т.е. в результате вызовов `sbrk` куча только растет
- *Пиковое использование памяти после k запросов*
  - $U_k = (max_{i<k} P_i) \ / \ H_k$

Внутренняя фрагментация

- *Внутренняя фрагментация* возникает если размер полезной нагрузки меньше размера блока



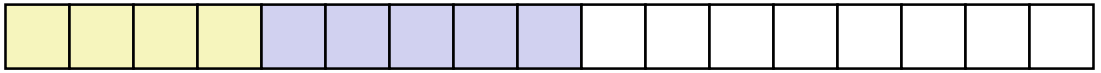
- Причины возникновения
  - Накладные расходы на поддержку внутренних структур данных
  - Выравнивание
  - Особенности политики выделения блоков (например, принудительно выделяется блок большего размера)
- Зависит только от последовательности предыдущих запросов памяти
  - Легко измерить

Внешняя фрагментация

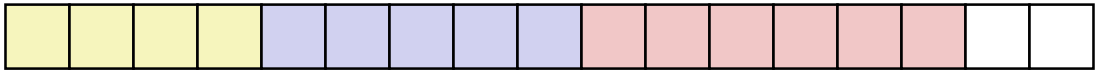
- Возникает, когда в куче суммарно содержится достаточное количество свободных блоков, но нет единого блока требуемого размера

```
p1 = malloc(16)
```

```
p2 = malloc(20)
```



```
p3 = malloc(24)
```



```
free(p2)
```

```
p4 = malloc(24)
```

Отказ в предоставлении памяти

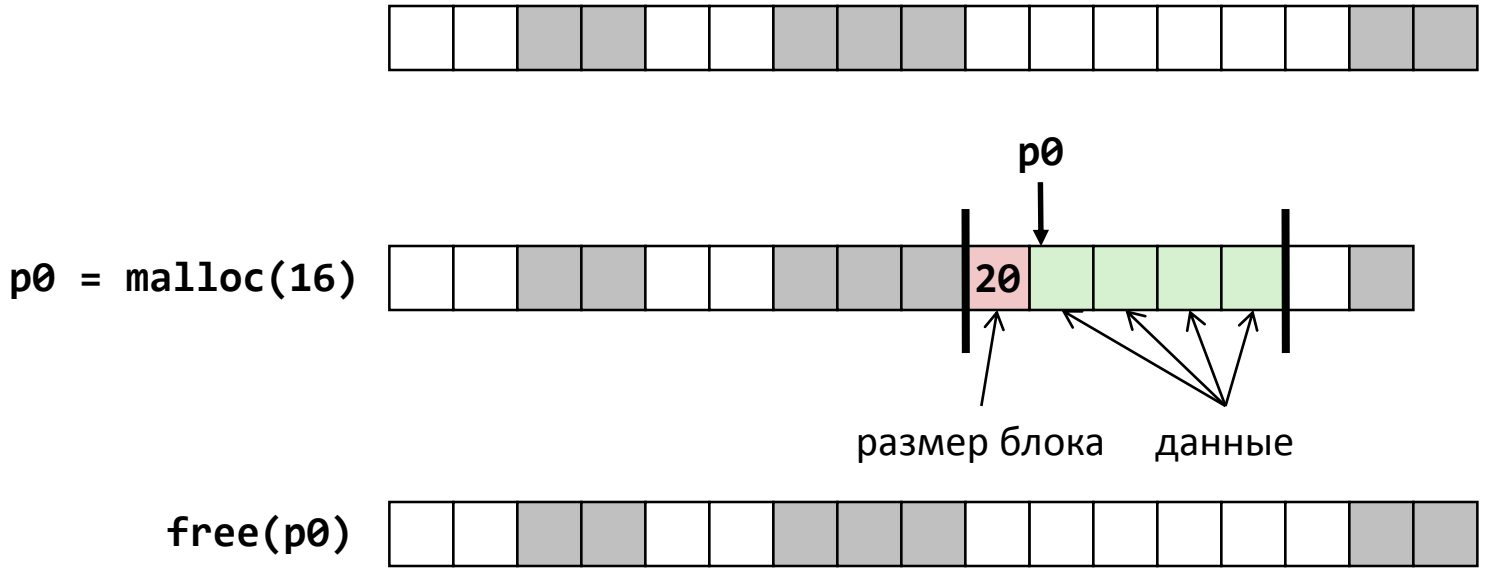
- Зависит от того, что будет запрашиваться в будущем
  - Трудно оценить

Проблемы реализации менеджера памяти

- Как следует запоминать, сколько памяти должно быть освобождено для данного адреса?
- Как лучше поддерживать информацию о свободных блоках?
- Если принято решение выделить блок большего размера, чем было запрошено, что делать с лишней памятью?
- Какой блок лучше выбрать для выделения?
- Как лучше распорядиться освобожденным блоком?

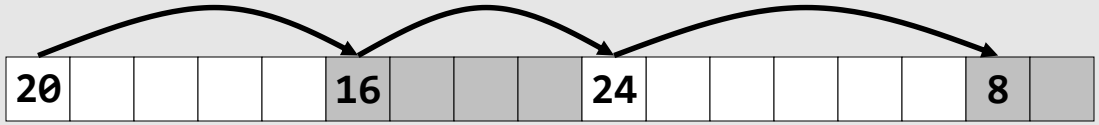
Сколько освобождать?

- Стандартный метод
  - Размещаем длину блока в слове, предшествующем блоку.
    - Такое слово называют ***заголовком***
  - Требуется дополнительное слово на каждый выделяемый блок

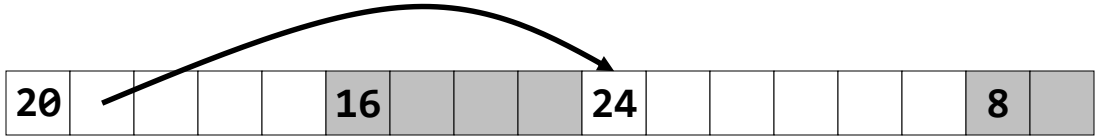


Как отслеживать свободные блоки

- Метод 1: *неявный список* с использованием длины блока



- Метод 2: *Явный список* свободных блоков с использованием указателей



- Метод 3: *Раздельные списки*
  - Распределение блоков по раздельным спискам, исходя из размеров этих блоков
- Метод 4: *Сортировка блоков по размеру*
  - Можно использовать сбалансированное дерево (например, Красно-Черные деревья) с указателями в каждом свободном блоке, и с длиной блока в качестве ключа

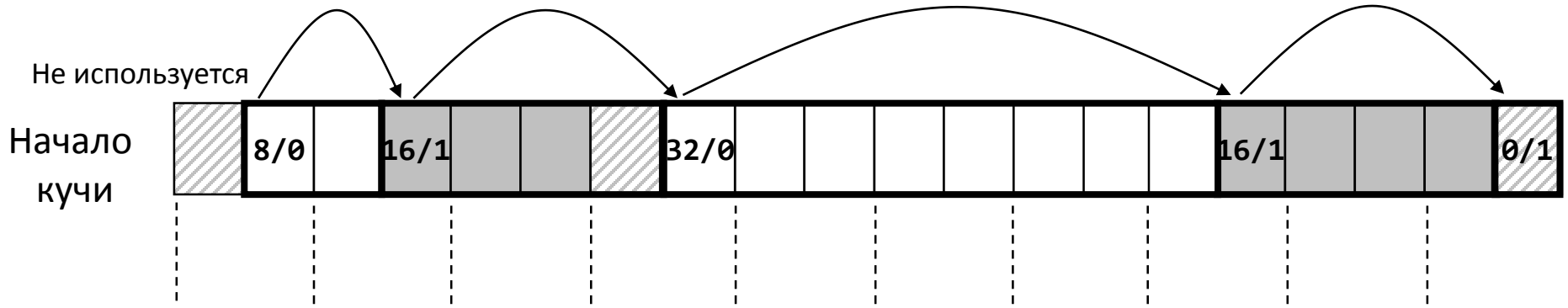
Метод 1: Неявный список

- Для каждого блока необходимо знать его длину и состояние - выделен/свободен
  - Расточительно использовать для этого два слова
- Стандартный прием
  - Если блоки выровнены в памяти, несколько младших битов адреса всегда 0, а размер блока кратен некоторой степени двойки
  - Вместо 0 храним в младшем бите заголовка флаг, выделен или свободен блок
  - Когда заголовок интерпретируется как размер блока, младший бит маскируется

Формат выделенных и свободных блоков

a = 1: блок занят
a = 0: блок свободен

Пример
Неявный список



Выровнено по границе двойного слова (8 байт)

Выделенные блоки: серая заливка
Свободные блоки: белое
Заголовки: обозначены размером в байтах /битом выделения

Неявный список
Поиск свободного блока

- *Первый подходящий:*
  - Проходим список с начала, выбираем ***первый*** подходящий блок:

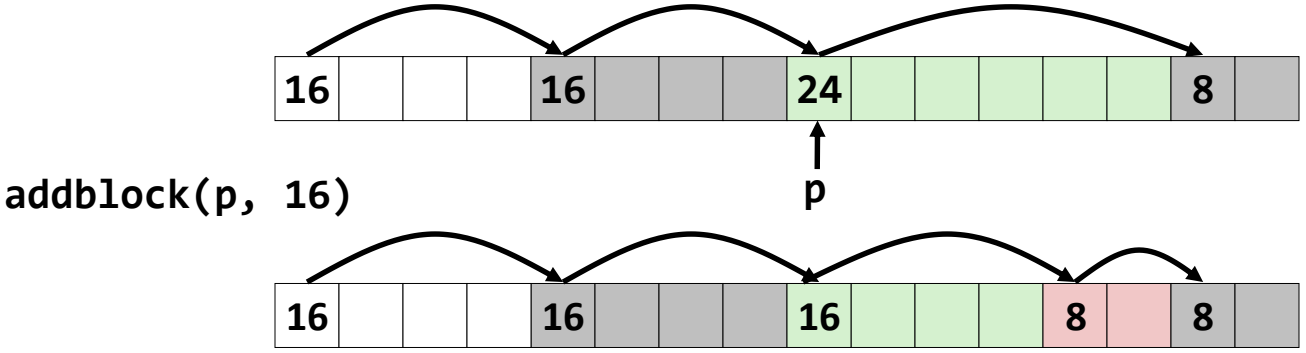
```
p = start;
while ((p < end) &&      \\ пока не дошли до конца
       ((*p & 1) ||      \\ уже выделен
       (*p < len)))      \\ маловато будет
  p = p + (*p & -2);     \\ переходим на следующий блок
```

Здесь и далее приводится Си-подобный псевдокод

  - Выделение за линейное время
  - На практике может вызывать «дробление» блоков в начале списка
- *Следующий подходящий:*
  - Аналогично предыдущему, поиск продолжается с позиции на которой он остановился ранее
  - Как правило работает быстрее: не происходит повторного просмотра неподходящих блоков
  - Некоторые исследования допускают худшую фрагментацию
- *Наилучший:*
  - Просмотр всего списка, выбор ***наилучшего*** свободного блока
    - меньше всего байт сверх запрошенного размера
  - Небольшой размер незанятых фрагментов
  - Как правило, работает медленнее, чем *первый подходящий*

Неявный список
Выделение свободного блока

- Выделение свободного блока: *расщепление*
  - Если размер требуемой памяти меньше, чем доступное в свободном блоке пространство, блок можно расщепить



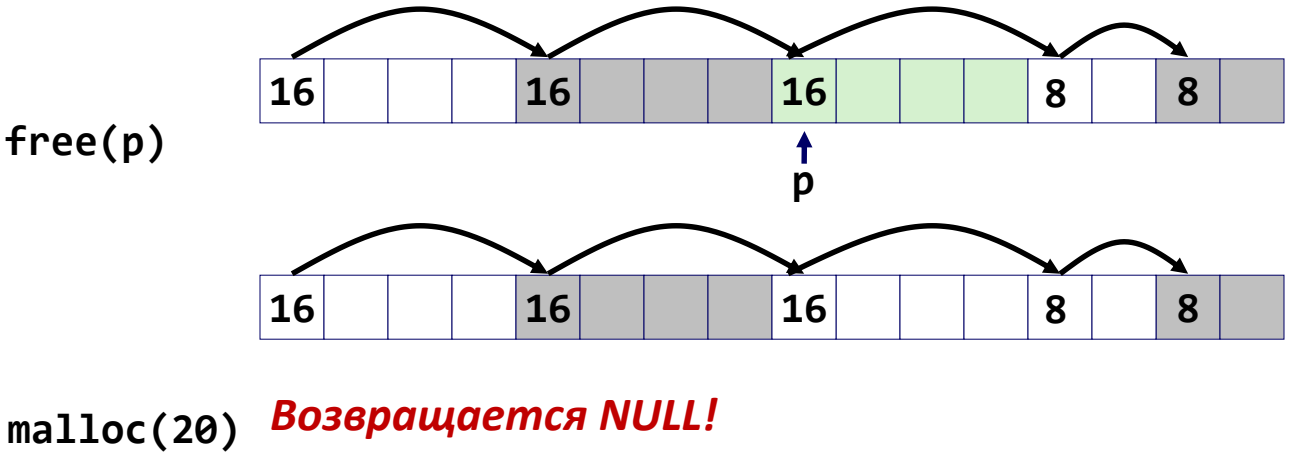

```
void addblock(ptr p, int len) {
  int newsize = ((7 + len) >> 3) << 3;   // «выравниваем вверх» по
                                         // 8 байтной границе
  int oldsize = *p & -2;                 // маскируем и считываем размер
  *p = newsize | 1;                      // выставляем новую длину блока
  if (newsize < oldsize)
    *(p + newsize) = oldsize - newsize;  // выставляем длину нового блока
}
```

Неявный список
Освобождение блока

- Невероятно простая реализация!
  - Всего лишь нужно сбросить флаг, показывающий выделен блок или свободен

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

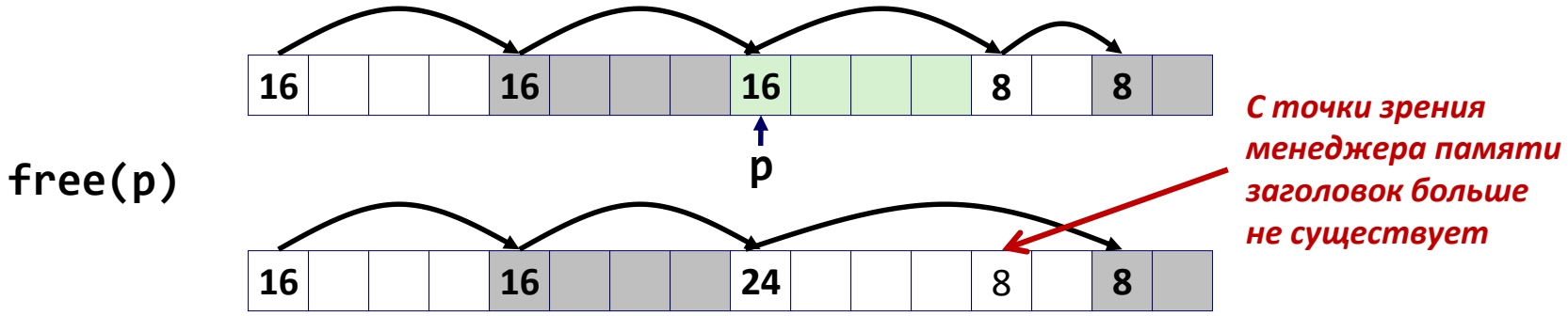
  - К сожалению, приходим к «ложной фрагментации»



Несмотря на то, что свободное пространство есть, менеджер памяти его не в состоянии найти

Неявный список
Слияние

- Объедение *(слияние)* со следующим/предыдущим блоком, если он свободен
  - Слияние со следующим блоком

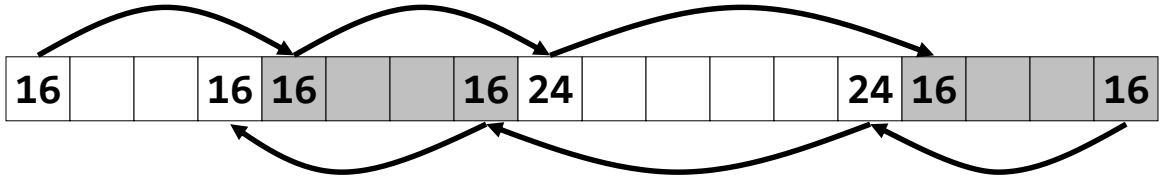



```
void free_block(ptr p) {
    *p = *p & -2;              // сбрасываем флаг
    next = p + *p;             // находим следующий блок
    if ((*next & 1) == 0)      // если он свободен
      *p = *p + *next;         // добавляем его к текущему блоку
}
```

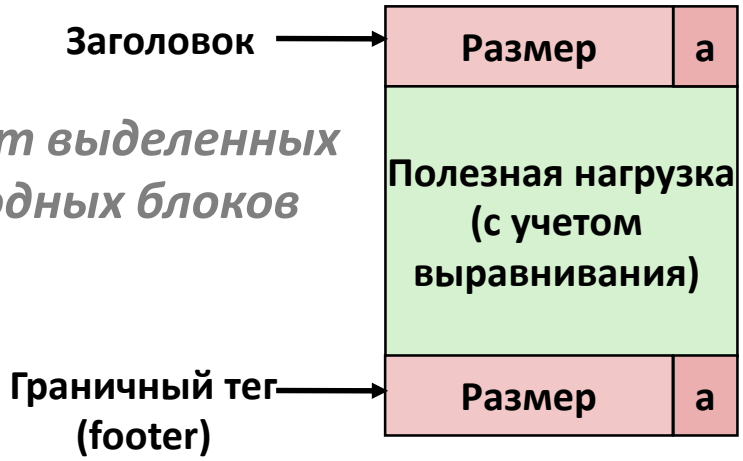
  - Как провести слияние с *предыдущим* блоком?

Неявный список
Двунаправленное слияние

- *Граничные теги* [Кнут 73]
  - Повторяем заголовок (размер/флаг) в конце блока
  - Появляется возможность проходить список в обратном направлении за счет дополнительного расходования памяти
  - Общеупотребительный технический прием



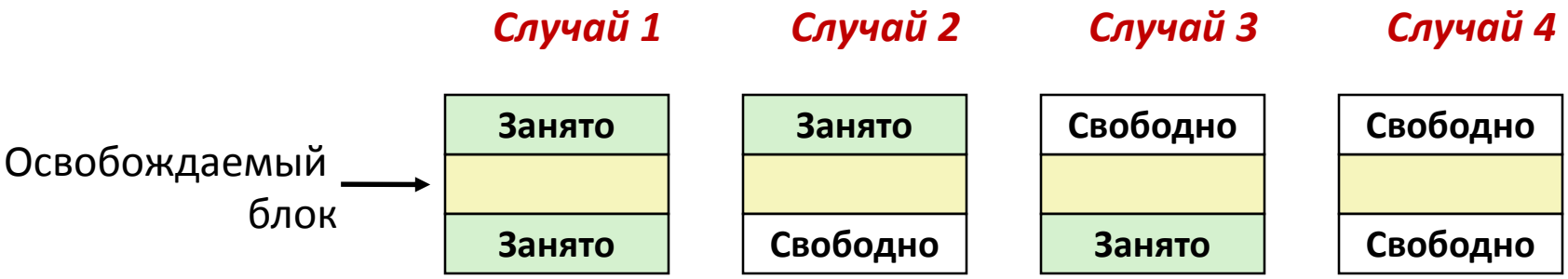
Формат выделенных и свободных блоков



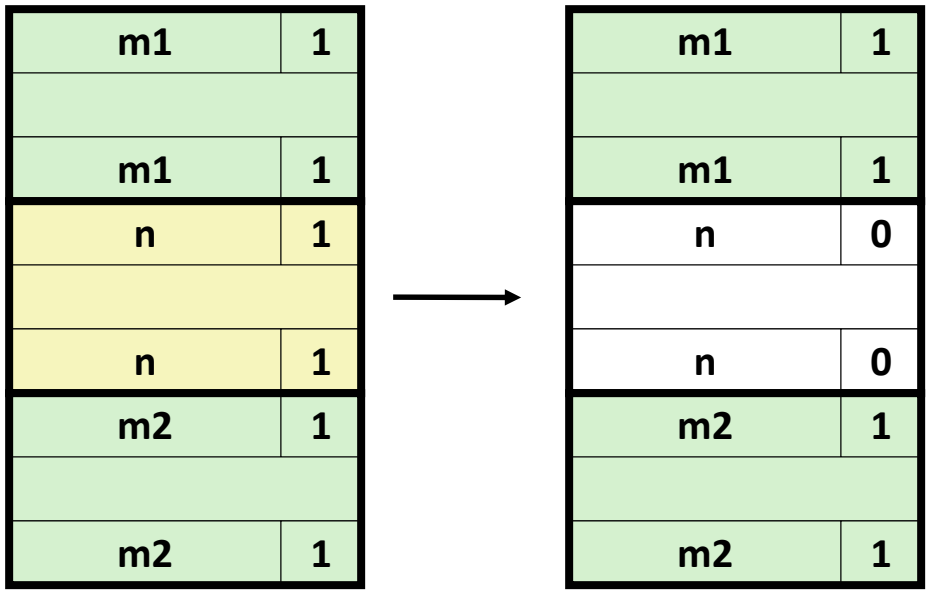
a = 1: Блок занят
a = 0: Блок свободен

Размер: Общий размер всего блока

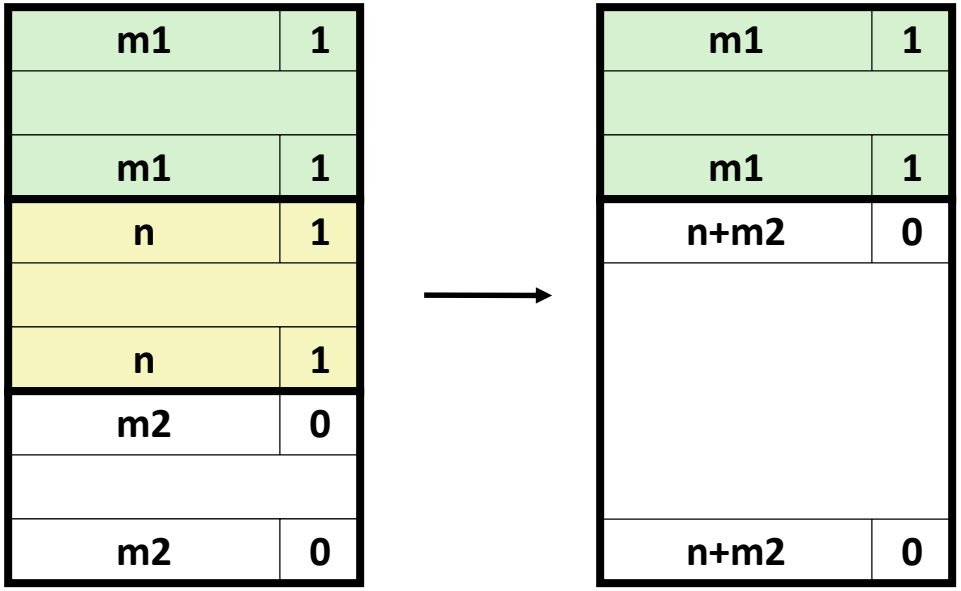
Слияние за фиксированное время



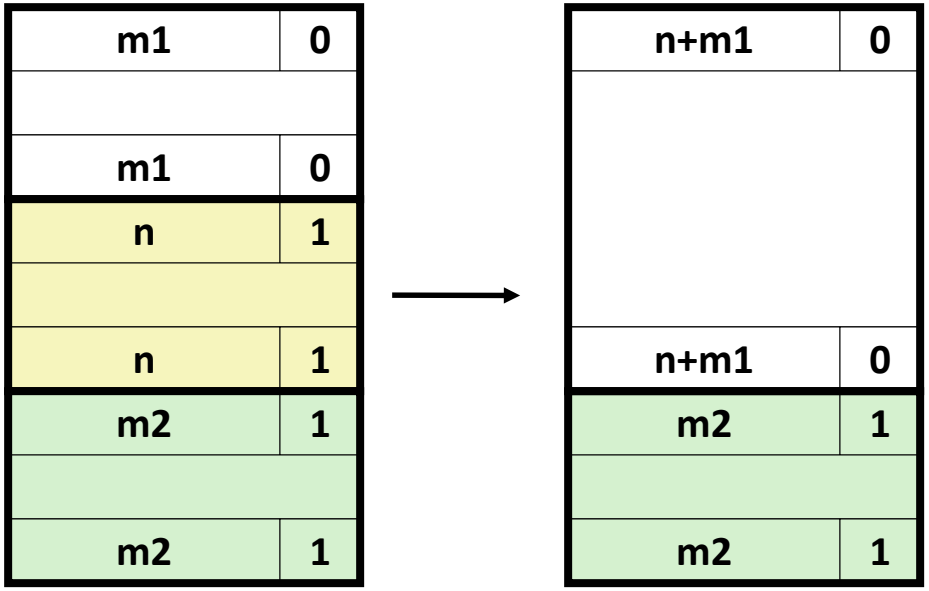
Слияние за фиксированное время (Случай 1)



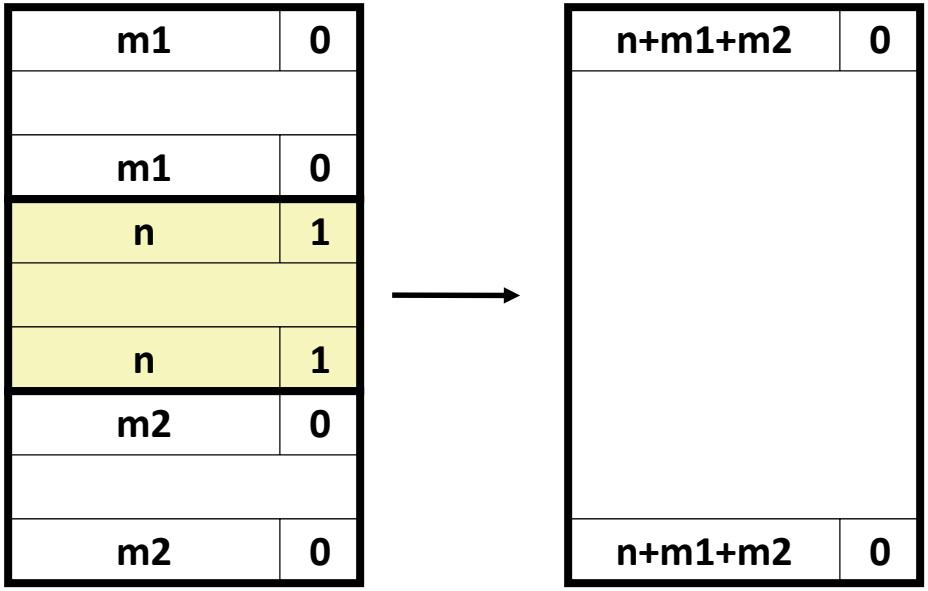
Слияние за фиксированное время (Случай 2)



Слияние за фиксированное время (Случай 3)



Слияние за фиксированное время (Случай 4)



Недостатки Граничных Тегов

- Внутренняя фрагментация

- Есть ли возможности для оптимизации?
  - Каким блокам нужен тег нижней границы?
  - … И что это значит?

Промежуточные итоги
Ключевые правила выделения памяти

- Правила размещения:
  - Первый подходящий, следующий подходящий, наилучший, и др.
  - Компромисс между пропускной способностью и фрагментацией
  - ***Дальнейший материал*: раздельные списки свободных блоков приближение к поиску наилучшего блока без просмотра всего списка свободных блоков**
- Правила расщепления:
  - При каких условиях следует расщеплять свободные блоки?
  - До какого уровня может быть доведена внутренняя фрагментация?
- Правила слияния:
  - ***Безотлагательное слияние:*** выполняем слияние каждый раз, когда вызываем функцию `free`
  - ***Отложенное слияние:*** можно попытаться улучшить производительность функции `free`, откладывая слияние на некоторое время. Примеры:
    - Объединяем при просмотре списка свободных блоков во время вызова функции `malloc`
    - Объединяем когда внешняя фрагментация достигает некоторого порогового значения

Промежуточные итоги
Неявные списки

- Реализация: крайне простая
- Стоимость выделения памяти:
  - в худшем случае линейная сложность (время)
- Стоимость освобождения:
  - константное время
  - даже при выполнении слияния!
- Использование памяти:
  - зависит от правил (политики) размещения данных в свободных блоках
  - Первый подходящий, следующий подходящий, или наилучший

- На практике `malloc/free` не используют этот метод по причине линейной сложности, возникающей при выделении памяти
  - используется во многих других случаях

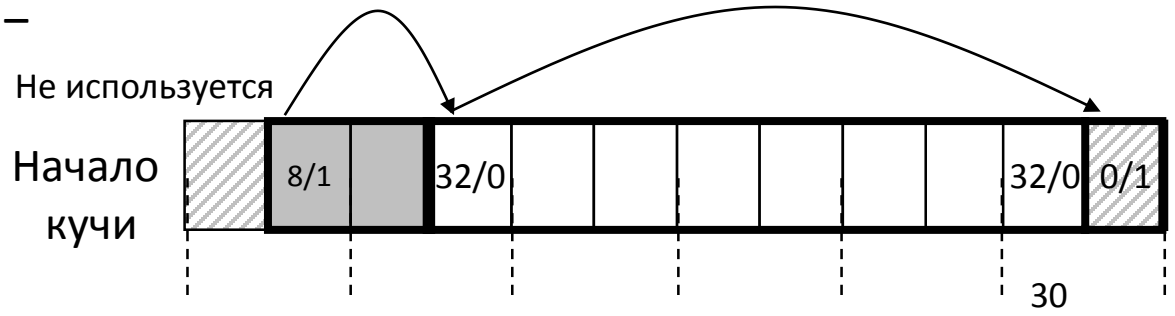
- Тем не менее, идеи расщепления, граничных тегов и слияния используются во *всех* менеджерах динамической памяти

Задача на моделирование работы менеджера динамической памяти

- Размер кучи – 12 четырехбайтных слов
- Неявный список
- Размер в заголовке и граничном теге
- В выделенных блоках граничный тег не используется
- Память выравнивается по 8-ми байтной границе
- Поиск свободного блока:
  с начала / с текущей позиции
- Выбирается первый подходящий свободный блок
- При расщеплении используется 1я часть
- Слияние проводится незамедлительно
- Первый выделенный блок – служебный, неудаляемая «голова» списка

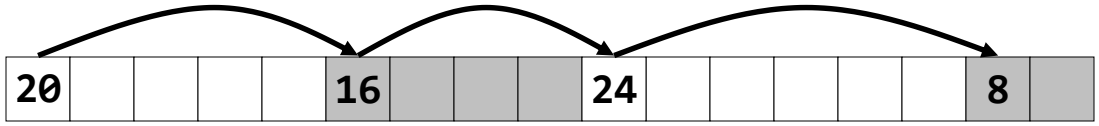
- Требуется определить
  - Состояние кучи после выполнения запросов
    1. p1=malloc(5)
    2. p2=malloc(11)
    3. free(p1)
    4. p3=malloc(4)
    5. p4=malloc(5)
    6. free(p2)
  - Пиковое использование памяти U_6

Начальное состояние кучи

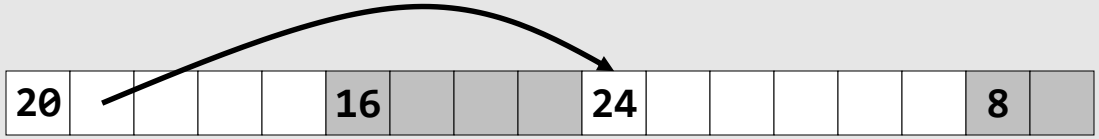


Как отслеживать свободные блоки

- Метод 1: *неявный список* с использованием длины блока



- Метод 2: *Явный список* свободных блоков с использованием указателей



- Метод 3: *Раздельные списки*
  - Распределение блоков по раздельным спискам, исходя из размеров этих блоков

- Метод 4: *Сортировка блоков по размеру*
  - Можно использовать сбалансированное дерево (например, Красно-Черные деревья) с указателями в каждом свободном блоке, и с длиной блока в качестве ключа

Явный список свободных блоков

Занятый блок (как и ранее)

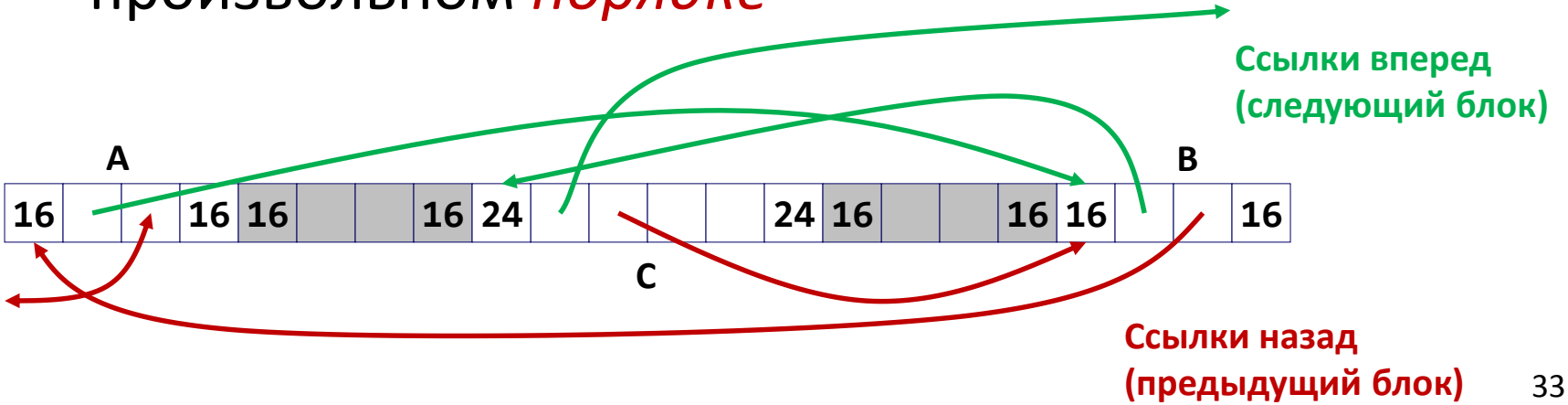
Свободный

- Поддерживаем список (списки) *свободных* блоков, а не *всех* существующих в памяти на данный момент
  - «Следующий» свободный блок может быть где угодно
    - Необходимо поддерживать не только размер текущего блока, но и указатели в оба направления: вперед и назад
  - Граничные теги все также необходимы для слияния
  - Поскольку отслеживаются только свободные блоки, можно хранить указатели в пространстве, отведенном под полезную нагрузку

Явный список свободных блоков

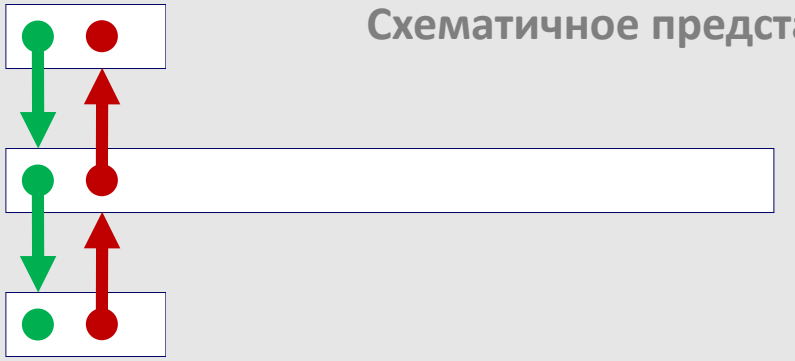
- Логическая организация

- Физическое размещение: блоки могут быть размещены в произвольных *местах* и в произвольном *порядке*

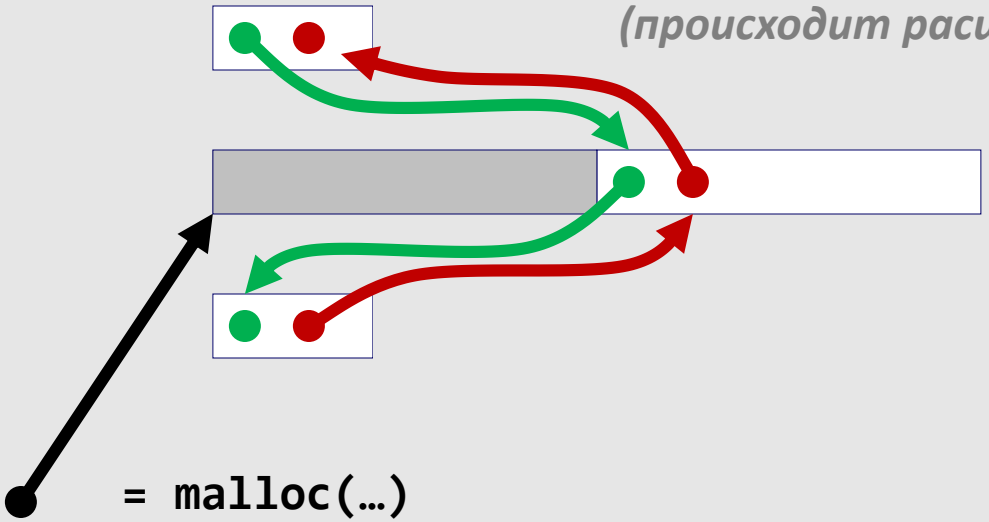


Явный список свободных блоков
Выделение памяти

До



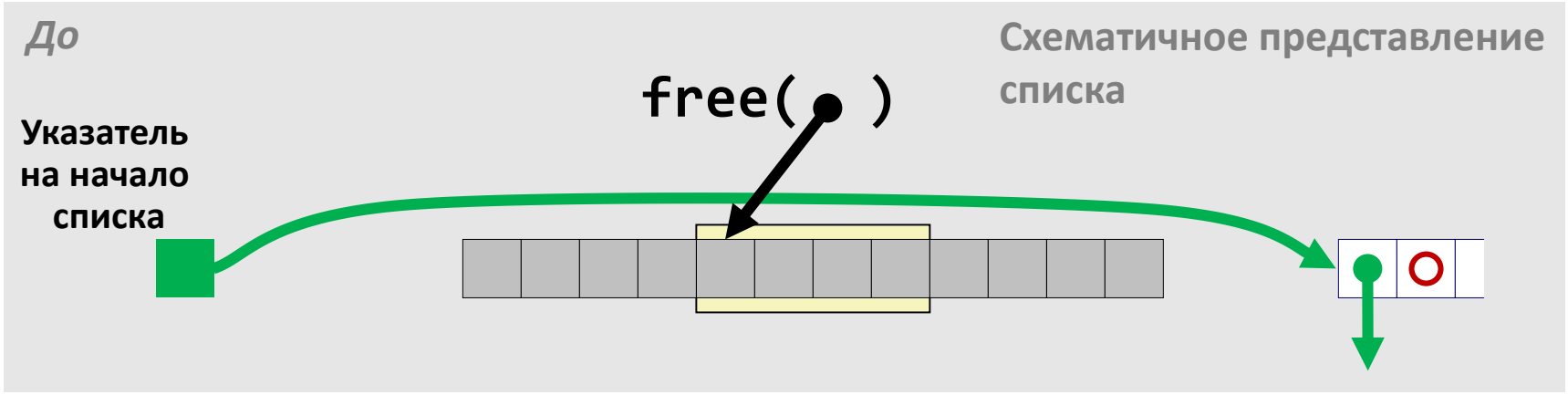
После



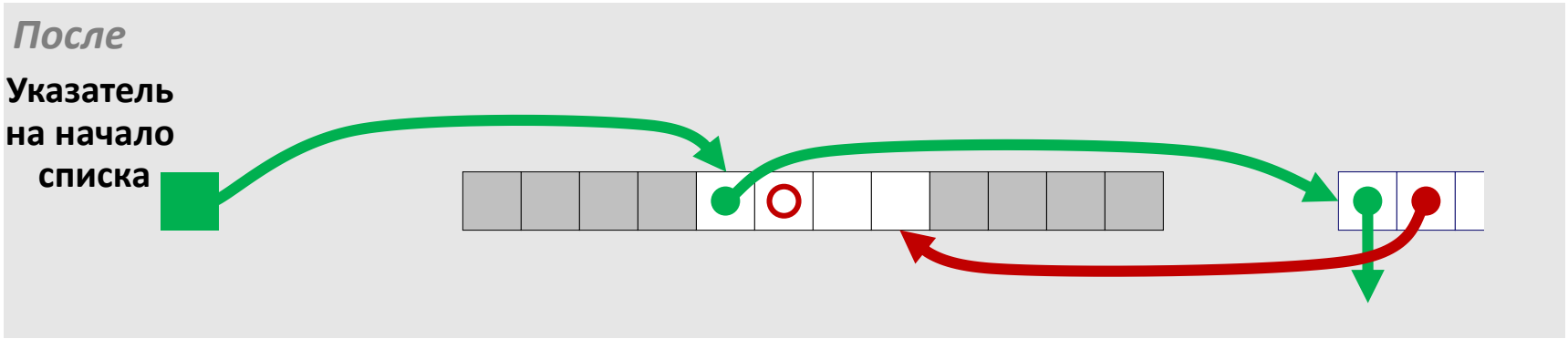
Явный список свободных блоков Освобождение памяти

- *Правила вставки блока*: В какое место списка следует поместить освобожденный блок?
  - **В порядке LIFO (last-in-first-out)**
    - Помещаем освобожденный блок в начало списка
    - ***За:*** простота реализации и константное время работы
    - ***Против:*** Исследования показывают, что возникает более сильная фрагментация по сравнению с тем, когда блоки упорядочены по адресам
  - **В порядке следования адресов**
    - Помещаем в список освобожденный блок так, что список всегда поддерживает упорядоченность по адресам:
      addr(prev) < addr(curr) < addr(next)
    - ***Против:*** необходимо искать место вставки
    - ***За:*** см. вопрос фрагментации для дисциплины LIFO

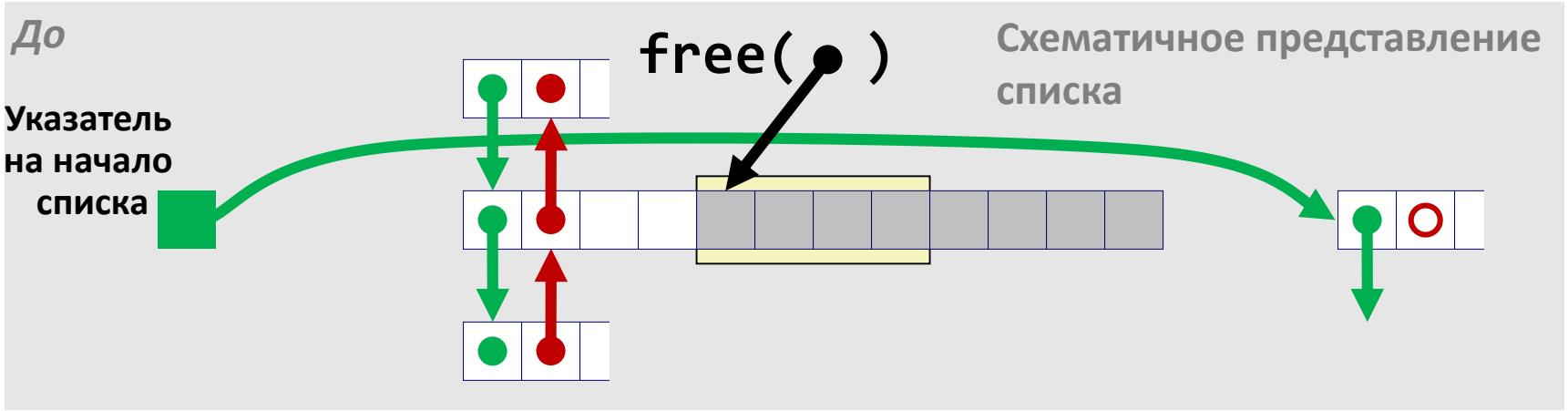
Освобождение блока в порядке LIFO (Случай 1)



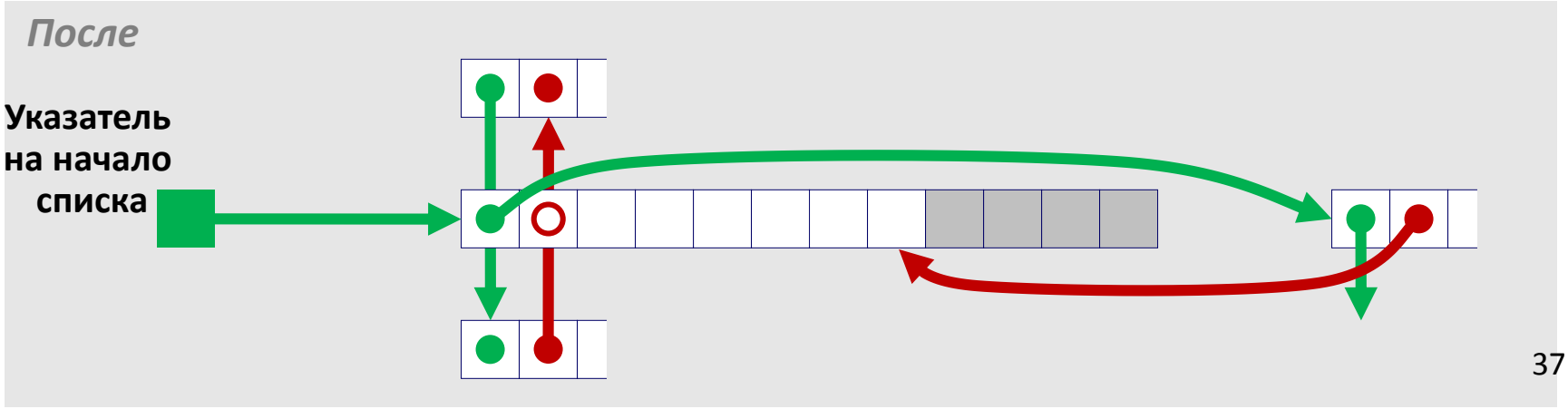
- Помещаем освобожденный блок в начало списка



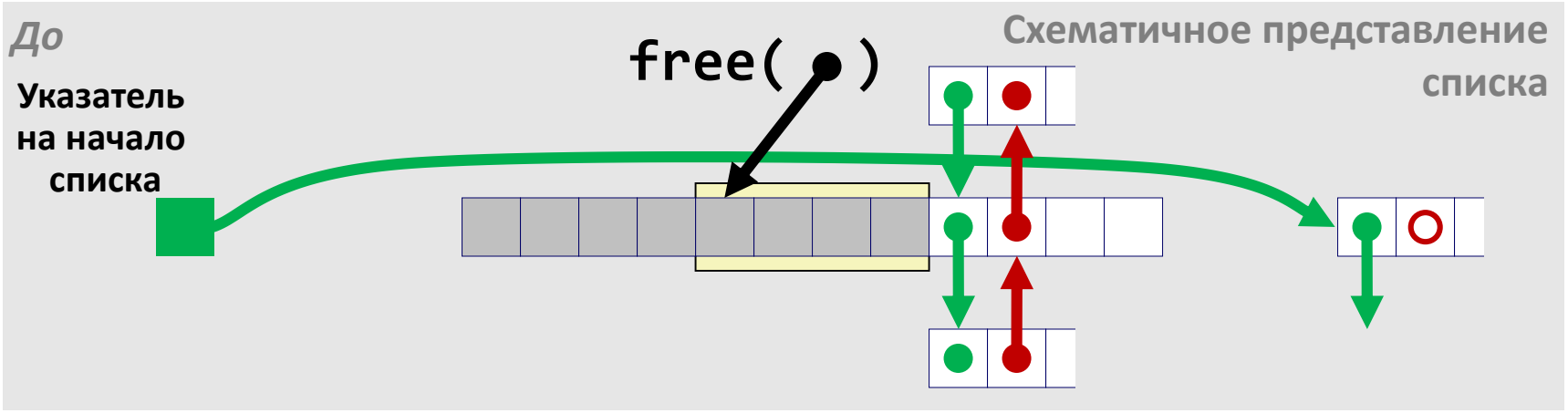
Освобождение блока в порядке LIFO (Случай 2)



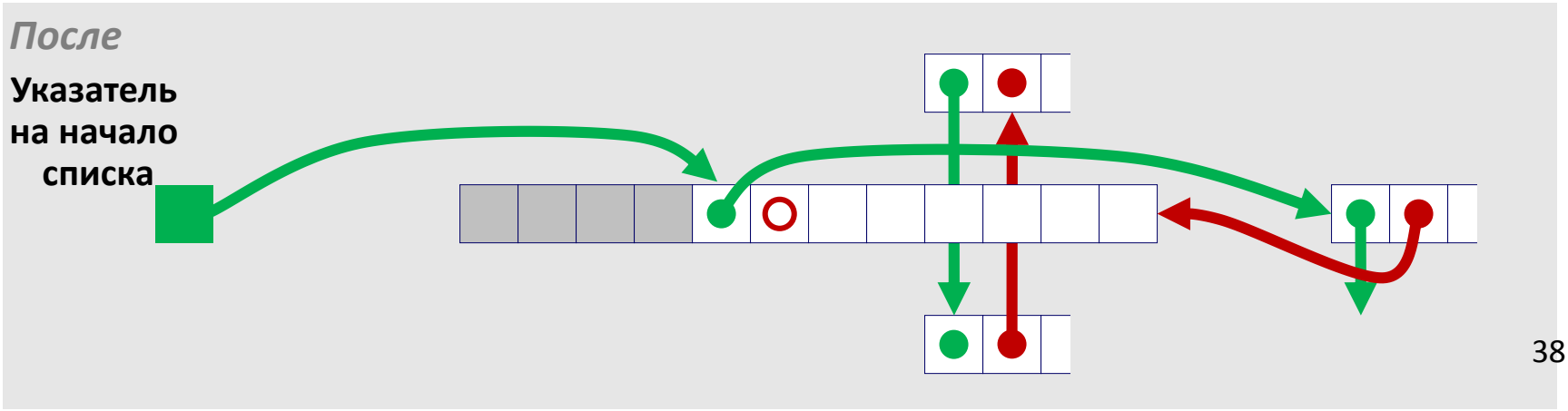
- Извлекаем из списка смежный (перед освобождаемым) в памяти блок, выполняем слияние, и вставляем образовавшийся блок в начало списка



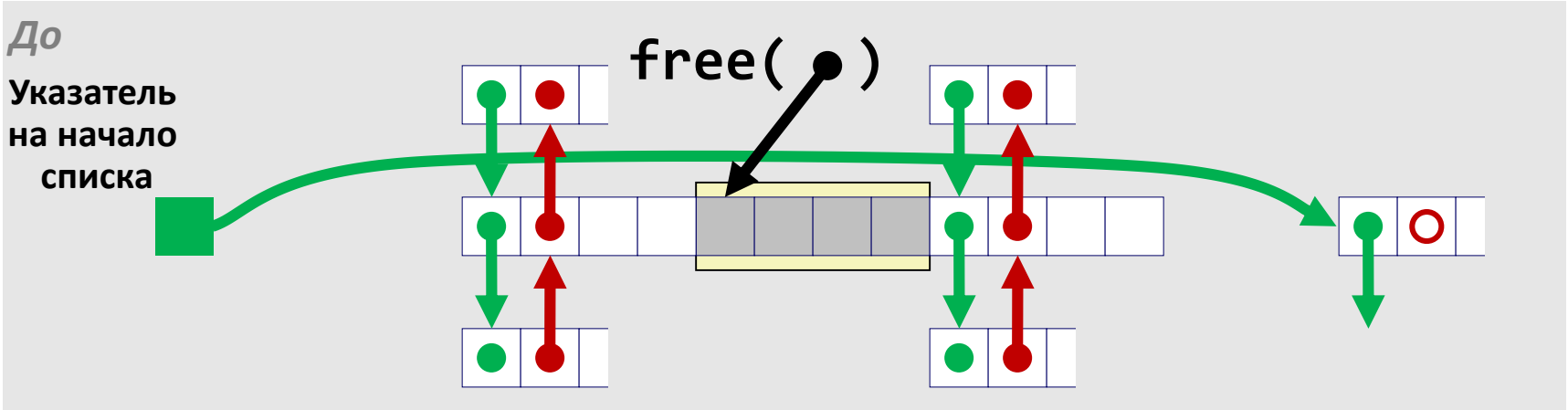
Освобождение блока в порядке LIFO (Случай 3)



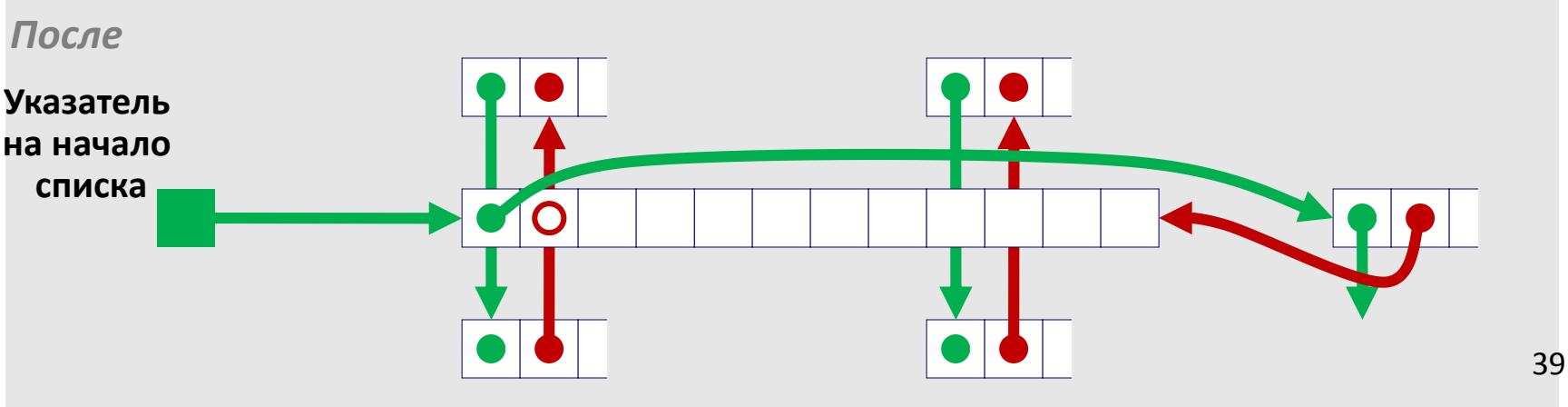
- Извлекаем из списка смежный (после освобождаемого) в памяти блок, выполняем слияние, и вставляем образовавшийся блок в начало списка



Освобождение блока в порядке LIFO (Случай 4)



- Извлекаем из списка смежные блоки, выполняем слияние трех блоков, и вставляем образовавшийся блок в начало списка



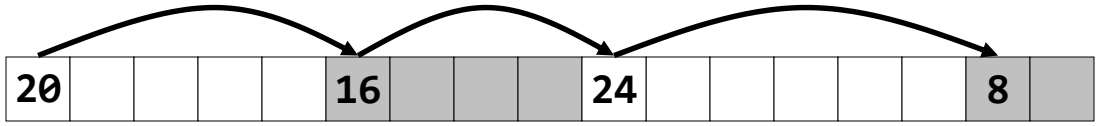
Промежуточные итоги
Явный список

- В сравнении с неявным списком:
  - Выделение памяти занимает «линейное время» от числа ***свободных***, а не ***всех*** блоков
    - ***Гораздо быстрее*** работает, когда большая часть памяти занята
  - Незначительно усложнилось выделение и освобождение блоков, поскольку необходимо извлекать и добавлять элементы в список
  - Требуется дополнительное место для размещения указателей (2 машинных слова на каждый блок)
    - Увеличивается при этом внутренняя фрагментация?

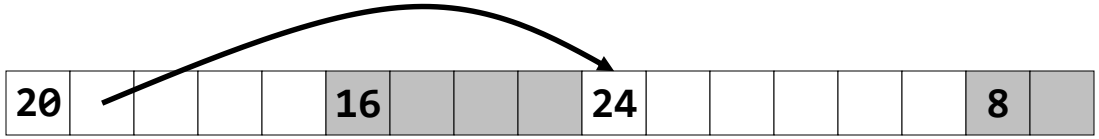
- Как правило подход с поддержкой явного списка комбинируют с разделением блоков по нескольким спискам
  - Блоки разделяют на несколько классов, в зависимости от их размера

Как отслеживать свободные блоки

- Метод 1: *неявный список* с использованием длины блока



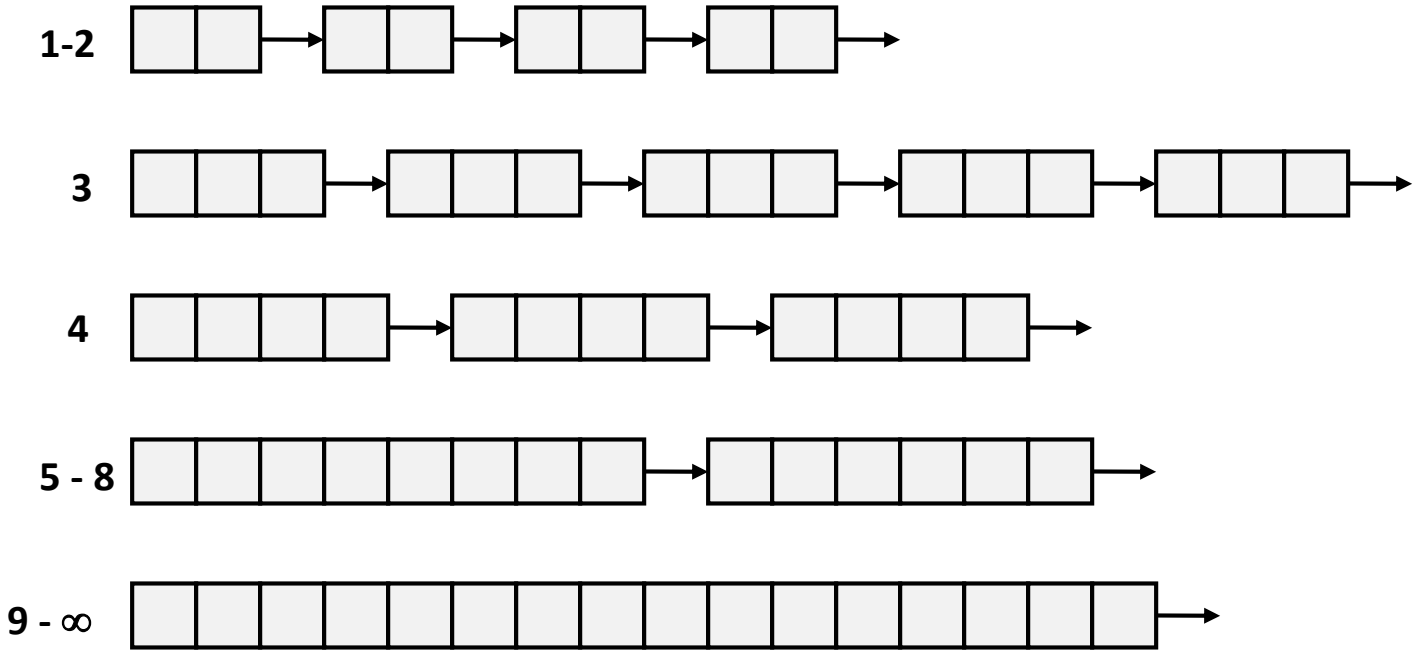
- Метод 2: *Явный список* свободных блоков с использованием указателей



- Метод 3: *Раздельные списки*
  - Распределение блоков по раздельным спискам, исходя из размеров этих блоков
- Метод 4: *Сортировка блоков по размеру*
  - Можно использовать сбалансированное дерево (например, Красно-Черные деревья) с указателями в каждом свободном блоке, и с длиной блока в качестве ключа

Раздельные списки (Seglist)

- Блоки каждого *класса* образуют отдельный список



- Для блоков малого размера заводят по отдельному классу для каждого размера
- Для блоков достаточного большого размера границы классов идут по степеням двойки

Выделение памяти по методу Seglist

- Дан массив список, для каждого класса блоков
- Чтобы выделить блок размера *n* байт:
  - В соответствующем списке ищем блок размера $m > n$
  - Если подходящий блок найден:
    - Расщепляем блок и помещаем оставшийся фрагмент в список соответствующего класса
  - Если блок найти не удалось, ищем его в списке следующего класса
  - Повторяем до тех пор, пока не найдем
- Если после просмотра всех списков блок так и не найден:
  - Запрашиваем у ОС дополнительную память для кучи (используя функцию `sbrk()`)
  - В предоставленной памяти создаем блок размера *n* байт
  - Всю оставшуюся память занимаем одним свободным блоком и помещаем его в список класса наибольших по размеру блоков (из числа подходящих).

Выделение памяти по методу Seglist

- Чтобы освободить блок:
  - При необходимости выполняем слияние и помещаем блок в список подходящего класса размеров
- Преимущества метода Seglist
  - Более высокая пропускная способность
    - Логарифмическая сложность поиска для классов большого размера (граница по степеням двойки)
  - Лучшее использование памяти
    - Поиск первого подходящего в раздельных списках показывает результаты, схожие с поиском наилучшего в рамка всей кучи
    - Предельная ситуация: если для каждого размера блока завести отдельный класс эффективность расходования памяти будет совпадать с поиском наилучшего

Далее ...

- *Динамическая память*
  - *Организация и управление*
  - *Численные характеристики*
  - *Управление свободными блоками*
- ***Числа с плавающей точкой***
  - ***Представления для вещественных чисел***
    - ***Дробные двоичные числа***
    - ***Числа с плавающей точкой***
  - ***Сопроцессор x87***
    - ***Устройство***
    - ***Примеры программ***