CS107, Lecture 7
Stack and Heap

Reading: K&R 5.6-5.9 or Essential C section 6 on the heap
Lecture Plan

• **Misc. topics: const, structs and the ternary operator**
• **Recap:** Pointers So Far
• The Stack
• The Heap and Dynamic Memory
• **Practice:** Pig Latin + Valgrind
• realloc

```bash
cp -r /afs/ir/class/cs107/lecture-code/lect7 .
```
• `const` is a keyword that indicates that a particular variable in a particular scope should not be modified.

• In 107, you won’t have to declare many `const` variables, but you will be provided parameters or use functions that have it.
You can use `const` to declare global constants in your program. This indicates the variable cannot change after being created. This makes an actual variable, whereas `#define` does not; `#define` is like “find-and-replace”.

```c
const double PI = 3.1415;
const int DAYS_IN_WEEK = 7;

int main(int argc, char *argv[]) {
    ...
    if (x == DAYS_IN_WEEK) {
        ...
    }
    ...
}
```
Use `const` with pointers to indicate that the data that is pointed to cannot be changed using that pointer. *It’s not protection for that memory in general – it’s just preventing modification using the const pointer.*

```c
char str[6];
strcpy(str, "Hello");
const char *s = str;

// Cannot use s to change characters it points to
s[0] = 'h';

// But we can still use str to change them
str[0] = 'h';
```
Sometimes we use `const` with pointer parameters to indicate that the function will not / should not change what it points to. The actual pointer can be changed, however.

```c
// This function promises to not change str’s characters
int countUppercase(const char *str) {
    int count = 0;
    for (int i = 0; i < strlen(str); i++) {
        if (isupper(str[i])) {
            count++;
        }
    }
    return count;
}
```
By definition, C gets upset when you set a **non-const** pointer equal to a **const** pointer. You need to be consistent with **const** to reflect what you cannot modify.

```c
// This function promises to not change str’s characters
int countUppercase(const char *str) {
    // compiler warning and error
    char *strToModify = str;
    strToModify[0] = …
}
```
By definition, C gets upset when you set a non-\texttt{const} pointer equal to a \texttt{const} pointer. You need to be consistent with \texttt{const} to reflect what you cannot modify. Think of \texttt{const} as part of the variable type.

// This function promises to not change str’s characters
int countUppercase(const char *str) {
    const char *strToModify = str;
    __strToModify[0] = …
}


**Const**

`const` can be confusing to interpret in some variable types.

```cpp
// cannot modify this char
const char c = 'h';

// cannot modify chars pointed to by str
const char *str = ...

// cannot modify chars pointed to by *strPtr
const char **strPtr = ...
```
A *struct* is a way to define a new variable type that is a group of other variables.

```c
struct date {
    int month;
    int day;
};
```

```c
struct date today;  // construct structure instances
today.month = 1;
today.day = 28;
```

```c
struct date new_years_eve = {12, 31};  // shorter initializer syntax
```
Wrap the struct definition in a `typedef` to avoid having to include the word `struct` every time you make a new variable of that type.

```c
typedef struct date {
    int month;
    int day;
} date;
...

date today;
today.month = 1;
today.day = 28;

date new_years_eve = {12, 31};
```
If you pass a struct as a parameter, like for other parameters, C passes a **copy** of the entire struct.

```c
void advance_day(date d) {
    d.day += 1;
}

int main(int argc, char *argv[]) {
    date my_date = {1, 28};
    advance_day(my_date);
    printf("%d", my_date.day); // 28
    return 0;
}
```
If you pass a struct as a parameter, like for other parameters, C passes a copy of the entire struct. **Use a pointer to modify a specific instance.**

```c
void advance_day(date *d) {
    (*d).day++;
}

int main(int argc, char *argv[]) {
    date my_date = {1, 28};
    advance_day(&my_date);
    printf("%d", my_date.day); // 29
    return 0;
}
```
The **arrow** operator lets you access the field of a struct pointed to by a pointer.

```c
void advance_day(date *d) {
    d->day++; // equivalent to (*d).day++;
}

int main(int argc, char *argv[]) {
    date my_date = {1, 28};
    advance_day(&my_date);
    printf("%d", my_date.day); // 29
    return 0;
}
```
C allows you to return structs from functions as well. It returns whatever is contained within the struct.

date create_new_years_date() {
    date d = {1, 1};
    return d;       // or return (date){1, 1};
}

int main(int argc, char *argv[]) {
    date my_date = create_new_years_date();
    printf("%d", my_date.day); // 1
    return 0;
}
**Structs**

`sizeof` gives you the entire size of a struct, which is the sum of the sizes of all its contents.

```c
typedef struct date {
    int month;
    int day;
} date;

int main(int argc, char *argv[]) {
    int size = sizeof(date);  // 8
    return 0;
}
```
Arrays of Structs

You can create arrays of structs just like any other variable type.

typedef struct my_struct {
    int x;
    char c;
} my_struct;

...

my_struct array_of_structs[5];
Arrays of Structs

To initialize an entry of the array, you must use this special syntax to confirm the type to C.

```c
typedef struct my_struct {
    int x;
    char c;
} my_struct;

my_struct array_of_structs[5];
array_of_structs[0] = (my_struct){0, 'A'};
```
Arrays of Structs

You can also set each field individually.

typedef struct my_struct {
    int x;
    char c;
} my_struct;

... my_struct array_of_structs[5];
array_of_structs[0].x = 2;
array_of_structs[0].c = 'A';
The ternary operator is a shorthand for using if/else to evaluate to a value.

```
int x;
if (argc > 1) {
    x = 50;
} else {
    x = 0;
}
```

// equivalent to
```
int x = argc > 1 ? 50 : 0;
```
CS107 Topic 3: How can we effectively manage all types of memory in our programs?
How can we effectively manage all types of memory in our programs?

Why is answering this question important?

• Shows us how we can pass around data efficiently with pointers (last time)
• Introduces us to the heap and allocating memory that we manually manage (this time)

**assign3**: implement a function using resizable arrays to read lines of any length from a file and write 2 programs using that function to print the last N lines of a file and print just the unique lines of a file. These programs emulate the `tail` and `uniq` Unix commands!
Learning Goals

• Learn about the differences between the stack and the heap and when to use each one

• Become familiar with the `malloc`, `calloc`, `realloc` and `free` functions for managing memory on the heap
Lecture Plan

- **Recap:** Pointers So Far
- The Stack
- The Heap and Dynamic Memory
- **Practice:** Pig Latin + Valgrind
- realloc
Lecture Plan

• Recap: Pointers So Far
  • The Stack
  • The Heap and Dynamic Memory
• Practice: Pig Latin + Valgrind
• realloc

cp -r /afs/ir/class/cs107/lecture-code/lect7.
• If you are performing an operation with some input and do not care about any changes to the input, **pass the data type itself**.

• If you are modifying a specific instance of some value, **pass the location** of what you would like to modify.

• If a function takes an address (pointer) as a parameter, it can **go to** that address if it needs the actual value.

• Strings are one application of pointers, and they can help us understand pointers more generally.
When you do pointer arithmetic, you are adjusting the pointer by a certain *number of places* (e.g. characters).

```c
char *str = "apple";  // e.g. 0xff0
char *str1 = str + 1;  // e.g. 0xff1
char *str3 = str + 3;  // e.g. 0xff3

printf("%s", str);    // apple
printf("%s", str1);   // pple
printf("%s", str3);   // le
```

<table>
<thead>
<tr>
<th>Address</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xff0</td>
<td>'a'</td>
</tr>
<tr>
<td>0xff1</td>
<td>'p'</td>
</tr>
<tr>
<td>0xff2</td>
<td>'p'</td>
</tr>
<tr>
<td>0xff3</td>
<td>'l'</td>
</tr>
<tr>
<td>0xff4</td>
<td>'e'</td>
</tr>
<tr>
<td>0xff5</td>
<td>'\0'</td>
</tr>
</tbody>
</table>
Pointer Arithmetic

Pointer arithmetic does not work in bytes. Instead, it works in the size of the type it points to.

```
// nums points to an int array
int *nums = … // e.g. 0xff0
int *nums1 = nums + 1; // e.g. 0xff4
int *nums3 = nums + 3; // e.g. 0xffc

printf("%d", *nums); // 52
printf("%d", *nums1); // 23
printf("%d", *nums3); // 34
```
Pointer Arithmetic

Pointer arithmetic does not work in bytes. Instead, it works in the size of the type it points to.

// nums points to an int array
int *nums = ... // e.g. 0xff0
int *nums3 = nums + 3; // e.g. 0xffff
int *nums2 = nums3 - 1; // e.g. 0xff8

printf("%d", *nums);  // 52
printf("%d", *nums2);  // 12
printf("%d", *nums3);  // 34
Pointer arithmetic with two pointers does *not* give the byte difference. Instead, it gives the number of *places* they differ by.

```c
// nums points to an int array
int *nums = ... // e.g. 0xff0
int *nums3 = nums + 3; // e.g. 0xffc
int diff = nums3 - nums; // 3
```

<table>
<thead>
<tr>
<th>Address</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1004</td>
<td>1</td>
</tr>
<tr>
<td>0x1000</td>
<td>16</td>
</tr>
<tr>
<td>0xffc</td>
<td>34</td>
</tr>
<tr>
<td>0xff8</td>
<td>12</td>
</tr>
<tr>
<td>0xff4</td>
<td>23</td>
</tr>
<tr>
<td>0xff0</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
Sometimes, we would like to modify a string’s pointer itself, rather than just the characters it points to. E.g. we want to write a function `skipSpaces` that modifies a string pointer to skip past any initial spaces. What should go in each of the blanks?

```c
void skipSpaces(char **strPtr) {
    int numSpaces = strspn(*strPtr, " ");
    *strPtr += numSpaces;
}

int main(int argc, char *argv[]) {
    char *str = "    hello"
    skipSpaces(&str);
    printf("%s", str);
    // should print "hello"
}
```

We are modifying a specific instance of the string pointer, so we pass the location of the string pointer we would like to modify.
Lecture Plan

• **Recap:** Pointers So Far
• **The Stack**
• The Heap and Dynamic Memory
• **Practice:** Pig Latin + Valgrind
• realloc

```
cp -r /afs/ir/class/cs107/lecture-code/lect7 .
```
• We are going to dive deeper into different areas of memory used by our programs.

• The **stack** is the place where all local variables and parameters live for each function. A function’s stack “frame” goes away when the function returns.

• The stack grows **downwards** when a new function is called and shrinks **upwards** when the function is finished.
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
```c
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
```
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
```c
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
```
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
The Stack

```c
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char **argv) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
```

Memory:
- `main`: a: 42, argc: 1
- `func1`: b: 17, argv: 0xffff0
- `func2`: c: 99, d: 0

Stack:
- 0x0
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done.");
    return 0;
}
```c
void func2() {
    int d = 0;
}

void func1() {
    int c = 99;
    func2();
}

int main(int argc, char *argv[]) {
    int a = 42;
    int b = 17;
    func1();
    printf("Done. ");
    return 0;
}
```
Each function call has its own stack frame for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own *stack frame* for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own *stack frame* for its own copy of variables.

```
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}
```

```
int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function call has its own stack frame for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own *stack frame* for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own **stack frame** for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}
```

```c
int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function call has its own stack frame for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own *stack frame* for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own *stack frame* for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own *stack frame* for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```

Returns 1
The Stack

Each function call has its own stack frame for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```

Returns 2
Each function **call** has its own *stack frame* for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}
```

```c
int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own **stack frame** for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```

Returns 24
Each function call has its own stack frame for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
Each function **call** has its own *stack frame* for its own copy of variables.

```c
int factorial(int n) {
    if (n == 1) {
        return 1;
    } else {
        return n * factorial(n - 1);
    }
}

int main(int argc, char *argv[]) {
    printf("%d", factorial(4));
    return 0;
}
```
• The stack behaves like a...well...stack! A new function call **pushes** on a new frame. A completed function call **pops** off the most recent frame.

• *Interesting fact:* C does not clear out memory when a function’s frame is removed. Instead, it just marks that memory as usable for the next function call. This is more efficient!

• A **stack overflow** is when you use up all stack memory. E.g. a recursive call with too many function calls.

• What are the limitations of the stack?
```c
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaa"
    return 0;
}
```
The Stack

```c
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaa"
    return 0;
}
```

Memory

- `main`: argc: 1, str: , argv: 0xfff0
- `argv`: 0xfff0
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str); // want "aaaa"
    return 0;
}
The Stack

char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str); // want "aaaa"
    return 0;
}
The Stack

```c
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaa"
    return 0;
}
```
The Stack

```c
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str); // want "aaaa"
    return 0;
}
```

Memory

- `main`
  - argc: 1
  - str: [ ]
  - argv: 0xffff0

- `create_string`
  - ch: 'a'
  - num: 4

new_str: 'a', 'a', 'a', 'a'

Returns e.g. 0xff50

Stack

- 0x0

char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaaa"
    return 0;
}
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str); // want "aaaa"
    return 0;
}
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaa"
    return 0;
}
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaa"
    return 0;
}

Sometimes, we can make the array in the caller and pass it as a parameter. But this isn't always possible if the size isn't known in advance.
This is a problem! We need a way to have memory that doesn’t get cleaned up when a function exits.
• **Recap:** Pointers So Far
• The Stack
• **The Heap and Dynamic Memory**
• **Practice:** Pig Latin + Valgrind
• realloc

```
cp -r /afs/ir/class/cs107/lecture-code/lect7 .
```
The Heap

```c
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);     // want "aaaa"
    return 0;
}
```

**Us:** hey C, is there a way to make this variable in memory that isn’t automatically cleaned up?
The Heap

```c
char *create_string(char ch, int num) {
    char new_str[num + 1];
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaa"
    return 0;
}
```

C: sure, but since I don’t know when to clean it up anymore, it’s your responsibility…
The Heap

• The **heap** is a part of memory that you can manage yourself.

• The **heap** is a part of memory below the stack that you can manage yourself. Unlike the stack, the memory only goes away when you delete it yourself.

• Unlike the stack, the heap grows **upwards** as more memory is allocated.

The heap is **dynamic memory** – memory that can be allocated, resized, and freed during **program runtime**.
Working with the heap consists of 3 core steps:

1. Allocate memory with malloc/realloc/strdup/calloc
2. Assert heap pointer is not NULL
3. Free when done

The heap is **dynamic memory**, so you may encounter many **runtime errors**, even if your code compiles!
void *malloc(size_t size);

To allocate memory on the heap, use the `malloc` function ("memory allocate") and specify the number of bytes you’d like.

• This function returns a pointer to the starting address of the new memory. It doesn’t know or care whether it will be used as an array, a single block of memory, etc.

• `void *` means a pointer to generic memory. You can set another pointer equal to it without any casting.

• The memory is not cleared out before being allocated to you!

• If `malloc` returns NULL, then there wasn’t enough memory for this request.
char *create_string(char ch, int num) {
    char *new_str = malloc(sizeof(char) * (num + 1));
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str); // want "aaaa"
    return 0;
}
The Heap

char *create_string(char ch, int num) {
    char *new_str = malloc(sizeof(char) * (num + 1));
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaaa"
    return 0;
}
The Heap

```c
char *create_string(char ch, int num) {
    char *new_str = malloc(sizeof(char) * (num + 1));
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char **argv) {
    char *str = create_string('a', 4);
    printf("%s", str); // want "aaaa"
    return 0;
}
```

Memory

- **Stack**
  - `main`: `argc: 1` and `str: 0xed0`
  - `argv: 0xffff0`

- **Heap**
  - `create_string`
    - `ch: 'a'` and `num: 4`
  - `new_str: 0xed0`
    - "\0" and 'a'

Returns e.g. 0xed0
char *create_string(char ch, int num) {
    char *new_str = malloc(sizeof(char) * (num + 1));
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str); // want "aaaaa"
    return 0;
}
char *create_string(char ch, int num) {
    char *new_str = malloc(sizeof(char) * (num + 1));
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str); // want "aaaa"
    return 0;
}
char *create_string(char ch, int num) {
    char *new_str = malloc(sizeof(char) * (num + 1));
    for (int i = 0; i < num; i++) {
        new_str[i] = ch;
    }
    new_str[num] = '\0';
    return new_str;
}

int main(int argc, char *argv[]) {
    char *str = create_string('a', 4);
    printf("%s", str);  // want "aaaaa"
    return 0;
}
Exercise: malloc multiples

Let’s write a function that returns an array of the first `len` multiples of `mult`.

```c
int *array_of_multiples(int mult, int len) {
    /* TODO: arr declaration here */
    for (int i = 0; i < len; i++) {
        arr[i] = mult * (i + 1);
    }
    return arr;
}
```

Line 2: How should we declare `arr`?

A. `int arr[len];`
B. `int arr[] = malloc(sizeof(int));`
C. `int *arr = malloc(sizeof(int) * len);`
D. `int *arr = malloc(sizeof(int) * (len + 1));`
E. Something else
Let's write a function that returns an array of the first `len` multiples of `mult`.

```c
int *array_of_multiples(int mult, int len) {
    /* TODO: arr declaration here */
    for (int i = 0; i < len; i++) {
        arr[i] = mult * (i + 1);
    }
    return arr;
}
```

Line 2: How should we declare `arr`?

A. `int arr[len];`
B. `int arr[] = malloc(sizeof(int));`
C. `int *arr = malloc(sizeof(int) * len);`
D. `int *arr = malloc(sizeof(int) * (len + 1));`
E. Something else

- Use a pointer to store the address returned by `malloc`.
- `Malloc`'s argument is the number of bytes to allocate.

⚠ This code is missing an assertion.
Let’s write a function that returns an array of the first \texttt{len} multiples of \texttt{mult}.

```c
int *array_of_multiples(int mult, int len) {
    int *arr = malloc(sizeof(int) * len);
    assert(arr != NULL);
    for (int i = 0; i < len; i++) {
        arr[i] = mult * (i + 1);
    }
    return arr;
}
```

- If an allocation error occurs (e.g. out of heap memory!), malloc will return NULL. This is an important case to check for robustness.
- \texttt{assert} will crash the program if the provided condition is false. A memory allocation error is significant, and we should terminate the program.
Other heap allocations: calloc

```c
void *calloc(size_t nmemb, size_t size);
```

calloc is like malloc that **zeros out** the memory for you—thanks, calloc!

- You might notice its interface is also a little different—it takes two parameters, which are multiplied to calculate the number of bytes (nmemb * size).

  ```c
  // allocate and zero 20 ints
  int *scores = calloc(20, sizeof(int));
  
  // alternate (but slower)
  int *scores = malloc(20 * sizeof(int));
  for (int i = 0; i < 20; i++) scores[i] = 0;
  ```

- calloc is more expensive than malloc because it zeros out memory. Use only when necessary!
Other heap allocations: strdup

```c
char *strdup(char *s);
```

`strdup` is a convenience function that returns a **null-terminated**, heap-allocated string with the provided text, instead of you having to `malloc` and copy in the string yourself.

```c
char *str = strdup("Hello, world!"); // on heap
str[0] = 'h';
```

You could imagine `strdup` might be implemented in terms of `malloc + strcpy`. 
void free(void *ptr);

• If we allocated memory on the heap and no longer need it, it is our responsibility to delete it.

• To do this, use the free command and pass in the starting address on the heap for the memory you no longer need.

• Example:

```c
char *bytes = malloc(4);
...
free(bytes);
```
Free

`void free(void *ptr);`

When you free an allocation, you are freeing up what it *points* to. You are not freeing the pointer itself. You can still use the pointer to point to something else.

```c
char *str = strdup("hello");
...
free(str);
str = strdup("hi");
```
Even if you have multiple pointers to the same block of memory, each memory block should only be freed **once**.

You must free the address you received in the previous allocation call; you cannot free just part of a previous allocation.

```c
char *bytes = malloc(4);
char *ptr = bytes;
...
free(bytes); ✔️
...
free(ptr);  ❌ Memory at this address was already freed!
```

```c
char *bytes = malloc(4);
char *ptr = malloc(10);
...
free(bytes);
...
free(ptr + 1); ❌
```
You may need to free memory allocated by other functions if that function expects the caller to handle memory cleanup.

```c
char *str = strdup("Hello!");
...
free(str); // our responsibility to free!
```
A memory leak is when you do not free memory you previously allocated.

```c
char *str = strdup("hello");
...
str = strdup("hi"); // memory leak! Lost previous str
```
Memory Leaks

• A memory leak is when you allocate memory on the heap, but do not free it.
• Your program should be responsible for cleaning up any memory it allocates but no longer needs.
• If you never free any memory and allocate an extremely large amount, you may run out of memory in the heap!
• However, memory leaks rarely (if ever) cause crashes.
• We recommend not to worry about freeing memory until your program is written. Then, go back and free memory as appropriate.
• Valgrind is a very helpful tool for finding memory leaks!
Lecture Plan

• **Recap**: Pointers So Far
• The Stack
• The Heap and Dynamic Memory
• **Practice**: Pig Latin + Valgrind
• realloc

```bash
cp -r /afs/ir/class/cs107/lecture-code/lect7 .
```
Let’s write a program that can convert text to Pig Latin! Simplified Pig Latin rules:

- If the word starts with a vowel, append “way”: `apple -> appleway`
- Otherwise, move all starting consonants to the end and append “ay”: `bridge -> idgebray`

We want to write a function `char *pig_latin(const char *in)` that returns the Pig Latin version of the given string.

- Good use case for heap allocation – array size is unknown until we convert it to Pig Latin! We’ll create and return a heap-allocated string.
- The caller must free the string when it is done.
Example: Pig Latin

We will also see an example of how to uncover memory leaks using Valgrind.

valgrind --leak-check=full --show-leak-kinds=all [program info here]
Demo: Pig Latin + Valgrind
Lecture Plan

• **Recap:** Pointers So Far
• The Stack
• The Heap and Dynamic Memory
• **Practice:** Pig Latin + Valgrind
• `realloc`

```
cp -r /afs/ir/class/cs107/lecture-code/lect7 .
```
void *realloc(void *ptr, size_t size);

• The `realloc` function takes an existing allocation pointer and enlarges to a new requested size. It returns the new pointer.

• If there is enough space after the existing memory block on the heap for the new size, `realloc` simply adds that space to the allocation.

• If there is not enough space, `realloc moves the memory to a larger location`, frees the old memory for you, and returns a pointer to the new location.
char *str = strdup("Hello");
assert(str != NULL);
...

// want to make str longer to hold "Hello world!"
char *addition = " world!";
str = realloc(str, strlen(str) + strlen(addition) + 1);
assert(str != NULL);

strcat(str, addition);
printf("%s", str);
free(str);
realloc

- realloc only accepts pointers that were previously returned by malloc/etc.
- Make sure to not pass pointers to the middle of heap-allocated memory.
- Make sure to not pass pointers to stack memory.
Cleaning Up with free and realloc

You only need to free the new memory coming out of realloc—the previous (smaller) one was already reclaimed by realloc.

```c
char *str = strdup("Hello");
assert(str != NULL);
...
// want to make str longer to hold "Hello world!"
char *addition = " world!";
str = realloc(str, strlen(str) + strlen(addition) + 1);
assert(str != NULL);
strcat(str, addition);
printf("%s", str);
free(str);
```
Heap allocation interface: A summary

void *malloc(size_t size);
void *calloc(size_t nmemb, size_t size);
void *realloc(void *ptr, size_t size);
char *strdup(char *s);
void free(void *ptr);

Heap memory allocation guarantee:
• NULL on failure, so check with assert
• Memory is contiguous; it is not recycled unless you call free
• realloc preserves existing data
• calloc zero-initializes bytes, malloc and realloc do not

Undefined behavior occurs:
• If you overflow (i.e., you access beyond bytes allocated)
• If you use after free, or if free is called twice on a location.
• If you realloc/free non-heap address
Heap allocator analogy: A hotel

Request memory by size (malloc)
• Receive room key to first of connecting rooms

Need more room? (realloc)
• Extend into connecting room if available
• If not, trade for new digs, employee moves your stuff for you

Check out when done (free)
• You remember your room number though

Errors! What happens if you...
• Forget to check out?
• Bust through connecting door to neighbor? What if the room is in use? Yikes...
• Return to room after checkout?
Engineering principles: stack vs heap

**Stack** ("local variables")

- **Fast**
  
  Fast to allocate/deallocate; okay to oversize

- **Convenient.**
  
  Automatic allocation/deallocation; declare/initialize in one step

- **Reasonable type safety**
  
  Thanks to the compiler

⚠️ **Not especially plentiful**

  Total stack size fixed, default 8MB

⚠️ **Somewhat inflexible**

  Cannot add/resize at runtime, scope dictated by control flow in/out of functions

**Heap** (dynamic memory)
Stack ("local variables")

- **Fast**
  Fast to allocate/deallocate; okay to oversize

- **Convenient.**
  Automatic allocation/deallocation; declare/initialize in one step

- **Reasonable type safety**
  Thanks to the compiler

⚠ **Not especially plentiful**
Total stack size fixed, default 8MB

⚠ **Somewhat inflexible**
Cannot add/resize at runtime, scope dictated by control flow in/out of functions

Heap (dynamic memory)

- **Plentiful.**
  Can provide more memory on demand!

- **Very flexible.**
  Runtime decisions about how much/when to allocate, can resize easily with realloc

- **Scope under programmer control**
  Can precisely determine lifetime

⚠ **Lots of opportunity for error**
Low type safety, forget to allocate/free before done, allocate wrong size, etc., Memory leaks (much less critical)
Stack and Heap

• Generally, unless a situation requires dynamic allocation, stack allocation is preferred. Often both techniques are used together in a program.

• Heap allocation is a necessity when:
  • you have a very large allocation that could blow out the stack
  • you need to control the memory lifetime, or memory must persist outside of a function call
  • you need to resize memory after its initial allocation
Recap

- **Misc. topics:** const, structs and the ternary operator
- **Recap:** Pointers So Far
- The Stack
- The Heap and Dynamic Memory
- **Practice:** Pig Latin
- Use-after-free bugs and vulnerability disclosure
- realloc

**Lecture 7 takeaway:** We can allocate memory on the heap to manage it ourselves. We manipulate heap memory via pointers. There are many opportunities for leaks and errors, and Valgrind can help detect them!

**Next time:** C Generics
Extra Practice
How can we implement `strdup` using functions we’ve already seen?

```c
1 char *mystrdup(const char *str) {
2     char *heapstr = _____(A)_____;  // Memory allocation
3     _____(B)_____;  // String allocation
4     _____(C)_____;  // String initialization
5     return heapstr;
6 }
```

[Note] Use library functions:
- `<stdlib.h>`: `malloc`
- `<assert.h>`: `assert`
- `<string.h>`: `strcpy`, `strlen`
How can we implement `strdup` using functions we’ve already seen?

```c
char *mystrdup(const char *str) {
    char *heapstr = malloc(strlen(str) + 1);
    assert(heapstr != NULL);
    strcpy(heapstr, str);
    return heapstr;
}
```

Char arrays differ from other arrays in that valid strings must be null-terminated (i.e., have an extra ending char).
(Note: library `strdup` doesn’t have an `assert`—it leaves the `assert` to the callee)
Goodbye, Free Memory

Where/how should we free memory below so that all memory is freed properly?

```c
char *str = strdup("Hello");
assert(str != NULL);
char *ptr = str + 1;
for (int i = 0; i < 5; i++) {
    int *num = malloc(sizeof(int));
    *num = i;
    printf("%s %d\n", ptr, *num);
}
printf("%s\n", str);
```

**Recommendation:** Don’t worry about putting in frees until **after** you’re finished with functionality. Memory leaks will rarely crash your CS107 programs.

**Answer in chat:**

“After line N: free(…);”

What if we didn’t free?

```bash
valgrind --leak-check=full --show-leak-kinds=all ...
```
Goodbye, Free Memory

Where/how should we free memory below so that all memory is freed properly?

```c
char *str = strdup("Hello");
assert(str != NULL);
char *ptr = str + 1;
for (int i = 0; i < 5; i++) {
    int *num = malloc(sizeof(int));
    *num = i;
    printf("%s %d\n", ptr, *num);
    free(num);
}
printf("%s\n", str);
free(str);
```

**Recommendation**: Don’t worry about putting in frees until **after** you’re finished with functionality.

Memory leaks will rarely crash your CS107 programs.
Write a function that takes in a heap-allocated `str1`, enlarges it, and concatenates `str2` onto it.

```c
char *strcat_extend(char *heap_str, const char *concat_str) {
    // (_________________(1)__________________);
    heap_str = realloc(___(2A)___,___(2B)___);
    // (_________________(3)__________________);
    strcat(___(3A)___, __(3B)___);
    return heapstr;
}
```

Example usage:

```c
char *str = strdup("Hello ");
str = strcat_extend(str, "world!");
printf("%s\n", str);
free(str);
```
Write a function that takes in a heap-allocated `str1`, enlarges it, and concatenates `str2` onto it.

```c
char *strcat_extend(char *heap_str, const char *concat_str) {
    int new_length = strlen(heap_str) + strlen(concat_str) + 1;
    heap_str = realloc(heap_str, new_length);
    assert(heap_str != NULL);
    strcat(heap_str, concat_str);
    return heapstr;
}
```

Example usage:

```c
char *str = strdup("Hello ");
str = strcat_extend(str, "world!");
printf("%s\n", str);
free(str);
```