CSCI 2021: C Basics

Chris Kauffman

Last Updated:
Mon 10 Feb 2020 10:04:54 AM CST
Logistics

Reading

- Bryant/O’Hallaron: Ch 1
- C references: whole language:
  types, pointers, addresses, arrays, conditionals, loops, structs, strings, malloc/free, preprocessor, compilation etc.

Goals

- Gain working knowledge of C
- Understand correspondence to lower levels of memory

Assignments

- HW02 due Wed night
- HW03 up later today
- Project 1 up now, submission available soon

Questions?
Announcements

CSE Career Fair,
https://cse.umn.edu/college/cse-career-fair
► Tue 2/04, 12-5pm, Mariucci Arena
► Go see what’s happening
► Bring some resumes, talk to employers, practice “networking”

Tool Time Session 1: Emacs
https://z.umn.edu/tooltime
► Tue 2/04, 6:30-8pm, Keller 3-180
► Optional evening lecture, no course credit
► Will discuss the power of the Emacs text editor
Every Programming Language

Look for the following as it should almost always be there

- Comments
- Statements/Expressions
- Variable Types
- Assignment
- Basic Input/Output
- Function Declarations
- Conditionals (if-else)
- Iteration (loops)
- Aggregate data (arrays, structs, objects, etc)
- Library System
Exercise: Traditional C Data Types

These are the traditional data types in C

<table>
<thead>
<tr>
<th>Bytes*</th>
<th>Name</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>INTEGRAL</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>char</td>
<td>-128 to 127</td>
</tr>
<tr>
<td>2</td>
<td>short</td>
<td>-32,768 to 32,767</td>
</tr>
<tr>
<td>4</td>
<td>int</td>
<td>-2,147,483,648 to 2,147,483,647</td>
</tr>
<tr>
<td>8</td>
<td>long</td>
<td>-9,223,372,036,854,775,808 to 9,223,372,036,854,775,807</td>
</tr>
<tr>
<td></td>
<td>FLOATING</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>float</td>
<td>±3.40282347E+38F (6-7 significant decimal digits)</td>
</tr>
<tr>
<td>8</td>
<td>double</td>
<td>±1.79769313486231570E+308 (15 significant decimal digits)</td>
</tr>
<tr>
<td></td>
<td>POINTER</td>
<td></td>
</tr>
<tr>
<td>4/8</td>
<td>pointer</td>
<td>Pointer to another memory location, 32 or 64bit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>double *d or int **ip or char *s or void *p (!?)</td>
</tr>
<tr>
<td></td>
<td>array</td>
<td>Pointer to a fixed location</td>
</tr>
<tr>
<td></td>
<td></td>
<td>double [] or int [][] or char []</td>
</tr>
</tbody>
</table>

*Number of bytes for each type is NOT standard but sizes shown are common. Portable code should NOT assume any particular size which is a huge pain in the @$$.

Inspect types closely and discuss...

Ranges of integral types?  void what now?
Missing types you expected?  How do you say char?
Answers: Traditional C Data Types

Ranges of signed integral types

Asymmetric: slightly more negative than positive

\[ \text{char} \quad | \quad -128 \text{ to } 127 \]

Due to use of Two’s Complement representation, many details and alternatives later in the course.

Missing: Boolean

Every piece of data in C is either truthy or falsey:

\[
\text{int } x; \quad \text{scanf}("%d", \&x);
\text{if}(x)\{ \quad \text{printf}("Truthy"); \} \quad \text{// very common}
\text{else}\{ \quad \text{printf}("Falsey"); \}
\]

Typically 0 is the only thing that is falsey

Missing: String

- char holds a single character like 'A' or '5'
- No String type: arrays of char like char str[] or char *s
- char pronounced CAR / CARE like “character” (debatable)
Exercise: Void Pointers

void *ptr; // void pointer
▶ Declares a pointer to something/anything
▶ Useful to store an arbitrary memory address
▶ Removes compiler’s ability to Type Check so introduces risks managed by the programmer

Example: void_pointer.c
▶ Predict output
▶ What looks screwy
▶ Anything look wrong?

File void_pointer.c:

```c
#include <stdio.h>

int main()
{
    int a = 5;
    double x = 1.2345;
    void *ptr;

    ptr = &a;
    int b = *((int *) ptr);
    printf("%d\n",b);

    ptr = &x;
    double y = *((double *) ptr);
    printf("%f\n",y);

    int c = *((int *) ptr);
    printf("%d\n",c);
    return 0;
}
```
> cat -n void_pointer.c
  1 // Demonstrate void pointer dereferencing and the associated
  2 // shenanigans. Compiler needs to be convinced to dereference in most
  3 // cases and circumventing the type system (compiler's ability to
  4 // check correctness) is fraught with errors.
  5 #include <stdio.h>
  6 int main(){
  7   int a = 5; // int
  8   double x = 1.2345; // double
  9   void *ptr; // pointer to anything
 10
 11   ptr = &a;
 12   int b = *((int *) ptr); // caste to convince compiler to deref
 13   printf("%d\n",b);
 14
 15   ptr = &x;
 16   double y = *((double *) ptr); // caste to convince compiler to deref
 17   printf("%f\n",y);
 18
 19   int c = *((int *) ptr); // kids: this is why types are useful
 20   printf("%d\n",c);
 21
 22 return 0;
 23 }

> gcc void_pointer.c
> a.out
5
1.234500
309237645 # interpreting floating point bits as an integer
Answers: Void Pointers

- The big weird integer 309237645 printed at the end is because...
  - `ptr` points at a memory location with a double
  - The compiler is “tricked” into treating this location as storing `int` data via the `(int *)` caste
  - Integer vs Floating layout is very different, we’ll see this later
  - Compiler generates low level instructions to move 4 bytes of the double data to an integer location
  - Both size and bit layout don’t match

- Since this is possible to do on a Von Neumann machine C makes it possible

- This does not mean it is a good idea: `void_pointer.c` illustrates weird code that usually doesn’t show up

- Avoid `void *` pointers when possible, take care when you must use them (there are many times you must use them in C)
But wait, there’re more types…

Unsigned Variants
Trade sign for larger positives

<table>
<thead>
<tr>
<th>Name</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>unsigned char</td>
<td>0 to 255</td>
</tr>
<tr>
<td>unsigned short</td>
<td>0 to 65,535</td>
</tr>
<tr>
<td>unsigned int</td>
<td>0 to 4,294,967,295</td>
</tr>
<tr>
<td>unsigned long</td>
<td>0 to… big, okay?</td>
</tr>
</tbody>
</table>

Fixed Width Variants since C99
Specify size / properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>int8_t</td>
<td>signed integer type with width of exactly 8, 16, 32 and 64 bits respectively</td>
</tr>
<tr>
<td>int16_t</td>
<td></td>
</tr>
<tr>
<td>int32_t</td>
<td></td>
</tr>
<tr>
<td>int64_t</td>
<td></td>
</tr>
<tr>
<td>int_fast8_t</td>
<td>fastest signed integer type with width of at least 8, 16, 32 and 64 bits respectively</td>
</tr>
<tr>
<td>int_fast16_t</td>
<td></td>
</tr>
<tr>
<td>int_fast32_t</td>
<td></td>
</tr>
<tr>
<td>int_fast64_t</td>
<td></td>
</tr>
<tr>
<td>int_least8_t</td>
<td>smallest signed integer type with width of at least 8, 16, 32 and 64 bits respectively</td>
</tr>
<tr>
<td>int_least16_t</td>
<td></td>
</tr>
<tr>
<td>int_least32_t</td>
<td></td>
</tr>
<tr>
<td>int_least64_t</td>
<td></td>
</tr>
<tr>
<td>intmax_t</td>
<td>maximum width integer type</td>
</tr>
<tr>
<td>intptr_t</td>
<td>integer type capable of holding a pointer</td>
</tr>
<tr>
<td>uint8_t</td>
<td>unsigned integer type with width of exactly 8, 16, 32 and 64 bits respectively</td>
</tr>
<tr>
<td>uint16_t</td>
<td></td>
</tr>
<tr>
<td>uint32_t</td>
<td></td>
</tr>
<tr>
<td>uint64_t</td>
<td></td>
</tr>
<tr>
<td>uint_fast8_t</td>
<td>fastest unsigned integer type with width of at least 8, 16, 32 and 64 bits respectively</td>
</tr>
<tr>
<td>uint_fast16_t</td>
<td></td>
</tr>
<tr>
<td>uint_fast32_t</td>
<td></td>
</tr>
<tr>
<td>uint_fast64_t</td>
<td></td>
</tr>
<tr>
<td>uint_least8_t</td>
<td>smallest unsigned integer type with width of at least 8, 16, 32 and 64 bits respectively</td>
</tr>
<tr>
<td>uint_least16_t</td>
<td></td>
</tr>
<tr>
<td>uint_least32_t</td>
<td></td>
</tr>
<tr>
<td>uint_least64_t</td>
<td></td>
</tr>
<tr>
<td>uintmax_t</td>
<td>maximum width unsigned integer type</td>
</tr>
<tr>
<td>uintptr_t</td>
<td>unsigned int capable of holding pointer</td>
</tr>
</tbody>
</table>

After our C crash course, we will discuss representation of integers with bits and relationship between signed / unsigned integer types.
Arrays and Pointers are Related with Subtle differences

<table>
<thead>
<tr>
<th>Property</th>
<th>Pointer</th>
<th>Array</th>
</tr>
</thead>
<tbody>
<tr>
<td>Declare like...</td>
<td>int *p; // rand val</td>
<td>int a[5]; // rand vals</td>
</tr>
<tr>
<td></td>
<td>int *p = &amp;x;</td>
<td>int a[] = {1, 2, 3};</td>
</tr>
<tr>
<td></td>
<td>int *p = q;</td>
<td>int a[2] = {2, 4};</td>
</tr>
<tr>
<td>Refers to a...</td>
<td>Memory location</td>
<td>Memory location</td>
</tr>
<tr>
<td>Which could be...</td>
<td>Anywhere</td>
<td>Fixed location</td>
</tr>
<tr>
<td>Location ref is</td>
<td>Changeable</td>
<td>Not changeable</td>
</tr>
<tr>
<td>Location...</td>
<td>Assigned by coder</td>
<td>Determined by compiler</td>
</tr>
<tr>
<td>Has at it...</td>
<td>One or more thing</td>
<td>One or more thing</td>
</tr>
<tr>
<td>Brace index?</td>
<td>Yep: int z = p[0];</td>
<td>Yep: int z = a[0];</td>
</tr>
<tr>
<td>Dereference?</td>
<td>Yep: int y = *p;</td>
<td>Nope</td>
</tr>
<tr>
<td>Arithmetic?</td>
<td>Yep: p++;</td>
<td>Nope</td>
</tr>
<tr>
<td>Assign to array?</td>
<td>Yep: int *p = a;</td>
<td>Nope</td>
</tr>
<tr>
<td>Interchangeable</td>
<td>doit_a(int a[]);</td>
<td>doit_p(int *p);</td>
</tr>
<tr>
<td></td>
<td>int *p = ...</td>
<td>int a[] = {1,2,3};</td>
</tr>
<tr>
<td></td>
<td>doit_a(p);</td>
<td>doit_p(a);</td>
</tr>
<tr>
<td>Tracks num elems</td>
<td>NOPE</td>
<td>NOPE</td>
</tr>
<tr>
<td></td>
<td>Nada, nothin, nope</td>
<td>No a.length or length(a)</td>
</tr>
</tbody>
</table>
Example: pointer_v_array.c

```c
// Demonstrate equivalence of pointers and arrays
#include <stdio.h>
void print0_arr(int a[]){ // print 0th element of a
    printf("%ld: %d\n", (long) a, a[0]); // address and 0th elem
}
void print0_ptr(int *p){ // print int pointed at by p
    printf("%ld: %d\n", (long) p, *p); // address and 0th elem
}
int main(){
    int *p = NULL; // declare a pointer, points nowhere
    printf("%ld: %ld\n", (long) &p, (long)p); // by casting to 64 bit long
    int x = 21; // declare an integer
    p = &x; // point p at x
    print0_arr(p); // pointer as array
    int a[] = {5,10,15}; // declare array, auto size
    print0_ptr(a); // array as pointer
    //a = p; // can't change where array points
    p = a; // point p at a
    print0_ptr(p);
    return 0;
}
```
1 #include <stdio.h>
2 void print0_arr(int a[]){
3   printf("%ld: %d\n",(long) a, a[0]);
4 }
5 void print0_ptr(int *p){
6   printf("%ld: %d\n",(long) p, *p);
7 }
8 int main(){
9   int *p = NULL;
10  printf("%ld: %ld\n", (long) &p, (long)p);
11
12  int x = 21;
13  p = &x;
14  print0_arr(p);
15  int a[] = {5,10,15};
16  print0_ptr(a);
17  //a = p;
18  p = a;
19  print0_ptr(p);
20  return 0;
21 }

Memory at indicated <POS>

<1>
<table>
<thead>
<tr>
<th>Addr</th>
<th>Type</th>
<th>Sym</th>
<th>Val</th>
</tr>
</thead>
<tbody>
<tr>
<td>#4948</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>#4944</td>
<td>int</td>
<td>a[2]</td>
<td>?</td>
</tr>
<tr>
<td>#4940</td>
<td>int</td>
<td>a[1]</td>
<td>?</td>
</tr>
<tr>
<td>#4936</td>
<td>int</td>
<td>a[0]</td>
<td>?</td>
</tr>
<tr>
<td>#4928</td>
<td>int*</td>
<td>p</td>
<td>NULL</td>
</tr>
<tr>
<td>#4924</td>
<td>int</td>
<td>x</td>
<td>?</td>
</tr>
</tbody>
</table>

<3>
<table>
<thead>
<tr>
<th>Addr</th>
<th>Type</th>
<th>Sym</th>
<th>Val</th>
</tr>
</thead>
<tbody>
<tr>
<td>#4948</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>#4944</td>
<td>int</td>
<td>a[2]</td>
<td>?</td>
</tr>
<tr>
<td>#4940</td>
<td>int</td>
<td>a[1]</td>
<td>?</td>
</tr>
<tr>
<td>#4936</td>
<td>int</td>
<td>a[0]</td>
<td>?</td>
</tr>
<tr>
<td>#4928</td>
<td>int*</td>
<td>p</td>
<td>#4924</td>
</tr>
<tr>
<td>#4924</td>
<td>int</td>
<td>x</td>
<td>21</td>
</tr>
</tbody>
</table>
1 #include <stdio.h>
2 void print0_arr(int a[]){
3   printf("%ld: %d\n", (long) a, a[0]);
4 }
5 void print0_ptr(int *p){
6   printf("%ld: %d\n", (long) p, *p);
7 }
8 int main(){
9   int *p = NULL;
10  printf("%ld: %ld\n", (long) &p, (long)p);
11  int x = 21;
12  p = &x;
13  print0_arr(p);
14  int a[] = {5,10,15};
15  print0_ptr(a);
16  //a = p;
17  p = a;
18  print0_ptr(p);
19  return 0;
20 }

Memory at indicated <POS>

<4>
| Addr | Type | Sym | Val |
|-------+------+------+-------|
| #4948 | ? | ? | ? |
| #4944 | int | a[2] | 15 |
| #4940 | int | a[1] | 10 |
| #4936 | int | a[0] | 5 |
| #4928 | int* | p | #4924 |
| #4924 | int | x | 21 |

<5>
| Addr | Type | Sym | Val |
|-------+------+------+-------|
| #4948 | ? | ? | ? |
| #4944 | int | a[2] | 15 |
| #4940 | int | a[1] | 10 |
| #4936 | int | a[0] | 5 |
| #4928 | int* | p | #4936 |
| #4924 | int | x | 21 |
Summary of Pointer / Array Relationship

Arrays
- Arrays are allocated by the Compiler at a **fixed location**
- Bare name a references is the starting address of the array
- Must use square braces $a[i]$ to index into them

Pointers
- Pointers can point to anything, can change, must be manually directed
- Can use square braces $p[i]$ or deref $*p$ to index into them

Interchangeability
- In most cases, functions that require an array can be passed a pointer
- Vice versa: requires a pointer can be passed an array
Exercise: Pointer Arithmetic

“Adding” to a pointer increases the position at which it points:
- Add 1 to an int*: point to the next int, add 4 bytes
- Add 1 to a double*: point to next double, add 8 bytes

Examine pointer_arithmetic.c below. Show memory contents and what’s printed on the screen.

```c
#include <stdio.h>

void print0_ptr(int *p){
    printf("%ld: %d\n", (long) p, *p);
}

int main(){
    int x = 21;
    int *p;
    int a[] = {5,10,15};
    p = a;
    print0_ptr(p);
    p = a+1;
    print0_ptr(p);
    p++;  
    print0_ptr(p);
    p += 2;
    print0_ptr(p);
    return 0;
}
```

<table>
<thead>
<tr>
<th>Addr</th>
<th>Type</th>
<th>Sym</th>
<th>Val</th>
</tr>
</thead>
<tbody>
<tr>
<td>#4948</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>#4944</td>
<td>int</td>
<td>a[2]</td>
<td>15</td>
</tr>
<tr>
<td>#4940</td>
<td>int</td>
<td>a[1]</td>
<td>10</td>
</tr>
<tr>
<td>#4936</td>
<td>int</td>
<td>a[0]</td>
<td>5</td>
</tr>
<tr>
<td>#4928</td>
<td>int*</td>
<td>p</td>
<td>?</td>
</tr>
<tr>
<td>#4924</td>
<td>int</td>
<td>x</td>
<td>21</td>
</tr>
</tbody>
</table>
```c
5 int main(){
6     int x = 21;
7     int *p;
8     int a[] = {5,10,15};
9     p = a;
10    printf_ptr(p);
11    p = a+1;
12    printf_ptr(p);
13    p++;
14    printf_ptr(p);
15    p+=2;
16    printf_ptr(p);
17    return 0;
18 }
```

### Table 1
<table>
<thead>
<tr>
<th>Addr</th>
<th>Type</th>
<th>Sym</th>
<th>Val</th>
<th>SCREEN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>#4948</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>5</td>
</tr>
<tr>
<td>#4944</td>
<td>int</td>
<td>a[2]</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>#4940</td>
<td>int</td>
<td>a[1]</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>#4936</td>
<td>int</td>
<td>a[0]</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>#4928</td>
<td>int*</td>
<td>p</td>
<td>#4940</td>
<td></td>
</tr>
<tr>
<td>#4924</td>
<td>int</td>
<td>x</td>
<td>21</td>
<td></td>
</tr>
</tbody>
</table>

### Table 2
<table>
<thead>
<tr>
<th>Addr</th>
<th>Type</th>
<th>Sym</th>
<th>Val</th>
<th>SCREEN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>#4948</td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>10</td>
</tr>
<tr>
<td>#4944</td>
<td>int</td>
<td>a[2]</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>#4940</td>
<td>int</td>
<td>a[1]</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>#4936</td>
<td>int</td>
<td>a[0]</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>#4928</td>
<td>int*</td>
<td>p</td>
<td>#4952</td>
<td></td>
</tr>
<tr>
<td>#4924</td>
<td>int</td>
<td>x</td>
<td>21</td>
<td></td>
</tr>
</tbody>
</table>
Pointer Arithmetic Alternatives

Pointer arithmetic often has more readable alternatives

```c
printf("enter 5 doubles\n");
double arr[5];
for(int i=0; i<5; i++){
    // POINTER: ick // PREFERRED
    scanf("%lf", arr+i); OR scanf("%lf", &arr[i]);
}
printf("you entered:\n");
for(int i=0; i<5; i++){
    // POINTER: ick // PREFERRED
    printf("%f ", *(arr+i)); OR printf("%f ",arr[i]);
}
```

But not always: following uses pointer arithmetic to append strings

```c
char name[128]; // up to 128 chars
printf("first name: ");
scanf(" %s", name); // read into name
int len = strlen(name); // compute length of string
name[len] = ' '; // replace \0 with space
printf("last name: ");
scanf(" %s",name+len+1); // read last name at offset
printf("full name: %s
",name);
```
Allocating Memory with `malloc()` and `free()`

**Dynamic Memory**
- Most C data has a fixed size: single vars or arrays with sizes specified at compile time
- `malloc()` is used to dynamically allocate memory
  - single arg: number of bytes of memory
  - frequently used with `sizeof()` operator
  - returns a `void*` to bytes found or `NULL` if not enough space could be allocated
- `free()` is used to release memory

```c
#include <stdio.h>
#include <stdlib.h> // malloc / free

int main(){
    printf("how many ints: ");
    int len;
    scanf(" %d",&len);
    int *nums = malloc(sizeof(int)*len);

    printf("initializing to 0\n");
    for(int i=0; i<len; i++){
        nums[i] = 0;
    }
    printf("enter %d ints: ",len);
    for(int i=0; i<len; i++){
        scanf(" %d",&nums[i]);
    }
    printf("nums are:\n");
    for(int i=0; i<len; i++){
        printf("[%d]: %d\n",i,nums[i]);
    }
    free(nums);
    return 0;
}
```
Exercise: Allocation Sizes

How Big

How many bytes allocated?
How many elements in the array?

```c
char  *a = malloc(16);
char  *b = malloc(16*sizeof(char));
int   *c = malloc(16);
int   *d = malloc(16*sizeof(int));
double *e = malloc(16);
double *f = malloc(16*sizeof(double));
int    **g = malloc(16);
int    **h = malloc(16*sizeof(int*));
```

Allocate

- Want an array of ints called ages, quantity 32
- Want an array of doubles called dps, quantity is in variable int size

Deallocate

Code to deallocate ages / dps

How many bytes CAN be allocated?

- Examine malloc_all_memory.c
Answers: Allocation Sizes

```c
char *a = malloc(16); // 16
char *b = malloc(16*sizeof(char)); // 16
int *c = malloc(16); // 16
int *d = malloc(16*sizeof(int)); // 64
double *e = malloc(16); // 16
double *f = malloc(16*sizeof(double)); // 128
int **g = malloc(16); // 16
int **h = malloc(16*sizeof(int*)); // 128

int *ages = malloc(sizeof(int)*32);
int size = ...;
double *dps = malloc(sizeof(double)*size);

free(ages);
free(dps);

Where does malloc()'d memory come from anyway...
```
When Should I `malloc()`?

**Compile Time**

- Sizes that are not known at **Compile Time** may need to be `malloc()`'d
- Compiler can calculate, sizes of fixed variables, arrays, sizes of stack frames for function calls
- Most of these are automatically managed on the **function call stack** and don’t require an special action

**Run Time**

- Compiler can’t predict the future, at **Run Time** programs must react to
  - Typed user input like names
  - Size of a file that is to be read
  - Elements to be added to a data structure
- As these things are determined, `malloc()` is used to allocate memory in the **heap**, when it is finished `free()` it
The Parts of Memory

- Running program typically has 4 regions of memory
  1. Stack: automatic, push/pop with function calls
  2. Heap: malloc() and free()
  3. Global: variables outside functions, static vars
  4. Text: Assembly instructions

- Stack grows into Heap, hitting the boundary results in stack overflow
- Will study ELF file format for storing executables
- Heap uses memory manager, will do an assignment on this
Valgrind\(^1\): Suite of tools including Memcheck

- Catches most memory errors\(^2\)
  - Use of uninitialized memory
  - Reading/writing memory after it has been free’d
  - Reading/writing off the end of malloc’d blocks
  - Memory leaks
- Source line of problem happened (but not cause)
- Super easy to use
- Slows execution of program way down

\(^1\)http://valgrind.org/
\(^2\)http://en.wikipedia.org/wiki/Valgrind
Valgrind in Action

See some common problems in badmemory.c

# Compile with debugging enabled: -g
> gcc -g badmemory.c

# run program through valgrind
> valgrind a.out
==12676== Memcheck, a memory error detector
==12676== Copyright (C) 2002-2013, and GNU GPL'd, by Julian Seward et al.
==12676== Using Valgrind-3.10.1 and LibVEX; rerun with -h for copyright info
==12676== Command: a.out
==12676==
==12676== Initialized memory
==12676== Conditional jump or move depends on uninitialised value(s)
==12676== at 0x4005C1: main (badmemory.c:7)
==12676==
==12676== Conditional jump or move depends on uninitialised value(s)
==12676== at 0x4E7D3DC: vfprintf (in /usr/lib/libc-2.21.so)
==12676== by 0x4E84E38: printf (in /usr/lib/libc-2.21.so)
==12676== by 0x4005D6: main (badmemory.c:8)
...

Link: Description of common Valgrind Error Messages
Exercise: free()’ing in the Wrong Spot

Common use for malloc() is for one function to allocate memory and return its location to another function (such as in A1). Question becomes when to free() such memory.

Program to the right is buggy, produces following output on one system

```c
#include <stdlib.h>
#include <stdio.h>

int *ones_array(int len){
    int *arr = malloc(sizeof(int)*len);
    for(int i=0; i<len; i++){
        arr[i] = 1;
    }
    free(arr);
    return arr;
}

int main(){
    int *ones = ones_array(5);
    for(int i=0; i<5; i++){
        printf("ones[%d] is %d\n",i,ones[i]);
    }
    free(ones);
    return 0;
}
```

▶ Why does this bug happen?
▶ How can it be fixed?
▶ Answers in free_twice.c

Apologies to those that printed slides on paper: the originally posted version had a correct code displayed rather than buggy code.
Answers: free()'ing in the Wrong Spot

- Once a malloc()'d area is free()'d, it is no longer valid
- Don’t free() data that is the return value of a function
- Never free() twice

```c
9 int *ones_array(int len){
10   int *arr = malloc(sizeof(int)*len);
11   for(int i=0; i<len; i++){
12     arr[i] = 1;
13   }
14   free(arr);  // should not free an array
15   return arr;  // being returned
16 }
17
18 int main(){
19   int *ones = ones_array(5);
20   for(int i=0; i<5; i++){
21     printf("ones[%d] is %d\n",i,ones[i]);
22   }
23
24   free(ones);  // 2nd free
25   return 0;
26 }
```

Note that the Valgrind output gives an **exact line number** where the problem occurs but this is **not the line to change** to fix the problem.
structs: Heterogeneous Groupings of Data

- Arrays are homogenous: all elements the same type
- structs are C's way of defining heterogeneous data
- Each field can be a different kind
- One instance of a struct has all fields
- Access elements with 'dot' notation
- Several syntaxes to declare, we'll favor modern approach
- Convention: types have _t at the end of their name to help identify them (not a rule but a good idea)

```c
typedef struct {
    // declare type
    int    field1;
    double field2;
    char   field3;
    int    field4[6];
} thing_t;

type_t a_thing;  // variable
    a_thing.field1 = 5;
    a_thing.field2 = 9.2;
    a_thing.field3 = 'c';
    a_thing.field4[2] = 7;
    int i = a_thing.field1;

type_t b_thing = {
    // variable
    .field1 = 15,  // initialize
    .field2 = 19.2,  // all fields
    .field3 = 'D',
    .field4 = {17, 27, 37, 47, 57, 67}
};
```
struct Ins/Outs

Recursive Types

- structs can have pointers to their same kind
- Syntax is a little wonky

```c
typedef struct node_struct {
    char data[128];
    struct node_struct *next;
} node_t;
```

Arrow Operator

- Pointer to struct, want to work with a field
- Use 'arrow' operator -> for this (dash/greater than)

```c
node_t *one_node = malloc(sizeof(node_t));
int length = 5;
node_t *node_arr = malloc(sizeof(node_t) * length);
node_t *node = ...;
if(node->next == NULL){ ... }
list_t *list = ...;
list->size = 5;
list->size++;
```

Dynamically Allocated Structs

- Dynamic Allocation of structs requires size calculation
- Use sizeof() operator

```c
node_t *one_node = malloc(sizeof(node_t));
int length = 5;
node_t *node_arr = malloc(sizeof(node_t) * length);

node_t *node = ...;
if(node->next == NULL){ ... }
list_t *list = ...;
list->size = 5;
list->size++;
```
Exercise: Structs in Memory

- Structs allocated in memory are laid out compactly
- Compiler may *pad* fields to place them at nice alignments (even addresses or word boundaries)

```c
typedef struct {
    double x;
    int y;
    char nm[4];
} small_t;

int main(){
    small_t a = 
        {.x=1.23, .y=4, .nm="hi"};
    small_t b =
        {.x=5.67, .y=8, .nm="bye"};
}
```

---

Memory layout of `main()`

<table>
<thead>
<tr>
<th>Addr</th>
<th>Type</th>
<th>Sym</th>
<th>Val</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>char</td>
<td>b.nm[3]</td>
<td>\0</td>
</tr>
<tr>
<td>#1031</td>
<td>char</td>
<td>b.nm[2]</td>
<td>e</td>
</tr>
<tr>
<td>#1030</td>
<td>char</td>
<td>b.nm[1]</td>
<td>y</td>
</tr>
<tr>
<td>#1029</td>
<td>char</td>
<td>b.nm[0]</td>
<td>b</td>
</tr>
<tr>
<td>#1028</td>
<td>int</td>
<td>b.y</td>
<td>8</td>
</tr>
<tr>
<td>#1024</td>
<td>double</td>
<td>b.x</td>
<td>5.67</td>
</tr>
<tr>
<td>#1016</td>
<td>char</td>
<td>a.nm[3]</td>
<td>?</td>
</tr>
<tr>
<td>#1015</td>
<td>char</td>
<td>a.nm[2]</td>
<td>\0</td>
</tr>
<tr>
<td>#1014</td>
<td>char</td>
<td>a.nm[1]</td>
<td>i</td>
</tr>
<tr>
<td>#1013</td>
<td>char</td>
<td>a.nm[0]</td>
<td>h</td>
</tr>
<tr>
<td>#1008</td>
<td>int</td>
<td>a.y</td>
<td>4</td>
</tr>
<tr>
<td>#1000</td>
<td>double</td>
<td>a.x</td>
<td>1.23</td>
</tr>
</tbody>
</table>

Result of?

```c
scanf("%d", &a.y); // input 7
scanf("%lf", &b.x); // input 9.4
scanf("%s", b.nm); // input yo
```
**Answers: Structs in Memory**

```c
scanf("%d", &a.y); // input 7
scanf("%lf", &b.x); // input 9.4
scanf("%s", b.nm); // input yo
```

| Addr   | Type  | Sym     | Before | After |
|--------+-------+---------+--------+-------|
| #1031  | char  | b.nm[3] | \0     |       |
| #1030  | char  | b.nm[2] | e      | \0    |
| #1029  | char  | b.nm[1] | y      | o     |
| #1028  | char  | b.nm[0] | b      | y     |
| #1024  | int   | b.y     | 8      |       |
| #1016  | double| b.x     | 5.67   | 9.4   |
| #1015  | char  | a.nm[3] | ?      |       |
| #1014  | char  | a.nm[2] | \0     |       |
| #1013  | char  | a.nm[1] | i      |       |
| #1012  | char  | a.nm[0] | h      |       |
| #1008  | int   | a.y     | 4      | 7     |
| #1000  | double| a.x     | 1.23   |       |
read_structs.c: malloc() and scanf() for structs

1 // Demonstrate use of pointers, malloc() with structs, scanning
2 // structs fields
3
4 #include <stdlib.h>
5 #include <stdio.h>
6
7 typedef struct { // simple struct
8     double x;    int y;    char nm[4];
9 } small_t;
10
11 int main(){
12     small_t c; // stack variable
13     small_t *cp = &c; // address of stack var
14     scanf("%lf %d %s", &cp->x, &cp->y, cp->nm); // read struct fields
15     printf("%f %d %s\n", cp->x, cp->y, cp->nm); // print struct fields
16
17     small_t *sp = malloc(sizeof(small_t)); // malloc'd struct
18     scanf("%lf %d %s", &sp->x, &sp->y, sp->nm); // read struct fields
19     printf("%f %d %s\n", sp->x, sp->y, sp->nm); // print struct fields
20
21     small_t *sarr = malloc(5*sizeof(small_t)); // malloc'd struct array
22     for(int i=0; i<5; i++){
23         scanf("%lf %d %s", &sarr[i].x, &sarr[i].y, sarr[i].nm); // read
24         printf("%f %d %s\n", sarr[i].x, sarr[i].y, sarr[i].nm); // print
25     }
26
27     free(sp); // free single struct
28     free(sarr); // free struct array
29     return 0;
30 }
File Input and Output

- Standard C I/O functions for reading/writing file data.
- Work with text data: formatted for human reading

```c
FILE *fopen(char *fname, char *mode);
// open file named fname, mode is "r" for reading, "w" for writing
// returns a File Handle (FILE *) on success
// returns NULL if not able to open file; do not fclose(NULL)

int fclose(FILE *fh);
// close file associated with fh, writes pending data to file,
// free()'s memory associated with open file
// Do not fclose(NULL)

int fscanf(FILE *fh, char *format, addr1, addr2, ...);
// read data from an open file handle according to format string
// storing parsed tokens in given addresses returns EOF if end of file
// is reached

int fprintf(FILE *fh, char *format, arg1, arg2, ...);
// prints data to an open file handle according to the format string
// and provided arguments

void rewind(FILE *fh);
// return the given open file handle to the beginning of the file.
```

Example of use in `struct_text_io.c`
Binary Data I/O Functions

- Open/close files same way with fopen()/fclose()
- Read/write raw bytes (not formatted) with the following

```c
size_t fread(void *dest, size_t byte_size, size_t count, FILE *fh);
// read binary data from an open file handle. Attempt to read
// byte_size*count bytes into the buffer pointed to by dest.
// Returns number of bytes that were actually read

size_t fwrite(void *src, size_t byte_size, size_t count, FILE *fh);
// write binary data to an open file handle. Attempt to write
// byte_size*count bytes from buffer pointed to by src.
// Returns number of bytes that were actually written
```

See examples of use in `struct_binary_io.c`

Tradeoffs between Binary and Textual Files

- Binary files usually smaller than text and can be directly read into memory but NOT easy on the eyes
- Text data more readable but more verbose, must be parsed and converted to binary numbers
Strings are Character Arrays

Conventions

- Convention in C is to use character arrays as strings
- Terminate character arrays with the \0 null character to indicate their end
  ```c
  char str1[6] = {'C','h','r','i','s','\0'};
  ```
- Null termination done by compiler for string constants
  ```c
  char str2[6] = "Chris"; // is null terminated
  ```
- Null termination done by most standard library functions like `scanf()`

Be aware

- `fread()` does not append nulls when reading binary data
- Manually manipulating a character array may overwrite ending null

String Library

- Include with `<string.h>`
- Null termination expected
- `strlen(s)`: length of string
- `strcpy(dest, src)`: copy chars from `src` to `dest`
- Limited number of others
Exercise: Common C operators

Arithmetic  +  -  *  /  %
Comparison ==  >  <  <=  >=  !=
Logical  &&  ||  !
Memory & and *
Compound +=  -=  *=  /=  ...
Bitwise Ops  ~  |  &  ~
Conditional  ?  :

Bitwise Ops
Will discuss soon

int x = y << 3;
int z = w & t;
long r = x | z;

Integer/Floating Division
Predict values for each variable

int q = 9 / 4;
int r = 9 % 4;
double x = 9 / 4;
double y = (double) 9 / 4;
double z = ((double)9) / 4;
double w = 9.0 / 4;
double t = 9 / 4.0;
int a=9, b=4;
double t = a / b;

Conditional (ternary) Operator

double x = 9.95;
int y = (x < 10.0) ? 2 : 4;
Integer versus real division: values for each of these are...

```java
int q = 9 / 4; // quotient 2
int r = 9 % 4; // remainder 1
double x = 9 / 4; // 2.0 (int quotient first)
double y = (double) 9 / 4; // 2.25
double z = ((double)9) / 4; // 2.25
double w = 9.0 / 4; // 2.25
double t = 9 / 4.0; // 2.25
int a=9, b=4;
double t = a / b; // 2 (int quotient)
```
C Control Structures

Looping/Iteration

// while loop
while(truthy){
  stuff;
  more stuff;
}

// for loop
for(init; truthy; update){
  stuff;
  more stuff;
}

// do-while loop
do{
  stuff;
  more stuff;
} while( truthy );

Conditionals

// simple if
if( truthy ){
  stuff;
  more stuff;
}

// chained exclusive if/elses
if( truthy ){
  stuff;
  more stuff;
}
else if(other){
  stuff;
}
else{
  stuff;
  more stuff;
}

// ternary ? : operator
int x = (truthy) ? yes : no;
Jumping Around in Loops

**break: often useful**

```plaintext
// break statement ends loop
// only valid in a loop
while(truthy){
    stuff;
    if( istrue ){
        something;
        break;-----+
    } |
    more stuff; |
}

after loop; <---+

// break ends inner loop,
// outer loop advances
for(int i=0; i<10; i++){
    for(int j=0; j<20; j++){ |
        printf("%d %d ",i,j);
        if(j == 7){ |
            break;----+
        } |
        printf("not div 3
");<--+
    }
}

Prints
i is 0
i is 1
not div 3
i is 2
not div 3
i is 3
i is 4
not div 3
...
```

**continue: occasionally useful**

```plaintext
// continue advances loop iteration
// does update in for loops

for(int i=0; i<10; i++){ |
    printf("i is %d\n",i); |
    if(i % 3 == 0){ |
        continue;-----------+
    }
    printf("not div 3\n");
}
```

Prints
i is 0
i is 1
not div 3
i is 2
not div 3
i is 3
i is 4
not div 3
...
Really Jumping Around: goto

- Machine-level control involves jumping to different instructions
- C exposes this as
  - somewhere: label for code position
  - goto somewhere; jump to that location
- goto_demo.c demonstrates a loop with gotos
- **Avoid** goto unless you have a compelling motive
- Beware spaghetti code...

```c
1 // Demonstrate control flow with goto
2 // Low level assembly jumps are similar
3 #include <stdio.h>
4 int main(){
5   int i=0;
6   beginning:   // a label for gotos
7       printf("i is %d\n",i);
8       i++;
9       if(i < 10){
10          goto beginning; // go back
11       }
12       goto ending;      // go forward
13       printf("print me please!\n");
14   ending:         // label for goto
15       printf("i ends at %d\n",i);
16       return 0;
17 }
```

XKCD #292
**switch()**/*case**: the **worst** control structure

- **switch/case** allows jumps based on an integral value
- **Frequent source of errors**
- **switch_demo.c** shows some features
  - use of **break**
  - fall through cases
  - default catch-all
  - Use in a loop
- May enable some small compiler optimizations
- **Almost never** worth correctness risks: one good use in my experience
- **Favor** if/else if/else unless compelled otherwise
A Program is Born: Compile, Assemble, Link, Load

- Write some C code in program.c
- Compile it with toolchain like GNU Compiler Collection
  
gcc -o program prog.c
- Compilation is a multi-step process
  - Check syntax for correctness/errors
  - Perform optimizations on the code if possible
  - Translate result to Assembly Language for a specific target processor (Intel, ARM, Motorola)
  - **Assemble** the code into object code, binary format (ELF) which the target CPU understands
  - **Link** the binary code to any required libraries (e.g. printing) to make an executable
- Result: executable program, but...
- To run it requires a **loader**: program which copies executable into memory, initializes any shared library/memory references required parts, sets up memory to refer to initial instruction
Exercise: Memory Review

1. How do you allocate memory on the Stack? How do de-allocate it?
2. How do you allocate memory dynamically (on the Heap)? How do de-allocate it?
3. What other parts of memory are there in programs?
4. How do you declare an array of 8 integers in C? How big is it and what part of memory is it in?
5. Describe several ways arrays and pointers are similar.
6. Describe several ways arrays and pointers are different.
7. Describe how the following two arithmetic expressions differ.

```c
int x=9, y=20;
int *p = &x;
x = x+1;
p = p+1;
```
Answers: Memory Review

1. How do you allocate memory on the Stack? How do de-allocate it?
   Declare local variables in a function and call the function. Stack frame has memory for all locals and is de-allocated when the function finishes/returns.

2. How do you allocate memory on the Heap? How do de-allocate it?
   Make a call to \( \text{ptr} = \text{malloc}(\text{nbytes}) \) which returns a pointer to the requested number of bytes. Call \( \text{free(ptr)} \) to de-allocate that memory.

3. What other parts of memory are there in programs?
   Global area of memory has constants and global variables. Text area has binary assembly code for CPU instructions.

4. How do you declare an array of 8 integers in C? How big is it and what part of memory is it in?
   An array of 8 ints will be 32 bytes big (usually).
   On the stack: \( \text{int arr[8]} \); De-allocated when function returns.
   On the heap: \( \text{int \ast arr = malloc(sizeof(int) \ast 8)} \); Deallocated with \( \text{free(arr)} \);
5. Describe several ways arrays and pointers are similar.

Both usually encoded as an address, can contain 1 or more items, may use square brace indexing like `arr[3] = 17`; Interchangeable as arguments to functions. Neither tracks size of memory area referenced.

6. Describe several ways arrays and pointers are different.

Pointers may be deref’d with `*ptr`; can’t do it with arrays. Can change where pointers point, not arrays. Arrays will be on the Stack or in Global Memory, pointers may also refer to the Heap.

7. Describe how the following to arithmetic expressions differ.

```c
int x=9, y=20; // x at #1024
int *p = &x; // p hold VALUE #1024 (points at x)
x = x+1; // x is now 10: normal arithmetic
p = p+1; // p is now #1028: pointer arithmetic
// may or may not point at y
```

Note: Last lecture is on Youtube due to a weather delay in Spring 2019.