Great Ideas in Computer Architecture

C Arrays, Strings, More Pointers

Instructor: Jenny Song

Review of Last Lecture

- C Basics
  - Variables, Functions, Control Flow, Syntax.
  - Only 0 and NULL evaluate to FALSE
- Pointers hold addresses
  - Address vs. Value
  - Allow for efficient code, but prone to errors
- C functions “pass by value”
  - Passing pointers circumvents this

Struct Clarification

- Structure definition:
  - Creates a variable type "struct foo", then declare the variable of that type

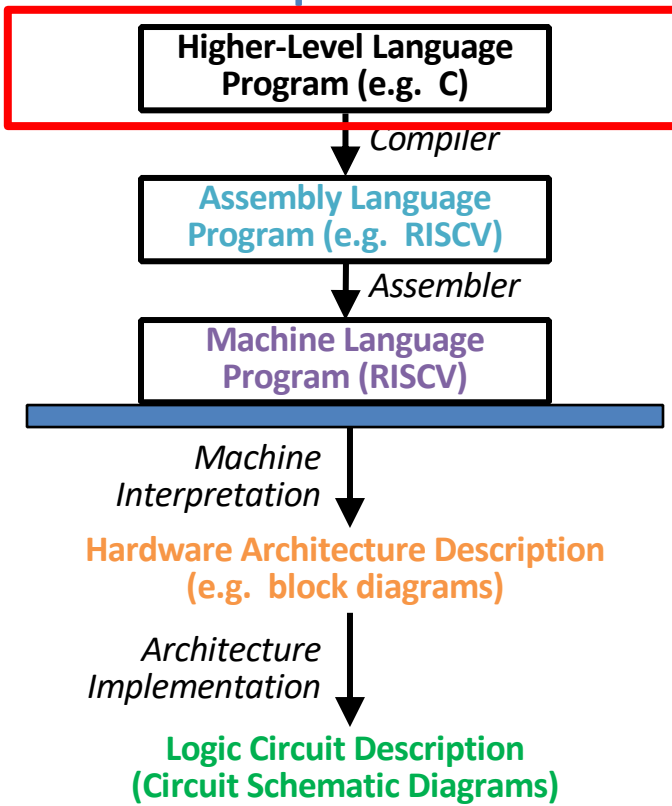
```
struct foo {
    /* fields */
};

struct foo name1;
struct foo *name2;
```

- Joint struct definition and typedef
  - Don't need to name struct in this case

```
struct foo {
    /* fields */
};
typedef struct foo bar;
bar name1;
```

```
typedef struct foo {
    /* fields */
} bar;
bar name1;
```

Great Idea #1: Levels of Representation/Interpretation

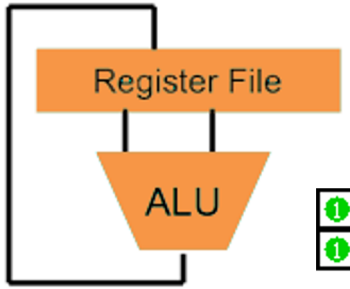


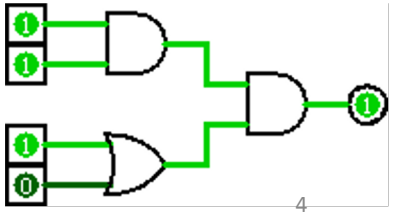

```
temp = v[k];
v[k] = v[k+1];
v[k+1] = temp;
```

We are here

```
lw    x5, 0(x2)
lw    x6, 4(x2)
sw    x6, 0(x2)
sw    x5, 4(x2)
```

```
0000 1001 1100 0110 1010 1111 0101 1000
1010 1111 0101 1000 0000 1001 1100 0110
1100 0110 1010 1111 0101 1000 0000 1001
0101 1000 0000 1001 1100 0110 1010 1111
```





Agenda

- C Operators
- Arrays
- Strings
- More Pointers
  - Pointer Arithmetic
  - Pointer Misc

Operator Precedence

Precedence	Operator	Description	Associativity
1	`++ --`	Suffix/postfix increment and decrement	Left-to-right
	`()`	Function call	
	`[]`	Array subscripting	
	`.`	Structure and union member access	
	`->`	Structure and union member access through pointer	
	`(`*type*`){`*list*`}`	Compound literal(C99)	
2	`++ --`	Prefix increment and decrement	Right-to-left
	`+ -`	Unary plus and minus	
	`! ~`	Logical NOT and bitwise NOT	
	`(`*type*`)`	Type cast	
	`*`	Indirection (dereference)	
	`&`	Address-of	
	`sizeof`	Size-of	
	`_Alignof`	Alignment requirement(C11)	

Assignment and Equality

- One of the most common errors for beginning C programmers

  `a = b` is *assignment*

  `a == b` is *equality test*

Operator Precedence

For precedence/order of execution, see Table 2-1 on p. 53 of K&R

- Use parentheses to manipulate
- Equality test (`==`) binds more tightly than logic (`&`, `|`, `&&`, `||`)
  - `x&1==0` means `x&(1==0)` instead of `(x&1)==0`

Operator Precedence

For precedence/order of execution, see Table 2-1 on p. 53 of K&R

- **Prefix** (++p) takes effect *immediately*
- **Postfix/Suffix** (p++) takes effect *last*

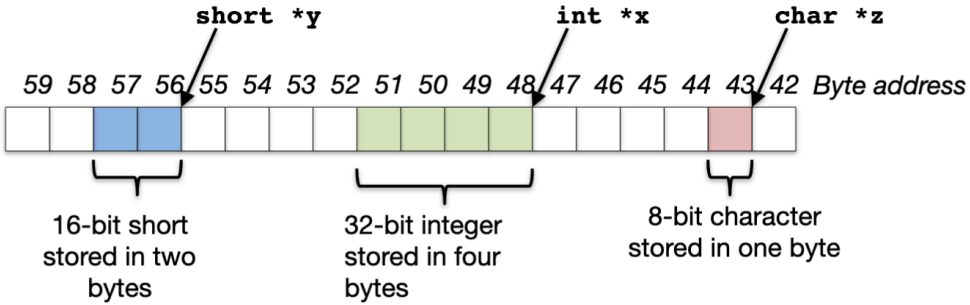
```
int main () {
  int x = 1;
  int y = ++x;   // y = 2, x = 2
  x--;           // x = 1
  int z = x++;   // z = 1, x = 2
  return 0;
}
```

Agenda

- C Operators
- Arrays
- Strings
- More Pointers
  - Pointer Arithmetic
  - Pointer Misc

Pointing to Different Size Objects

- Modern machines are “byte-addressable”
  - Hardware’s memory composed of 8-bit storage cells, each has a unique address
- A C pointer is just abstracted memory address
- Type declaration tells compiler how many bytes to fetch on each access through pointer
  -E.g., 32-bit integer stored in 4 consecutive 8-bit bytes
- But we actually want “word alignment”
  -Some processors will not allow you to address 32b values without being on 4 byte boundaries
  - Others will just be very slow if you try to access “unaligned” memory.



sizeof()

- Integer and pointer sizes are machine dependent—how do we tell?
- Use `sizeof()` operator
  - Returns size in bytes of variable or data type name

Examples:

```
int x;
int *y;
sizeof(x);      // 4  (32-bit int)
sizeof(int);    // 4  (32-bit int)
sizeof(y);      // 4  (32-bit addr)
sizeof(char);   // 1  (always)
```

sizeof()

- Acts differently with arrays and structs (to be explained later)
  - Arrays: returns size of whole array
  - Structs: returns size of one instance of struct (sum of sizes of all struct variables + padding)

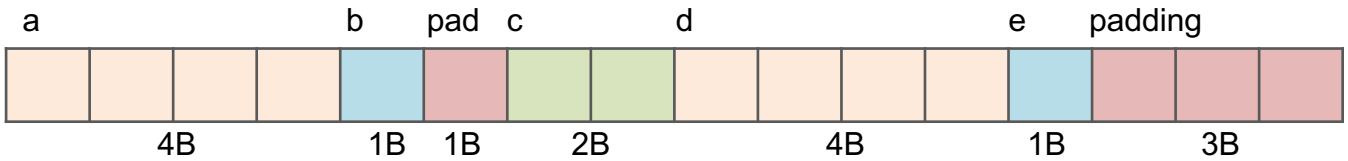
Struct Alignment

```
struct hello {
        int a;
        char b;
        short c;
        char *d;
        char e;
};
sizeof(hello)= ?  //4+1+2+4+1=12 no alignment
```

- Assume the default alignment rule is “32b architecture”
- char: 1 byte, no alignment needed
- short: 2 bytes, ½ word aligned
- int: 4 bytes, word aligned
- Pointers are the same size as int

Struct Alignment

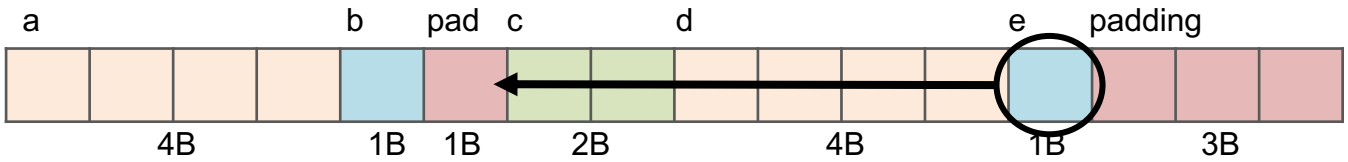
```
struct hello {
        int a;
        char b;
        short c;
        char *d;
        char e;
};
sizeof(hello) = 16
```



Struct Alignment

```
struct hello {
        int a;
        char b;
        short c;
        char *d;
        char e;
};
sizeof(hello) = 16
```

```
struct hello {
        int a;
        char b;
        char e;
        short c;
        char *d;
};
sizeof(hello) = 12
```



Array Basics

- **Declaration:**

  `int ar[2];` declares a 2-element integer array (just a block of memory)

  `int ar[] = {795, 635};` declares and **initializes** a 2-element integer array

- **Accessing elements:**

  `ar[num]` returns the numth element

  —Zero-indexed

Arrays Basics

- **Pitfall:** An array in C does not know its own length, and its bounds are not checked!
  - We can accidentally access off the end of an array
  - We must pass the array **and its size** to any procedure that is going to manipulate it
- Mistakes with array bounds cause *segmentation faults* and *bus errors*
  - Be careful! These are VERY difficult to find (You'll learn how to debug these in lab)

Accessing an Array

- Array size *n*: access entries *0* to *n-1*
- Use separate variable for array declaration & array bound to be reused (eg: no hard-coding)

Bad Pattern

```
int ar[10];
for(int i=0; i<10; i++) {...}
```

Better Pattern

```
const int ARRAY_SIZE = 10;
int ar[ARRAY_SIZE];
for(int i=0; i<ARRAY_SIZE; i++)
{...}
```

Single source of truth!

Arrays and Pointers

- Arrays are (almost) identical to pointers
  - `char *buffer` and `char buffer[]` are nearly identical declarations
  - Differ in subtle ways: initialization, sizeof(), etc.
- **Key Concept:** An array variable looks like a pointer to the first (0^{th}) element
  - `ar[0]` same as `*ar`; `ar[2]` same as `*(ar+2)`
  - We can use pointer arithmetic to conveniently access arrays
- An array variable is read-only (no assignment) (i.e. cannot use "`ar = <anything>`")

Array and Pointer Example

- `ar[i]` is treated as `*(ar+i)`
- To zero an array, the following three ways are equivalent:

1) `for(i=0; i<SIZE; i++){ar[i] = 0;}`

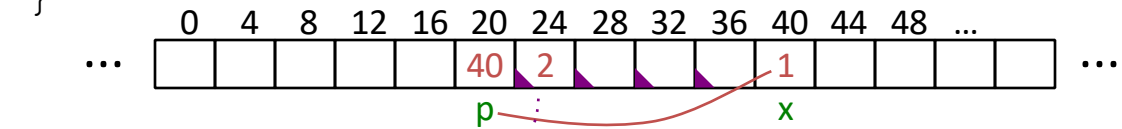
2) `for(i=0; i<SIZE; i++){*(ar+i) = 0;}`

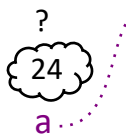
3) `for(p=ar; p<ar+SIZE; p++){*p = 0;}`

- These use *pointer arithmetic*, which we will get to shortly

Arrays Stored Differently Than Pointers

```
void foo() {
  int *p, a[4], x;
  p = &x;

  *p = 1; // or p[0]
  printf("*p:%u, p:%u, &p:%u\n",*p,p,&p);
  *a = 2; // or a[0]
  printf("*a:%u, a:%u, &a:%u\n",*a,a,&a);
}
```





***p:1, p:40, &p:20**

***a:2, a:24, &a:24**

K&R: "An array name is not a variable"

Arrays and Functions

- Declared arrays only allocated while the scope is valid:

```
char *foo() {
  char string[32]; ...;
  return string;
}
```

BAD

- An array is passed to a function as a pointer:

```
int foo(int ar[], unsigned int size)
{
   ... ar[size-1] ...
}
```

Really `int *ar`

Must explicitly pass the size!

Arrays and Functions

- Array size gets lost when passed to a function
- What prints in the following code:

```
int foo(int array[],
    unsigned int size) {
    ...
    printf("%d\n", sizeof(array));
}

int main(void) {
    int a[10], b[5];
    ... foo(a, 10) ...
    printf("%d\n", sizeof(a));
}
```

sizeof(int *)

10*sizeof(int)

Agenda

- C Operators
- Arrays
- Strings
- More Pointers
  - Pointer Arithmetic
  - Pointer Misc

C Strings

- A String in C is just an array of characters

```
char letters[] = "abc";
const char letters[] = {'a','b','c','\0'};
```

- But how do we know when the string ends?
  (because arrays in C don't know their size)
  - Last character is followed by a 0 byte (`'\0'`)
    (a.k.a. "null terminator")

This means you need an extra space in your array!!!

C Strings

- How do you tell how long a C string is?
  - Count until you reach the null terminator

```
int strlen(char s[]) {
    int n = 0;
    while (s[n] != 0){n++;}
    return n;
}
```

- Danger: What if there is no null terminator?

C String Standard Functions

- Accessible with `#include <string.h>`
- `int strlen(char *string);`
  - Returns the length of string (not including null term)
- `int strcmp(char *str1, char *str2);`
  - Return 0 if `str1` and `str2` are identical (how is this different from `str1 == str2`?)
- `char *strcpy(char *dst, char *src);`
  - Copy contents of string `src` to the memory at `dst`. Caller must ensure that `dst` has enough memory to hold the data to be copied
  - Note: `dst = src` only copies *pointer* (the address)

String Examples

```
#include <stdio.h>
#include <string.h>
int main () {
   char s1[10], s2[10], s3[]="hello", *s4="hola";
   strcpy(s1,"hi");  strcpy(s2,"hi");
}
```

Value of the following expressions?

`sizeof(s1)` 10

`strlen(s1)` 2

`s1==s2` 0 Point to different locations!

`strcmp(s1,s2)` 0

`strcmp(s1,s3)` 4 (s1 > s3) e, f, g, h, i

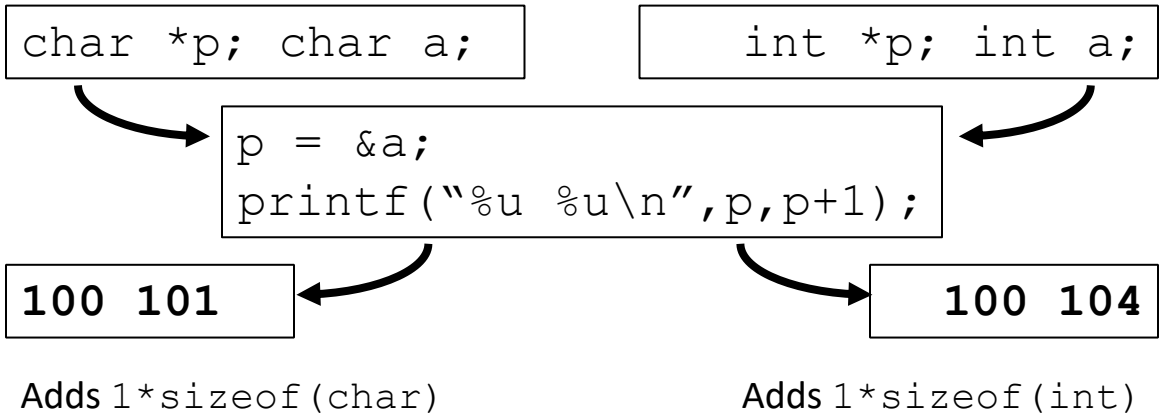
`strcmp(s1,s4)` -6 (s1 < s4) i, j, k ,l , m, n, o

Agenda

- Miscellaneous C Syntax
- Arrays
- Strings
- More Pointers
  - Pointer Arithmetic
  - Pointer Misc

Pointer Arithmetic

- *pointer* ± *number*
  - e.g. *pointer* + 1 adds 1 something to the address
- Compare what happens: (assume `a` at address 100)



- *Pointer arithmetic should be used cautiously*

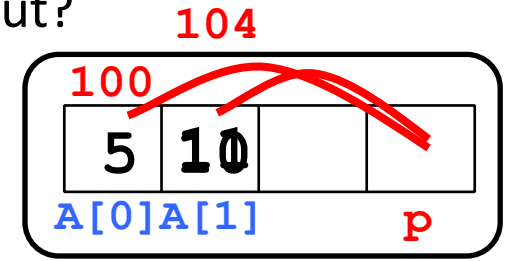
Pointer Arithmetic

- A pointer is just a memory address, so we can add to/subtract from it to move through an array
- `p+1` correctly increments `p` by `sizeof(*p)`
  - i.e. moves pointer to the next array element
- What about an array of structs?
  - Struct declaration tells C the size to use, so handled like basic types

Pointer Arithmetic

- What is valid pointer arithmetic?
  - Add an integer to a pointer
  - Subtract 2 pointers (in the same array)
  - Compare pointers (<, <=, ==, !=, >, >=)
  - Compare pointer to NULL (indicates that the pointer points to nothing)
- Everything else is illegal since it makes no sense:
  - Adding two pointers
  - Multiplying pointers
  - Subtract pointer from integer

Question: The first `printf` outputs `100 5 5 10`. What will the next two `printf` output?




```
int main(void){
    int A[] = {5,10};
    int *p = A;

    printf("%u %d %d %d\n", p, *p, A[0], A[1]);
    p =  p + 1;
    printf("%u %d %d %d\n", p, *p, A[0], A[1]);
    *p = *p + 1;
    printf("%u %d %d %d\n", p, *p, A[0], A[1]);
}
```

(A) 101 10 5 10 then 101 11 5 11

(B) 104 10 5 10 then 104 11 5 11

(C) 100 6 6 10 then 101 6 6 10

(D) 100 6 6 10 then 104 6 6 10

(REVIEW) Operator Precedence

For precedence/order of execution, see Table 2-1 on p. 53 of K&R

- **Prefix** (++p) takes effect *immediately*
- **Postfix/Suffix** (p++) takes effect *last*

```
int main () {
  int x = 1;
  int y = ++x;  // y = 2, x = 2
  x--;
  int z = x++;  // z = 1, x = 2
  return 0;
}
```

Increment and Dereference

- When multiple prefixal operators are present, they are applied from *right to left*

`*--p` decrements `p`, returns val at that addr

- `--` binds to `p` before `*` and takes effect first

`++*p` increments `*p` and returns that val

- `*` binds first (get val), then increment immediately

Increment and Dereference

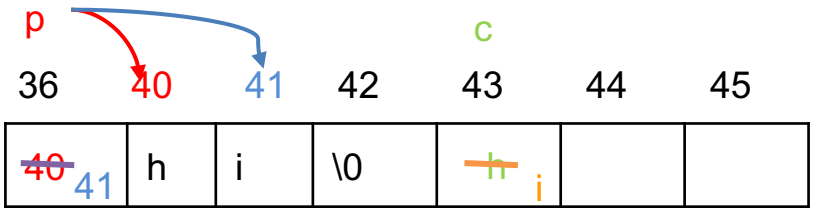
- *Postfixal* in/decrement operators have precedence over prefixal operators (e.g. `*`)
  - BUT the in/decrementation takes effect last because it is a postfix. The “front” of expression is returned.
- `*p++` returns `*p`, then increments `p`
  - `++` binds to `p` before `*`, but takes effect last

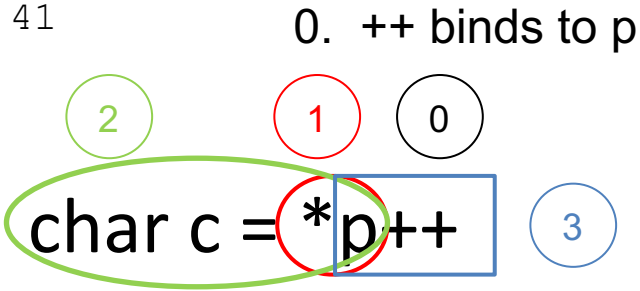
Increment and Dereference

*p++ returns *p, then increments p

- ++ binds to p before *, but takes effect last

```
char *p = "hi"; // assume p has value 40
char c = *p++;  // c = 'h', p = 41
c      = *p;    // c = 'i'
```





1. Evaluate *p = 'h'
2. Assignment c = 'h'
3. p++; p = 41
4. c = *p; c = 'i'

Increment and Dereference

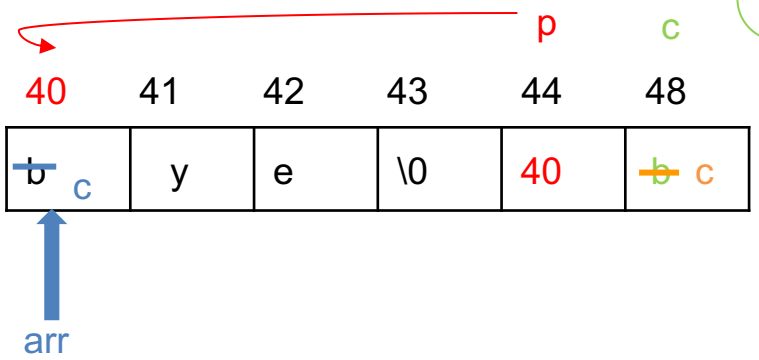
- *Postfixal* in/decrement operators have precedence over prefixal operators (e.g. `*`)
  - BUT the in/decrementation takes effect last because it is a postfix. The “front” of expression is returned.
- `(*p)++` returns `*p`, then increments in mem
  - Post-increment happens last

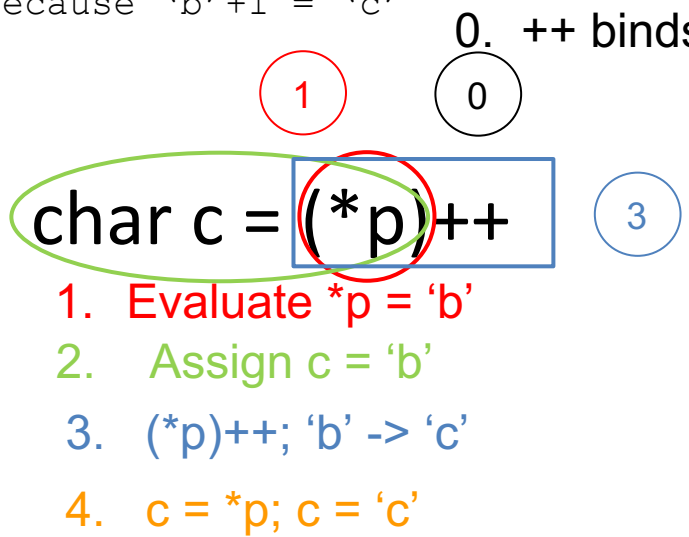
Increment and Dereference

`(*p)++` returns `*p`, then increments in mem

- Post-increment happens last

```
char arr[] = "bye";
char *p = arr;      // assume p has value 40
char c  = (*p)++;   // c = 'b', p = 40
c       = *p;       // c = 'c'  because 'b'+1 = 'c'
```





Agenda

- C Operators
- Arrays
- Strings
- More Pointers
  - Pointer Arithmetic
  - Pointer Misc

Pointers and Allocation

- When you declare a pointer (e.g. `int *ptr;`), it doesn't actually point to anything yet
  - It points somewhere (garbage; don't know where)
  - Dereferencing will usually cause an error
- **Option 1:** Point to something that already exists
  - `int *ptr,var; var = 5; ptr = &var;`
  - `var` has space implicitly allocated for it (declaration)
- **Option 2:** Allocate room in memory for new thing to point to (next lecture)

Pointers and Structures

Variable declarations:

```
struct Point {
    int x;
    int y;
    struct Point *p;
};

struct Point pt1;
struct Point pt2;
struct Point *ptaddr;
```

Cannot contain an instance of itself, but can point to one

Valid operations:

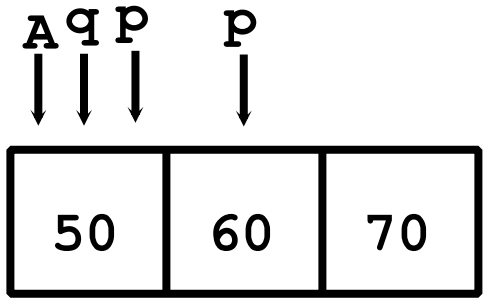
```
/* dot notation */
int h = pt1.x;
pt2.y = pt1.y;

/* arrow notation */
int h = ptaddr->x;
int h = (*ptaddr).x;

/* This works too */
pt1 = pt2;
```

Copies contents

Pointers to Pointers

- What if want function to change a pointer?

```
void IncrementPtr(int *p) {
    p = p + 1;
}

int A[3] = {50, 60, 70};
int *q = A;
IncrementPtr(q);
printf("*q = %d\n", *q);
```

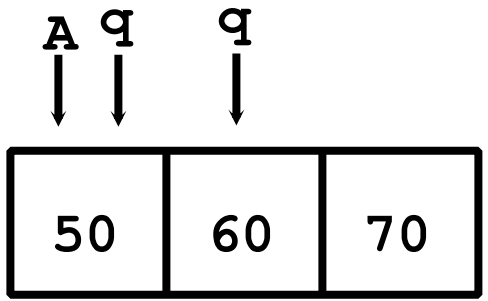


***q: 50**

Pointers to Pointers

- *Pointer to a pointer*, declared as `**h`
- Example:

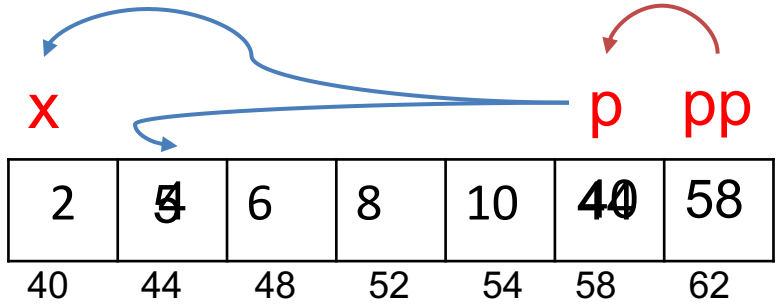
```
void IncrementPtr(int **h) {
    *h = *h + 1;
}

int A[3] = {50, 60, 70};
int *q = A;
IncrementPtr(&q);
printf("*q = %d\n", *q);
```



***q: 60**

Pointers to Pointers

```
int x[] = { 2, 4, 6, 8, 10 };
int *p = x;
int **pp = &p;
(*pp)++;
(*(*pp))++;
printf("%d\n", *p);
```



Result is:

A: 2

B: 3

C: 4

D: 5

E: None of the above

Summary

- Pointers and array variables are very similar
  - Can use pointer or array syntax to index into arrays
- Strings are null-terminated arrays of characters
- Pointer arithmetic moves the pointer by the size of the thing it's pointing to
- Pointers are the source of many bugs in C, so handle with care