

CS319: Scientific Computing (with C++)

# Week 6: The Password Problem

9am, 16 March, 2021

Title change to:

"Composing Algorithms"

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &amp; 3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON ERRORS)</p>	<p>~28 BITS OF ENTROPY</p> <p><math>2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>(PRACTICAL ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A SCREEN WHEN IS STAGGER, BUT IT'S NOT WHAT THE PROBLEM WOULD BE ASKED ABOUT)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p><math>2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}</math></p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE. CORRECT.</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

<http://xkcd.com/936>


## Usual reminders...

	Mon	Tue	Wed	Thu	Fri
9 – 10		LECTURE	X		
10 – 11		* LAB			
11 – 12					
12 – 1					
1 – 2		LAB			
2 – 3					
3 – 4					
4 – 5			<del>LECTURE</del>		

1. This week, we have just one recorded class: **Tuesdays** at 9.00.
2. **Lab times: Tuesday 10.00-10:50, and 13.00-13.50.** You should try to attend at least one of these.
3. A short introduction to the lab will be recorded.

# Usual reminders...

---

- 1 Part 1: A note on complexity
  - 2 Part 2: Merge Sort
    - Why is Merge Sort is fast
    - Implementation
  - 3 Part 3: Comparing in practice
  - 4 Part 4: The Password problem
    - Algorithm (high-level)
    - Implementation
- 

# Part 1: A note on complexity

/

CS319 – Week 6  
Week 6: The Password Problem

Start of ...

**PART 1: A note on complexity**

.

## Part 1: A note on complexity

Before we introduce an algorithm that is “better” than Bubble Sort, we need to explain what “better” means.

There are many ways that one algorithm could be considered superior to another, for example:

- ▶ takes less time to run; ✓
- ▶ takes less memory to run; ✓
- ▶ takes less time to program; ←
- ▶ is more accurate;
- ▶ is more reliable;

▶ ...? Do you have any idea?  
Eg: more parallelizable.

## Part 1: A note on complexity

$O = \text{"oh"} = \text{"Order"}$

Focusing on **efficiency**, we now need a way of discussing how the time taken by an algorithm depends on the problem size.

The usual way to discuss this in terms of the **"Big O"** notation, which is used to classify how their run-times (for example) grow as the input size grows.

For example, if we say an algorithm for a problem of size  $n$  has complexity  $O(n^2)$ , then we mean there is some constant,  $C$  such that the run-time is at most  $Cn^2$ . We don't really care too much about what  $C$  is. For example, if Algorithm 1 had complexity  $0.1n^2$ , and Algorithm 2 had complexity  $100n$ , then...

Problem size, when sorting, we mean the number of items to be sorted.

## Part 1: A note on complexity

Focusing on efficiency, we now need a way of discussing how the time taken by an algorithm depends on the problem size.

The usual way to discuss this is in terms of the “Big  $O$ ” notation, which is used to classify how their run-times (for example) grow as the input size grows.

For example, if we say an algorithm for a problem of size  $n$  has complexity  $O(n^2)$ , then we mean there is some constant,  $C$  such that the run-time is at most  $Cn^2$ . We don't really care too much about what  $C$  is.

For example, if Algorithm 1 had complexity  $0.1n^2$  and Algorithm 2 had complexity  $100n$ , then...

$n$	$0.1 n^2$	$100 n$
1	0.1s	100s
10	$(0.1)(100) = 10$	1,000
100	$(0.1)(10,000)$ $= 1,000$	10,000
1000	100,000	100,000

Generally, we work out the “ $n$ ” part mathematically and  $C$  by computing.

← break - even

## Part 1: A note on complexity

The best to worst, some common complexities are

▶  $O(1)$  → "Time is independent of Problem Size"

▶  $O(\log n)$  →

▶  $O(n)$

▶  $O(n \log n)$

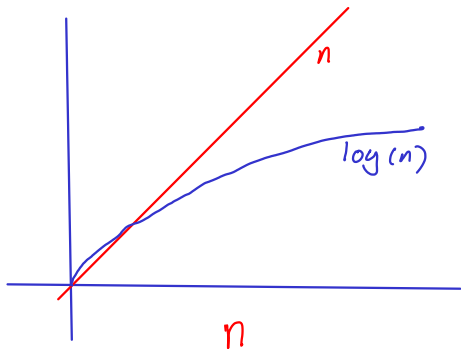
▶  $O(n^2)$

▶  $O(n^3)$

▶  $O(2^n)$

▶  $O(n!)$

Common, but  
terrific.





# Part 1: A note on complexity

---

**CS319 – Week 5**  
**Week 6: The Password Problem**

**END OF PART 1**

# Part 2: Merge Sort

CS319 – Week 6  
Week 6: The Password Problem

Start of ...

**PART 2: Merge Sort**  
*Merge*  
*Merge*

## Part 2: Merge Sort

The **Bubble Sort algorithm** from last week is much too slow for the project we have in mind: its worst-case complexity is  $\mathcal{O}(N^2)$  for a list of length  $N$ .

Instead we'll implement the **Merge Sort** algorithm. It has complexity  $\mathcal{O}(N \log N)$ .

### Merge Sort

- ▶ Split the list into two smaller lists,
- ▶ Split each of those into 2 smaller lists.
- ▶ Keep doing this until each list is of length 1.
- ▶ A list of length 1 is already sorted, so...
- ▶ Reassemble each of your sub-lists by merging these sorted list.

## Part 2: Merge Sort

It is useful to write this as a **recursive algorithm**:

### Recursive Merge Sort Algorithm

```
procedure mergesort( $L = a_1, a_2, \dots, a_n$ )
  if  $n \geq 1$  then [if  $n=0$  or  $1$ , we are done!]
     $m := \text{floor}(n/2)$   $\rightarrow$  (if  $n$  is even,  $m = n/2$ ; if  $n$  is odd,  $m = (n-1)/2$ )
     $L_1 := (a_1, a_2, \dots, a_m)$ 
     $L_2 := (a_{m+1}, a_{m+2}, \dots, a_n)$ 
     $L := \text{merge}(\text{mergesort}(L_1), \text{mergesort}(L_2))$ 
  end if
```

So we need two functions:

- (i) A `Merge()` function to merge two sorted list
- (ii) A `MergeSort()` function that
  - ▶ splits the list in two,
  - ▶ calls `MergeSort()` for each half
  - ▶ calls the `Merge()` function

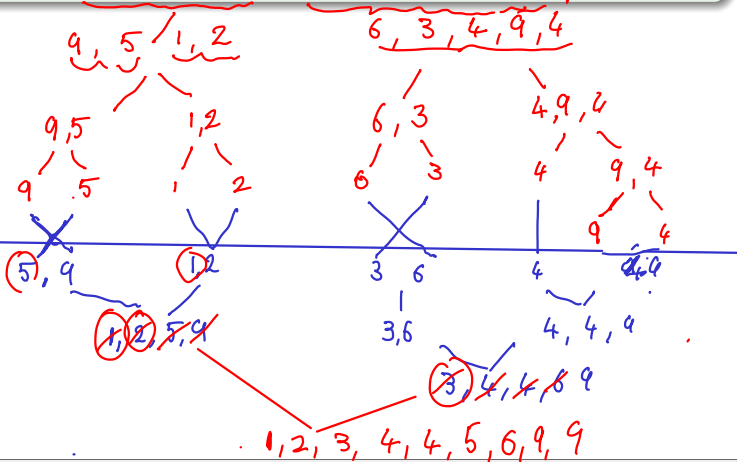
# Part 2: Merge Sort

## Example (Merge Sort)

Show how **Merge Sort** would sort the list

9 5 1 2 6 3 4 9 4

$n = 9$   
 $m = 4$



## Part 2: Merge Sort

## Why is Merge Sort is fast

First, why is Bubble Slow?

For this algorithm, we find the largest element in a list of length  $n$ . That takes  $n-1$  steps.

Next apply bubble to a list of length  $n-1$ , which takes  $n-2$  steps. Repeating, this needs

$$\begin{array}{r} n-1 \\ + n-2 \\ + n-3 \\ + \vdots \\ + 2 \\ + 1 \end{array}$$

$$\begin{aligned} & (n-1) + (n-2) + (n-3) + \dots + (2) + 1 \\ & = (n-1) \left(\frac{n}{2}\right) \quad \text{[check this!]} \\ & = \frac{1}{2}n^2 - \frac{n}{2} \end{aligned}$$

which is  $O(n^2)$ .

But Merge Sort : Splits the list into lists of length 1 in  $\log_2(n)$  steps. (Eg if  $n=8$ , 3 steps are needed).

Then merging requires  $O(n)$  steps

Total is  $n \log_2(n)$   
 i.e.  $O(n \log(n))$ .

!

Our first function will take two sorted lists, and combine them.

00MergeSort.cpp

This function sorts  
list 1 and list 2

```

56 template <typename MyType>
void Merge(MyType *list1, unsigned int length1,
           MyType *list2, unsigned int length2,
58           MyType *Merged)
{
60     unsigned int i=0, j=0;
    for (unsigned int k=0; k<length1+length2; k++)
62         if ( (i != length1) && ((j==length2)
                || (list1[i] <= list2[j])) ) {
64             Merged[k] = list1[i];
                i++;
66         }
        else {
68             Merged[k] = list2[j];
                j++;
70         }
    }

```

into  
the  
"Merged"  
array



00MergeSort.cpp

```

82 template <typename MyType>
void MergeSort(MyType *list , unsigned int length)
{
84     if (length <=1) // A list of length 0 or 1 is sorted.
        return;
86     else {
        unsigned int m = (unsigned int) floor(((double)length / 2.0))
88     MyType *list1 = new MyType [m];
        MyType *list2 = new MyType [length-m];
90     for (unsigned int i=0; i<m; i++)
        list1[i]=list[i];
92     for (unsigned int i=0; i<length-m; i++)
        list2[i]=list[m+i];
94     MergeSort(list1 , m);
        MergeSort(list2 , length-m);
96     Merge(list1 , m, list2 , length-m, list);
        delete [] list1;    delete [] list2;
98     }
}

```

*m = floor(N/2)*  
*n*  
*making sublists*

**CS319 – Week 5**  
**Week 6: The Password Problem**

**END OF PART 2**

# Part 3: Comparing in practice

CS319 – Week 6  
Week 6: The Password Problem

Start of ...

## PART 3: Comparing in practice (of 3)

## Part 3: Comparing in practice

Today, we considered two sorting algorithms

- ▶ **Bubble Sort** which is conceptually simple, and has a **worst-case** complexity of  $\mathcal{O}(N^2)$  for a list of length  $N$ .
- ▶ A recursive **Merge Sort**, which has a worst-case complexity of  $\mathcal{O}(N \log N)$  for a list of length  $N$ .

This means that if we have a list of length  $N$ , then the expected time taken for the methods are  $C_B N^2$  and  $C_M N \log N$ , for some constants  $C_B$  and  $C_M$ .

↓  
 $C_B =$  "constant for Bubble"  
 $C_M =$  "constant for Merge"

/

## Part 3: Comparing in practice

---

We want to estimate these constants so that we can predict how long the algorithm will take for some given  $N$ .

Before class, I ran both algorithms. Here is a snippet of the code I used, and the output. **Can we estimate how long each algorithm would take for a list of length 32 million?**

## Part 3: Comparing in practice

See `01CompareSorts.cpp` for more details

```
40 for (int n=1000; n<=32000; n*=2) {  
    for (int i=0; i<n; i++)  
        Copy[i] = Numbers[i];  
42 start=clock();  
    BubbleSort(Copy, n);  
44 diff = (double)(clock()-start);  
    diff_seconds = diff/CLOCKS_PER_SEC;  
46 C_bubble = diff_seconds / ((double)(n*n));  
    std::cout << "Bubble: n=" << n <<  
48 " took " << diff_seconds <<  
    " seconds. C=" << C_bubble << std::endl;  
50 }
```

Output (Bubble Sort):

```
Bubble: n = 1000 took 0.01468 seconds. C=1.468e-08  
Bubble: n = 2000 took 0.0265 seconds. C=6.625e-09  
Bubble: n = 4000 took 0.06219 seconds. C=3.887e-09  
Bubble: n = 8000 took 0.2737 seconds. C=4.276e-09  
Bubble: n = 16000 took 1.134 seconds. C=4.428e-09  
Bubble: n = 32000 took 4.623 seconds. C=4.514e-09
```

## Part 3: Comparing in practice

See 01CompareSorts.cpp for more details

```
66  for (int n=1000; n<=32000; n*=2) {
68      for (int i=0; i<n; i++)
        Copy[i] = Numbers[i];
70      start=clock();
        MergeSort(Copy, n);
        diff = (double)(clock()-start);
72      diff_seconds = diff/CLOCKS_PER_SEC;
        C_merge= diff_seconds / ( (double)(n*log2(n)));
74      std::cout << "Merge: _n=_\n" << std::setw(5) << n <<
        "_took_" << std::setw(5) << diff_seconds <<
76          << "_seconds..C=" << C_merge << std::endl;
    }
```

Output (Merge Sort):

Merge: n = 1000 took 0.000245 seconds. C=2.458e-08

Merge: n = 2000 took 0.000425 seconds. C=1.938e-08

Merge: n = 4000 took 0.000873 seconds. C=1.824e-08

Merge: n = 8000 took 0.001754 seconds. C=1.691e-08

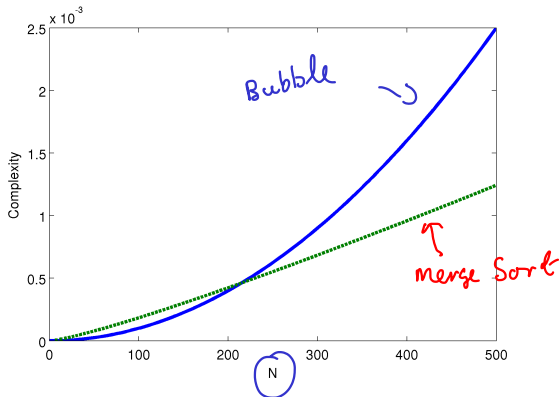
Merge: n = 16000 took 0.003692 seconds. C=1.652e-08

Merge: n = 32000 took 0.008756 seconds. C=1.828e-08

## Part 3: Comparing in practice

### Question?

How long would it take to sort a list of length 32,000,000?





## Part 3: Comparing in practice

---

### CS319 – Week 5 Week 6: The Password Problem

**END OF PART 3**

*Finished Here*