15 May 2023
MAT 2250

Last time: to sort a list of n elements, we constructed a binary decision tree with $n!$ leaves. Hence, by Thm 9.1, in the worst case we need at least:

$\log_2 n!$

compare operations.

By Stirling's approximation for factorials

$\Rightarrow \log_2 n! = n \log_2 n - n \log_2 e + O(\log_2 n)$.

Insertion sort:

Input: a list $a_1, \dots, a_n$ of different numbers

Output: a permutation $b_1, \dots, b_n$ of $a_1, \dots, a_n$ such that $b_1 < \dots < b_n$.

Step 1: Choose $B = a_1$

Step k: Assume that we already have a sorted sublist $B = b_1 < \dots < b_k$, $k \le n$.

$k = n \Rightarrow$ done.

$k < n \Rightarrow$ we will add a_{k+1} to get a sorted list $b_1' < \dots < b_k' < b_{k+1}'$.

Compare a_{k+1} with the "modified" median of the list $b_1 < \dots < b_k$, where the modified median is defined as follows:

it is $b_{\frac{k+1}{2}}$ if k is odd

$b_{\left[\frac{k}{2}\right]}$ if k is even.

If $a_{k+1} <$ median, then do again but now with a shorter list $b_1, \dots, b_{\text{median}-1}$

If $a_{k+1} >$ median then do again but now with a shorter list $b_{\text{median}+1}, \dots, b_k$.

Example:

Original list:

4, 8, 9, 5, 2, 1, 6, 7, 3

Step 1: $B = a_1 = 4$

Step 2: insert $a_2 = 8$ into B.

$8 > 4 \Rightarrow B = 4, 8$

Step 3: insert $a_3 = 9$ into B.

Median is $a_1 = 4$.

$9 > 4 \Rightarrow$ try to insert into the second half of B, which is 8.

$9 > 8 \Rightarrow B = 4, 8, 9$.

Step 4: Insert $a_4 = 5$ into $B: 4, 8, 9$ (8: median key)

$5 < 8 \Rightarrow$ insert 5 into the first key of B: 4.

$5 > 4 \Rightarrow B = 4, 5, 8, 9.$

Step 5: Insert 2 into $4, 5, 8, 9$ (5: median)

$2 < 5 \Rightarrow$ insert 2 into 4 (median)

$2 < 4 \Rightarrow 2, 4, 5, 8, 9$

Step 6: Insert 1 into $2, 4, 5, 8, 9$ (4: median)

$1 < 5 \Rightarrow$ insert 1 into $2, 4$ (2: median)

$1 < 2 \Rightarrow B = 1, 2, 4, 5, 8, 9$

Step 7: Insert 6 into $B = 1, 2, 4, 5, 8, 9$ (8: median)

$6 > 4 \Rightarrow$ insert 6 into $5, 8, 9$ (8: median)

$6 < 8 \Rightarrow$ insert 6 into 5

$6 > 5 \Rightarrow B = 1, 2, 4, 5, 6, 8, 9$

Step 8 & Step 9: HW.

Complexity of insertion sort:

When we want to insert a_{k+1} into $B = b_1 < \dots < b_k$, how many operations we need to do? $\sim \log_2 k$ operations (we consecutively divide the list by 2)

We need to do n times $\Rightarrow$ complexity is about:

$\log_2 1 + \log_2 2 + \dots + \log_2 n$

$\simeq$ ~~$n \log_2 n$~~ $O(n \log_2 n)$

$\downarrow$

optimal complexity!

Merge Sort:

Idea: We want to sort a list A of n elements. $A = a_1, \dots, a_n$

We divide A into 2 sublists of approximately the same size, A_1 & A_2. Say $A_1 = a_1, \dots, a_{\lfloor n/2 \rfloor}$, $A_2 = A \setminus A_1$.

We sort A_1 & A_2 ($\downarrow$ B_1: sorted list) ($\downarrow$ B_2: sorted list)

Now we merge B_1 & B_2 into a sorted list B as follows: $b_{1,1}, \dots, b_{1,k}$ $=$ $b_{2,1}, \dots, b_{2,k}$

$B = \emptyset$

Step 1: $B = \text{add } \min\{B_1, B_2\}$ into B

$= \text{add } \min\{b_{1,1}, b_{2,1}\}$ into B

Take the element $\min\{B_1, B_2\}$ out of B_1 or B_2 (depending on where it belongs to).

Step 2: Repeat Step 1 until B_1 or B_2 becomes empty. Then add the remaining list into B.

Example: $A = \{4, 8, 9, 5, 2, 1, 6, 7\}$

$A_1 = \{4, 8, 9, 5\}$

$A_2 = \{2, 1, 6, 7, 3\}$

Sorting $A_1 \Rightarrow B_1 = \{4, 5, 8, 9\}$

Sorting $A_2 \Rightarrow B_2 = \{1, 2, 3, 6, 7\}$

Step 1: $B = \emptyset$

$\min\{B_1, B_2\} = \min\{4, 1\} = 1.$

$B = B + \{1\} = \{1\}$

$B_1 = \{4, 5, 8, 9\}$

$B_2 = B_2 \setminus \{1\} = \{2, 3, 6, 7\}$

Step 2: $\min\{B_1, B_2\} = \min\{4, 2\} = 2$

$B = \{1, 2\}$

$B_1 = \{4, 5, 8, 9\}$

$B_2 = \{3, 6, 7\}$

Step 3: $B = \{1, 2, 3\}$

$B_1 = \{4, 5, 8, 9\}$

$B_2 = \{6, 7\}$

Step 4: $B = \{1, 2, 3, 4\}$

$B_1 = \{5, 8, 9\}$

$B_2 = \{6, 7\}$

Step 5: $B = \{1, 2, 3, 4, 5\}$

$B_1 = \{8, 9\}$

$B_2 = \{6, 7\}$

Step 6: $B = \{1, 2, 3, 4, 5, 6\}$

$B_1 = \{8, 9\}$

$B_2 = \{7\}$

Step 7: $B = \{1, 2, 3, 4, 5, 6, 7\}$

$B_1 = \{8, 9\}$, $B_2 = \emptyset$

$B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}.$

Quick sort: In practice, when using merge sort we can use recurrence to also sort A_1 & A_2 using Merge sort.

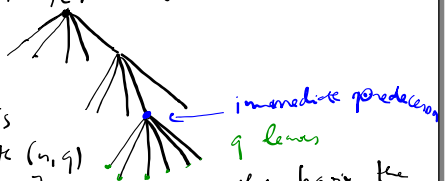
Quick sort $A = (\text{Quick sort}(A_1), \text{Quick sort}(A_2))$ (Merge sort)

Thm: Complexity of Quick sort is also $O(n \log_2 n)$. (optimal)

Proof: See the

Q: If T is a complete (n,q)-tree then $q-1 \mid n-1$.

For example, can prove by induction w.r.t n.



Because T is a complete (n,q)-tree $\Rightarrow \exists$ q leaves that have the same immediate predecessor.

If we delete the q green leaves, we get a new tree which is complete $(n-q+1, q)$-tree leaves.

$q-1 \mid (n-q+1)-1 = n-q$

$\Rightarrow q-1 \mid (n-1) = (n-q)+(q-1)$

(Q.E.D.)

9.4. Binary search tree

~~One way to~~

~~Q:~~ Look into the book.

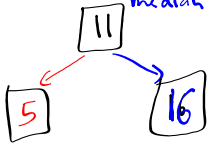
A binary tree is that:

For each vertex x, every ~~the~~ successors of x on the left is $< x$ & every successors of x on the right is $> x$.

Usually, the way to construct is to make the median to be the root.

$\{(2, 4, 5, 7, 8, 10), 11, (12, 13, 15, 16, 18, 20)\}$

median median



Chapter 12: Modular Arithmetic

§12.1: Congruence

Let $m \neq 0, 1$ be an integer.

We say that $a \equiv b \pmod m$ iff $a-b$ is divisible by m.

Example: $7 \equiv 2 \pmod{-5}$

$6 \equiv -1 \pmod 7$

Properties: $a_1 \overset{(\bmod m)}{\equiv} a_2$ & $b_1 \equiv b_2 \pmod m$:

$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m$

$a_1 a_2 \equiv b_1 b_2 \pmod m$

Prof: Easy. (Q.E.D)

Example: $1 \equiv 10001 \pmod{10000}$

$2 \equiv 10002 \pmod{10000}$

$\Rightarrow 1 \times 2 \equiv 10001 \times 10002 \pmod{10000}$

Property: $\equiv$ is an equivalence relation.

Prof: Reflexive $a \equiv a \pmod m$

Symmetric: $a \equiv b \pmod m \Rightarrow a-b$ is divisible by $m \Rightarrow b-a = -(a-b)$ is also divisible by $m \Rightarrow b \equiv a \pmod m$

Transitive: $a \equiv b \pmod m$ & $b \equiv c \pmod m \Rightarrow a-b$ is divisible by m & $b-c$ is divisible by m

$\Rightarrow a-c = (a-b)+(b-c)$ is divisible by m.

Definition: $\mathbb{Z}_m = \mathbb{Z}/m$

$\overset{\text{def}}{=} \mathbb{Z}/\equiv \pmod m$

Property: $\mathbb{Z}/m$ is a ring wrt unity.

Prof: Use the addition & multiplication & 0, & 1 for $\mathbb{Z}$. (Q.E.D)

Example: What is $\mathbb{Z}/6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Addition

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	6=0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplication

Invertible elements in $\mathbb{Z}/m$:

$x \in \mathbb{Z}/m$ is invertible if $\forall z \in \mathbb{Z}/m$, $\exists y \in \mathbb{Z}/m$ such that $xy = z$.

Properties:

(1) x is invertible in $\mathbb{Z}/m$ iff $\exists y_0 \in \mathbb{Z}/m$ s.t. $xy_0 = 1$ in $\mathbb{Z}/m$.

(Prof: if $xy_0 = 1$

$\Rightarrow x.(y_0 z) = z \quad \forall z$)

(2) x is invertible in $\mathbb{Z}/m$ iff x & m have no common divisor.

(Prof: Use Euclidean's division algorithm)

↳ Example: Show that 5 is invertible in $\mathbb{Z}/6$?

Euclidean algorithm for 5 & 6:

$6 = 5 \cdot 1 + 1$

$\Rightarrow 5 \cdot 1 + 1 \equiv 0 \pmod 6$

$\Rightarrow 5 \cdot 1 \equiv -1 \pmod 6$

$\Rightarrow 5(-1) \equiv 1 \pmod 6$

Use (1) of the properties.

Show that 35 is invertible in $\mathbb{Z}/6$.

Euclidean's algorithm for 35 & 6:

$35 = 6 \times 5 + 5$

$6 = 5 \times 1 + 1$

$\Rightarrow 35 \equiv 5 \equiv -1 \pmod 6$

Question: R

Def: A field is a ring with unity so that every non-zero element is invertible.

(i.e. $\forall x \in R, x \neq 0$

$\Rightarrow y \in R : xy = 1$)

Example: $\mathbb{Z}/6$ is not invertible.

Q: When is $\mathbb{Z}/n$ invertible? ($n \geq 2$)

First, $\mathbb{Z}/n$ is finite & is represented by $0, 1, \dots, n-1$.

By the property before, an element $x \in \mathbb{Z}/n$ is invertible iff $GCD(x, n) = 1$. ($n \geq 2$)

(Greatest Common divisor)

Thm: $\mathbb{Z}/n$ is a field $\Leftrightarrow$ n is a prime number.

Proof: $\mathbb{Z}/n$ is a field $\Leftrightarrow \forall x \in \{1, \dots, n-1\} \Rightarrow GCD(x, n) = 1$.

$\Leftrightarrow n$ is a prime number. (Q.E.D.)

Example:

$\mathbb{Z}/101$ is a field

$\mathbb{Z}/49$ is not a field.

$49 = 7 \times 7$.

Corollary: For every prime number p, there is a field with p elements.

Proof: $\mathbb{Z}/p$ has p elements $0, 1, \dots, p-1$, & is a field. (Q.E.D.).

§12.2 Finite fields

Q: If $n \geq 2$ is a positive integer, is there a field F with exactly n elements?

Thm: There is a field F with exactly n elements iff $\exists$ a prime number p & a positive integer k s.t. $n = p^k$. p is called the characteristic of F.

Proof: ($\Rightarrow$) If F has elements $\Rightarrow n = p^k$ quite complicated. Proof omitted.

($\Leftarrow$) If $n = p^k$ we will construct a field F with n elements.

(Q.E.D.)

Example: Construct a field with $n = 3^2$ elements. Not obvious:

$\mathbb{Z}/3 \times \mathbb{Z}/3$ is not a field.

Because $(3,1)$ the unit of "this field" would be $(1,1)$. Now $(0,1) \neq (0,0)$, but there is no $(x_1, x_2) \in \mathbb{Z}/3 \times \mathbb{Z}/3$ such that $(0,1) \times (x_1, x_2) = (1,1)$.

The "heuristic" way to go is this:

look at the equation $z^9 = z$.

(Use that if F is a field with n elements & $z \in F$, $z \neq 0 \Rightarrow z^{n-1} = 1$.)

Now consider the 9 solutions in $\mathbb{C}$ of this. But we impose also the condition that for these numbers ζ_i we have:

$3\zeta_i = 0$. (not true if $3 \in \mathbb{Q}$, $3 \neq 0$)

Then check that this is a field with 9 elements: $\zeta_i^9 = \zeta_i \quad \forall i = 0, \ldots, 8$

Check that $\zeta_i + \zeta_j$ also satisfies this equation:

$$(\zeta_i + \zeta_j)^9 = \zeta_i^9 + 9\zeta_i^8\zeta_j + 36\zeta_i^7\zeta_j^2 + \cdots + 9\zeta_i\zeta_j^8 + \zeta_j^9$$

(ζ_i, 0, ζ_j)

ζ_i

$\zeta_i + \zeta_j \in F$.

$\zeta_i^9 = \zeta_i \quad (\zeta_i \neq 0)$

$\Rightarrow \left(\frac{1}{\zeta_i}\right)^9 = \frac{1}{\zeta_i}$ ✓ inverse to ζ_i.

$\Rightarrow$ $\forall \zeta_i \in F \Rightarrow \frac{1}{\zeta_i} \in F$.

Thm: Up to isomorphisms, there is only a unique field with $n = p^k$ elements.