Randomised Algorithms

Lecture 3: Concentration Inequalities, Application to Quick-Sort, Extensions

Thomas Sauerwald (tms41@cam.ac.uk)

Lent 2025



Outline

Application 2: Randomised QuickSort

Extensions of Chernoff Bounds

Applications of Method of Bounded Differences

QuickSort

```
QUICKSORT (Input A[1], A[2], \ldots, A[n])
1: Pick an element from the array, the so-called pivot
2. If n = 0 or n = 1 then
3.
       return A
4. else
5:
        Create two subarrays A_1 and A_2 (without the pivot) such that:
           A_1 contains the elements that are smaller than the pivot
6.
           A_2 contains the elements that are greater (or equal) than the pivot
7:
        QUICKSORT(A_1)
8.
        QUICKSORT(A_2)
9:
        return A
10.
```

```
QUICKSORT (Input A[1], A[2], \ldots, A[n])
 1: Pick an element from the array, the so-called pivot
 2. If n = 0 or n = 1 then
3.
        return A
4. else
        Create two subarrays A_1 and A_2 (without the pivot) such that:
 5:
           A_1 contains the elements that are smaller than the pivot
6.
            A<sub>2</sub> contains the elements that are greater (or equal) than the pivot
7:
        QUICKSORT(A_1)
8.
        QUICKSORT(A_2)
9:
        return A
10.
```

• Example: Let A = (2, 8, 9, 1, 7, 5, 6, 3, 4) with A[7] = 6 as pivot.

```
QUICKSORT (Input A[1], A[2], \ldots, A[n])
 1: Pick an element from the array, the so-called pivot
 2. If n = 0 or n = 1 then
3.
        return A
4. else
 5:
        Create two subarrays A_1 and A_2 (without the pivot) such that:
           A_1 contains the elements that are smaller than the pivot
6.
           A<sub>2</sub> contains the elements that are greater (or equal) than the pivot
 7:
        QUICKSORT(A_1)
8.
        QUICKSORT(A_2)
9:
        return A
10.
```

• Example: Let A = (2, 8, 9, 1, 7, 5, 6, 3, 4) with A[7] = 6 as pivot.

 $\Rightarrow A_1 = (2, 1, 5, 3, 4) \text{ and } A_2 = (8, 9, 7)$

```
QUICKSORT (Input A[1], A[2], \ldots, A[n])
1: Pick an element from the array, the so-called pivot
2. If n = 0 or n = 1 then
3.
       return A
4. else
5:
        Create two subarrays A_1 and A_2 (without the pivot) such that:
           A_1 contains the elements that are smaller than the pivot
6.
           A<sub>2</sub> contains the elements that are greater (or equal) than the pivot
7:
        QUICKSORT(A_1)
8.
        QUICKSORT(A_2)
9:
        return A
10.
```

 $\Rightarrow A_1 = (2, 1, 5, 3, 4) \text{ and } A_2 = (8, 9, 7)$

• Example: Let A = (2, 8, 9, 1, 7, 5, 6, 3, 4) with A[7] = 6 as pivot.

• Worst-Case Complexity (number of comparisons) is $\Theta(n^2)$,

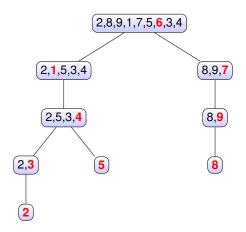
```
QUICKSORT (Input A[1], A[2], \ldots, A[n])
1: Pick an element from the array, the so-called pivot
2. If n = 0 or n = 1 then
3.
       return A
4. else
5:
        Create two subarrays A_1 and A_2 (without the pivot) such that:
           A_1 contains the elements that are smaller than the pivot
6.
           A<sub>2</sub> contains the elements that are greater (or equal) than the pivot
7:
        QUICKSORT(A_1)
8.
        QUICKSORT(A_2)
9:
        return A
10.
```

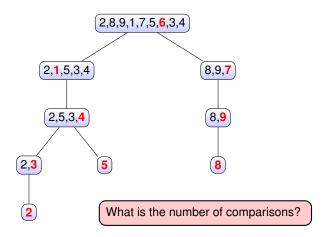
- Example: Let A = (2, 8, 9, 1, 7, 5, 6, 3, 4) with A[7] = 6 as pivot. $\Rightarrow A_1 = (2, 1, 5, 3, 4)$ and $A_2 = (8, 9, 7)$
- Worst-Case Complexity (number of comparisons) is Θ(n²),
 while Average-Case Complexity is O(n log n).

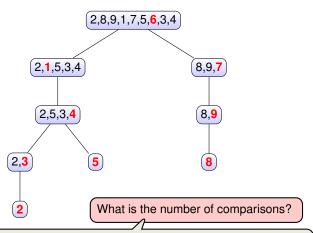
```
QUICKSORT (Input A[1], A[2], \ldots, A[n])
1: Pick an element from the array, the so-called pivot
2. If n = 0 or n = 1 then
3.
       return A
4. else
5:
        Create two subarrays A_1 and A_2 (without the pivot) such that:
           A_1 contains the elements that are smaller than the pivot
6.
           A<sub>2</sub> contains the elements that are greater (or equal) than the pivot
7:
        QUICKSORT(A_1)
8.
        QUICKSORT(A_2)
9:
        return A
10.
```

- Example: Let A = (2, 8, 9, 1, 7, 5, 6, 3, 4) with A[7] = 6 as pivot. $\Rightarrow A_1 = (2, 1, 5, 3, 4)$ and $A_2 = (8, 9, 7)$
- Worst-Case Complexity (number of comparisons) is $\Theta(n^2)$, while Average-Case Complexity is $O(n \log n)$.

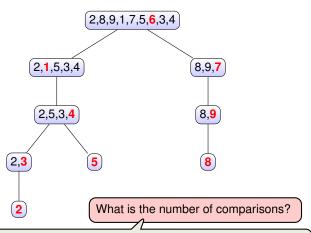
We will now give a proof of this "well-known" result!







Note that the number of comparison by QUICKSORT is equivalent to the sum of the depths of all nodes in the tree (why?).



Note that the number of comparison by QUICKSORT is equivalent to the sum of the depths of all nodes in the tree (why?). In this case:

$$0+1+1+2+2+3+3+3+4=19.$$

How to pick a good pivot? We don't, just pick one at random.

How to pick a good pivot? We don't, just pick one at random.

This should be your standard answer in this course ©

How to pick a good pivot? We don't, just pick one at random.

This should be your standard answer in this course $\ensuremath{\mathfrak{D}}$

Let us analyse QUICKSORT with random pivots.

How to pick a good pivot? We don't, just pick one at random.

This should be your standard answer in this course ©

Let us analyse QUICKSORT with random pivots.

1. Assume A consists of *n* different numbers, w.l.o.g., {1,2,...,n}

How to pick a good pivot? We don't, just pick one at random.

This should be your standard answer in this course ©

Let us analyse QUICKSORT with random pivots.

- 1. Assume A consists of n different numbers, w.l.o.g., $\{1, 2, ..., n\}$
- 2. Let H_i be the deepest level where element i appears in the tree. Then the number of comparison is $H = \sum_{i=1}^{n} H_i$

How to pick a good pivot? We don't, just pick one at random.

This should be your standard answer in this course ©

Let us analyse QUICKSORT with random pivots.

- 1. Assume A consists of n different numbers, w.l.o.g., $\{1, 2, ..., n\}$
- 2. Let H_i be the deepest level where element i appears in the tree. Then the number of comparison is $H = \sum_{i=1}^{n} H_i$
- 3. We will prove that there exists C > 0 such that

$$\mathbf{P}[H \le Cn\log n] \ge 1 - n^{-1}.$$

How to pick a good pivot? We don't, just pick one at random.

This should be your standard answer in this course ©

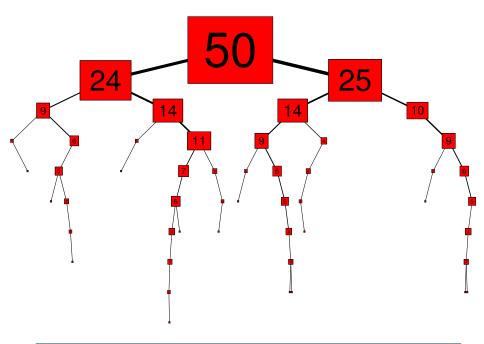
Let us analyse QUICKSORT with random pivots.

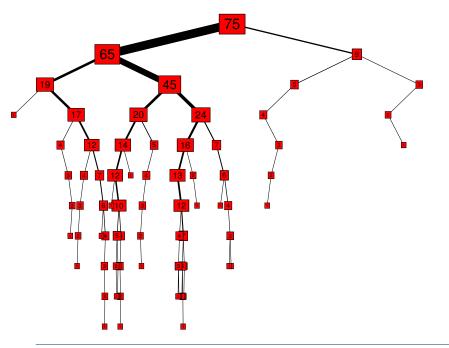
- 1. Assume A consists of n different numbers, w.l.o.g., $\{1, 2, ..., n\}$
- 2. Let H_i be the deepest level where element i appears in the tree. Then the number of comparison is $H = \sum_{i=1}^{n} H_i$
- 3. We will prove that there exists C > 0 such that

$$P[H \le Cn \log n] \ge 1 - n^{-1}$$
.

4. Actually, we will prove sth slightly stronger:

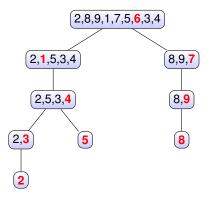
$$\mathbf{P}\left[\bigcap_{i=1}^n \{H_i \leq C \log n\}\right] \geq 1 - n^{-1}.$$



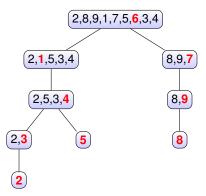


Let P be a path from the root to the deepest level of some element

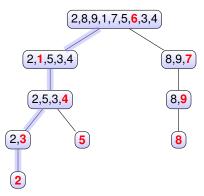
Let P be a path from the root to the deepest level of some element



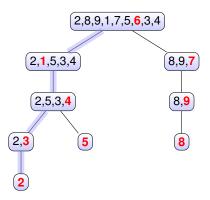
Let P be a path from the root to the deepest level of some element



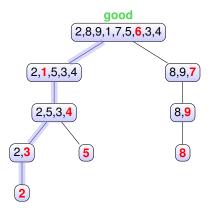
Let P be a path from the root to the deepest level of some element



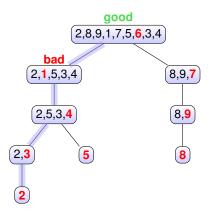
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad



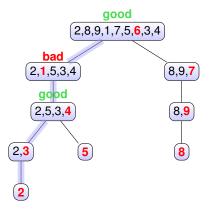
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad



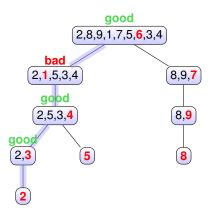
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad



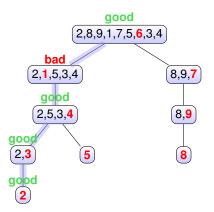
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad



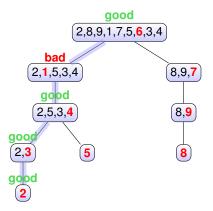
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad



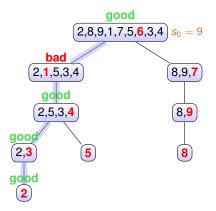
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad



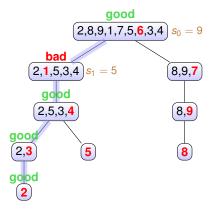
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad
- Further let s_t be the size of the array at level t in P.



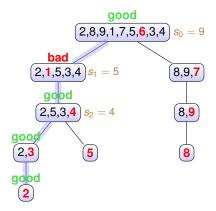
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad
- Further let s_t be the size of the array at level t in P.



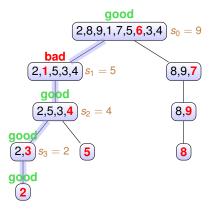
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad
- Further let s_t be the size of the array at level t in P.



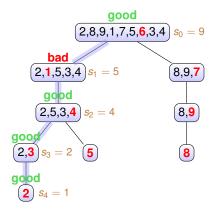
- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad
- Further let s_t be the size of the array at level t in P.



- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad
- Further let s_t be the size of the array at level t in P.



- Let P be a path from the root to the deepest level of some element
 - A node in P is called good if the corresponding pivot partitions the array into two subarrays each of size at most 2/3 of the previous one
 - otherwise, the node is bad
- Further let s_t be the size of the array at level t in P.



■ Element 2: $(2,8,9,1,7,5,6,3,4) \rightarrow (2,1,5,3,4) \rightarrow (2,5,3,4) \rightarrow (2,3) \rightarrow (2)$

• Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For *P* to proceed from level *k* to k + 1, the condition $s_k > 1$ is necessary

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For *P* to proceed from level *k* to k + 1, the condition $s_k > 1$ is necessary

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For P to proceed from level k to k+1, the condition $s_k > 1$ is necessary

How far could such a path P possibly run until we have $s_k = 1$?

• We start with $s_0 = n$

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For P to proceed from level k to k+1, the condition $s_k > 1$ is necessary

- We start with s₀ = n
- First Case, good node: $s_{k+1} \leq \frac{2}{3} \cdot s_k$.

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For P to proceed from level k to k+1, the condition $s_k > 1$ is necessary

- We start with s₀ = n
- First Case, good node: $s_{k+1} \leq \frac{2}{3} \cdot s_k$.
- Second Case, bad node: $s_{k+1} \le s_k$.

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For *P* to proceed from level *k* to k + 1, the condition $s_k > 1$ is necessary

- We start with s₀ = n
- First Case, good node: $s_{k+1} \leq \frac{2}{3} \cdot s_k$.
- Second Case, bad node: $s_{k+1} \le s_k$.
- \Rightarrow There are at most $T = \frac{\log n}{\log(3/2)} < 3 \log n$ many good nodes on any path P.

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For P to proceed from level k to k+1, the condition $s_k > 1$ is necessary

How far could such a path P possibly run until we have $s_k = 1$?

- We start with s₀ = n
- First Case, good node: $s_{k+1} \leq \frac{2}{3} \cdot s_k$.
- Second Case, bad node: $s_{k+1} \le s_k$.

This even holds always, i.e., deterministically!

⇒ There are at most $T = \frac{\log n}{\log(3/2)} < 5 \log n$ many good nodes on any path P.

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For P to proceed from level k to k+1, the condition $s_k > 1$ is necessary

How far could such a path P possibly run until we have $s_k = 1$?

- We start with s₀ = n
- First Case, good node: $s_{k+1} \leq \frac{2}{3} \cdot s_k$. This
- Second Case, bad node: $s_{k+1} \le s_k$.

This even holds always, i.e., deterministically!

.....

- \Rightarrow There are at most $T = \frac{\log n}{\log(3/2)} < \overline{3} \log n$ many good nodes on any path P.
 - Assume $|P| \ge C \log n$ for C := 24

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For P to proceed from level k to k + 1, the condition $s_k > 1$ is necessary

How far could such a path P possibly run until we have $s_k = 1$?

- We start with s₀ = n
- First Case, good node: $s_{k+1} \le \frac{2}{3} \cdot s_k$. This even holds always,
- Second Case, bad node: $s_{k+1} \leq s_k$.

i.e., deterministically!

- \Rightarrow There are at most $T = \frac{\log n}{\log(3/2)} < \overline{3} \log n$ many good nodes on any path P.
 - Assume $|P| \ge C \log n$ for C := 24
 - \Rightarrow number of **bad** nodes in the first 24 log *n* levels is more than 21 log *n*.

- Consider now any element $i \in \{1, 2, ..., n\}$ and construct the path P = P(i) one level by one
- For P to proceed from level k to k + 1, the condition $s_k > 1$ is necessary

How far could such a path P possibly run until we have $s_k = 1$?

- We start with s₀ = n
- First Case, good node: $s_{k+1} \leq \frac{2}{3} \cdot s_k$.
- Second Case, bad node: $s_{k+1} \leq s_k$.

This even holds always,

i.e., deterministically!

- \Rightarrow There are at most $T = \frac{\log n}{\log(3/2)} < 3 \log n$ many good nodes on any path P.
 - Assume $|P| \ge C \log n$ for C := 24
 - \Rightarrow number of **bad** nodes in the first 24 log *n* levels is more than 21 log *n*.

Let us now upper bound the probability that this "bad event" happens!

• Consider the first 24 log *n* nodes of *P* to the deepest level of element *i*.

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, ..., 24 \log n 1\}$, define an indicator variable X_j :

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

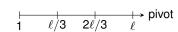
- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.
- **P**[$X_i = 1 \mid X_0 = X_0, \dots, X_{i-1} = X_{i-1}$] $\leq \frac{2}{3}$

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■ **P**[
$$X_j = 1 \mid X_0 = x_0, \dots, X_{j-1} = x_{j-1}$$
] $\leq \frac{2}{3}$



- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■ **P**[
$$X_j = 1 \mid X_0 = x_0, \dots, X_{j-1} = x_{j-1}$$
] $\leq \frac{2}{3}$

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■
$$P[X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}] \le \frac{2}{3}$$



Question: Edge Case: What if the path P does not reach level j?

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■ P[
$$X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}$$
] $\leq \frac{2}{3}$





Question: Edge Case: What if the path P does not reach level j?

Answer: We can then simply define X_i as 0.

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■
$$P[X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}] \le \frac{2}{3}$$

1 $\ell/3$ $2\ell/3$ ℓ

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)



Question: Edge Case: What if the path P does not reach level j?

Answer: We can then simply define X_i as 0.

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_i = 0 if the node at level j is good.

■
$$P[X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}] \le \frac{2}{3}$$
 1 $\ell/3$ 2 $\ell/3$ ℓ

• $X := \sum_{i=0}^{24 \log n-1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■
$$P[X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}] \le \frac{2}{3}$$
 1 $\ell/3$ $2\ell/3$ ℓ

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■
$$P[X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}] \le \frac{2}{3}$$
 1 $\ell/3$ $2\ell/3$ ℓ

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

We can now apply a **Chernoff Bound!** (We use the "nice" version.)

• We have **E** [X] \leq (2/3) \cdot 24 log $n = 16 \log n$

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :

 - X_j = 1 if the node at level j is bad,
 X_i = 0 if the node at level j is good.

■
$$P[X_j = 1 \mid X_0 = x_0, \dots, X_{j-1} = x_{j-1}] \le \frac{2}{3}$$
 1 $\ell/3$ $2\ell/3$ ℓ

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- We have **E** [X] \leq (2/3) \cdot 24 log $n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■ **P**[
$$X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}$$
] $\leq \frac{2}{3}$

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- We have **E** [X] \leq (2/3) \cdot 24 log $n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds $\sqrt{\mathbf{P}[X \ge \mathbf{E}[X] + t]} \le e^{-2t^2/n}$

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

• **P**[
$$X_j = 1 \mid X_0 = x_0, \dots, X_{j-1} = x_{j-1}$$
] $\leq \frac{2}{3}$

$$\begin{array}{c|c}
 & \text{bad} & \text{good} & \text{bad} \\
1 & \ell/3 & 2\ell/3 & \ell
\end{array}$$
 pivo

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- We have **E** [X] \leq (2/3) \cdot 24 log $n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds $\left\{ \mathbf{P}[X \geq \mathbf{E}[X] + t] \leq e^{-2t^2/n} \right\}$

$$P[X > 21 \log n] \le P[X > E[X] + 5 \log n]$$

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■ **P**[
$$X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}$$
] $\leq \frac{2}{3}$

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- We have **E** [X] \leq (2/3) \cdot 24 log $n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds $\left\{ \mathbf{P}[X \geq \mathbf{E}[X] + t] \leq e^{-2t^2/n} \right\}$

$$P[X > 21 \log n] \le P[X > E[X] + 5 \log n] \le e^{-2(5 \log n)^2/(24 \log n)}$$

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■
$$P[X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}] \le \frac{2}{3}$$
 | $\ell/3$ | $2\ell/3$ | $\ell/3$ | $\ell/3$

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- We have **E** [X] \leq (2/3) \cdot 24 log $n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds $\{ \mathbf{P}[X \ge \mathbf{E}[X] + t] \le e^{-2t^2/n} \}$ $\{ \mathbf{P}[X > 21 \log n] \le \mathbf{P}[X > \mathbf{E}[X] + 5 \log n] \le e^{-2(5 \log n)^2/(24 \log n)} \le n^{-2} \}$

$$P[X > 21 \log n] \le P[X > E[X] + 5 \log n] \le e^{-2(5 \log n)^2/(24 \log n)} \le n^{-2}$$

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

•
$$P[X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}] \le \frac{2}{3}$$

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

We can now apply a **Chernoff Bound!** (We use the "nice" version.)

- We have **E** [X] \leq (2/3) \cdot 24 log $n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds $\left\{ \mathbf{P}[X \geq \mathbf{E}[X] + t] \leq e^{-2t^2/n} \right\}$

$$P[X > 21 \log n] \le P[X > E[X] + 5 \log n] \le e^{-2(5 \log n)^2/(24 \log n)} \le n^{-2}$$

• Hence P has more than $24 \log n$ nodes with probability at most n^{-2} .

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_i = 0 if the node at level j is good.

■ **P**[
$$X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}$$
] $\leq \frac{2}{3}$

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- We have $\mathbf{E}[X] \le (2/3) \cdot 24 \log n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds $\left\{ \mathbf{P}[X \geq \mathbf{E}[X] + t] \leq e^{-2t^2/n} \right\}$

$$P[X > 21 \log n] \le P[X > E[X] + 5 \log n] \le e^{-2(5 \log n)^2/(24 \log n)} \le n^{-2}$$

- Hence P has more than $24 \log n$ nodes with probability at most n^{-2} .
- As there are in total n paths, by the union bound, the probability that at least one of them has more than $24 \log n$ nodes is at most n^{-1} .

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

■
$$P[X_j = 1 \mid X_0 = x_0, ..., X_{j-1} = x_{j-1}] \le \frac{2}{3}$$
 1 $\ell/3$ $2\ell/3$ ℓ

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- We have $\mathbf{E}[X] \le (2/3) \cdot 24 \log n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds $\left\{ \mathbf{P}[X \geq \mathbf{E}[X] + t] \leq e^{-2t^2/n} \right\}$ $P[X > 21 \log n] \le P[X > E[X] + 5 \log n] \le e^{-2(5 \log n)^2/(24 \log n)} < n^{-2}$
- Hence P has more than $24 \log n$ nodes with probability at most n^{-2} .
- As there are in total n paths, by the union bound, the probability that at least one of them has more than $24 \log n$ nodes is at most n^{-1} .
- This implies $P \left[\bigcap_{i=1}^{n} \{H_i \le 24 \log n\} \right] \ge 1 n^{-1}$, as needed.

- Consider the first 24 log n nodes of P to the deepest level of element i.
- For any level $j \in \{0, 1, \dots, 24 \log n 1\}$, define an indicator variable X_i :
 - X_j = 1 if the node at level j is bad,
 X_j = 0 if the node at level j is good.

• **P**[
$$X_j = 1 \mid X_0 = X_0, \dots, X_{j-1} = X_{j-1}$$
] $\leq \frac{2}{3}$

$$\begin{array}{c|c}
 & \text{bad} & \text{good} & \text{bad} \\
1 & \ell/3 & 2\ell/3 & \ell
\end{array}$$
 pivo

• $X := \sum_{i=0}^{24 \log n - 1} X_i$ satisfies relaxed independence assumption (Lecture 2)

- We have $\mathbf{E}[X] \le (2/3) \cdot 24 \log n = 16 \log n$
- Then, by the "nicer" Chernoff Bounds $\left\{ \mathbf{P}[X \geq \mathbf{E}[X] + t] \leq e^{-2t^2/n} \right\}$

$$P[X > 21 \log n] \le P[X > E[X] + 5 \log n] \le e^{-2(5 \log n)^2/(24 \log n)} \le n^{-2}$$

- Hence P has more than $24 \log n$ nodes with probability at most n^{-2} .
- As there are in total n paths, by the union bound, the probability that at least one of them has more than $24 \log n$ nodes is at most n^{-1} .
- This implies $P \left[\bigcap_{i=1}^{n} \{H_i \le 24 \log n\} \right] \ge 1 n^{-1}$, as needed.

Randomised QuickSort: Final Remarks

- Well-known: any comparison-based sorting algorithm needs $\Omega(n \log n)$
- A classical result: expected number of comparison of randomised QUICKSORT is $2n \log n + O(n)$ (see, e.g., book by Mitzenmacher & Upfal)

Randomised QuickSort: Final Remarks

- Well-known: any comparison-based sorting algorithm needs $\Omega(n \log n)$
- A classical result: expected number of comparison of randomised QUICKSORT is $2n \log n + O(n)$ (see, e.g., book by Mitzenmacher & Upfal)



Exercise: [Ex 2-3.6] Our upper bound of $O(n \log n)$ whp also immediately implies a $O(n \log n)$ bound on the expected number of comparisons!

Randomised QuickSort: Final Remarks

- Well-known: any comparison-based sorting algorithm needs $\Omega(n \log n)$
- A classical result: expected number of comparison of randomised QUICKSORT is $2n \log n + O(n)$ (see, e.g., book by Mitzenmacher & Upfal)



Exercise: [Ex 2-3.6] Our upper bound of $O(n \log n)$ whp also immediately implies a $O(n \log n)$ bound on the expected number of comparisons!

- It is possible to deterministically find the best pivot element that divides the array into two subarrays of the same size.
- The latter requires to compute the median of the array in linear time, which is not easy...
- The presented randomised algorithm for QUICKSORT is much easier to implement!

Outline

Application 2: Randomised QuickSort

Extensions of Chernoff Bounds

Applications of Method of Bounded Differences

 Besides sums of independent Bernoulli random variables, sums of independent and bounded random variables are very frequent in applications.

- Besides sums of independent Bernoulli random variables, sums of independent and bounded random variables are very frequent in applications.
- Unfortunately the distribution of the X_i may be unknown or hard to compute, thus it will be hard to compute the moment-generating function.

- Besides sums of independent Bernoulli random variables, sums of independent and bounded random variables are very frequent in applications.
- Unfortunately the distribution of the X_i may be unknown or hard to compute, thus it will be hard to compute the moment-generating function.
- Hoeffding's Lemma helps us here:

- Besides sums of independent Bernoulli random variables, sums of independent and bounded random variables are very frequent in applications.
- Unfortunately the distribution of the X_i may be unknown or hard to compute, thus it will be hard to compute the moment-generating function.
- Hoeffding's Lemma helps us here:

Hoeffding's Extension Lemma ———

Let X be a random variable with mean 0 such that $a \leq X \leq b$. Then for all $\lambda \in \mathbb{R}$,

$$\mathbf{E}\left[e^{\lambda X}\right] \leq \exp\left(\frac{(b-a)^2\lambda^2}{8}\right)$$

- Besides sums of independent Bernoulli random variables, sums of independent and bounded random variables are very frequent in applications.
- Unfortunately the distribution of the X_i may be unknown or hard to compute, thus it will be hard to compute the moment-generating function.

• Hoeffding's Lemma helps us here: You can always consider $X' = X - \mathbf{E}[X]$

Hoeffding's Extension Lemma -

Let X be a random variable with mean 0 such that a < X < b. Then for all $\lambda \in \mathbb{R}$,

$$\mathbf{E}\left[e^{\lambda X}\right] \leq \exp\left(\frac{(b-a)^2\lambda^2}{8}\right)$$

- Besides sums of independent Bernoulli random variables, sums of independent and bounded random variables are very frequent in applications.
- Unfortunately the distribution of the X_i may be unknown or hard to compute, thus it will be hard to compute the moment-generating function.

• Hoeffding's Lemma helps us here: You can always consider
$$X' = X - \mathbf{E}[X]$$

Hoeffding's Extension Lemma —

Let X be a random variable with mean 0 such that a < X < b. Then for all $\lambda \in \mathbb{R}$,

$$\mathbf{E}\left[e^{\lambda X}\right] \leq \exp\left(\frac{(b-a)^2\lambda^2}{8}\right)$$

We omit the proof of this lemma!

Hoeffding Bounds

Hoeffding's Inequality

Let X_1,\ldots,X_n be independent random variables with mean μ_i such that $a_i \leq X_i \leq b_i$. Let $X = X_1 + \ldots + X_n$, and let $\mu = \mathbf{E}[X] = \sum_{i=1}^n \mu_i$. Then for any t > 0,

$$\mathbf{P}[X \ge \mu + t] \le \exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right),\,$$

and

$$\mathbf{P}[X \leq \mu - t] \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right).$$

Hoeffding Bounds

Hoeffding's Inequality

Let X_1,\ldots,X_n be independent random variables with mean μ_i such that $a_i \leq X_i \leq b_i$. Let $X = X_1 + \ldots + X_n$, and let $\mu = \mathbf{E}[X] = \sum_{i=1}^n \mu_i$. Then for any t > 0,

$$\mathbf{P}[X \ge \mu + t] \le \exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right),\,$$

and

$$\mathbf{P}[X \leq \mu - t] \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n (b_i - a_i)^2}\right).$$

Proof Outline (skipped):

■ Let
$$X_i' = X_i - \mu_i$$
 and $X' = X_1' + \ldots + X_n'$, then $\mathbf{P}[X \ge \mu + t] = \mathbf{P}[X' \ge t]$

$$\bullet \ \mathbf{P}[\,X' \geq t\,] \leq e^{-\lambda t} \textstyle\prod_{i=1}^n \mathbf{E}\left[\,e^{\lambda X_i'}\,\right] \leq \exp\left[-\lambda t + \frac{\lambda^2}{8} \textstyle\sum_{i=1}^n (b_i - a_i)^2\right]$$

■ Choose $\lambda = \frac{4t}{\sum_{i=1}^{n} (b_i - a_i)^2}$ to get the result.

This is not "magic" – you just need to optimise λ !

Framework -

Suppose, we have independent random variables X_1, \ldots, X_n . We want to study the random variable:

$$f(X_1,\ldots,X_n)$$

Framework -

Suppose, we have independent random variables X_1, \ldots, X_n . We want to study the random variable:

$$f(X_1,\ldots,X_n)$$

Some examples:

1. $X = X_1 + ... + X_n$ (our setting earlier)

Framework

Suppose, we have independent random variables X_1, \ldots, X_n . We want to study the random variable:

$$f(X_1,\ldots,X_n)$$

Some examples:

- 1. $X = X_1 + \ldots + X_n$ (our setting earlier)
- 2. In balls into bins, X_i indicates where ball i is allocated, and $f(X_1, \ldots, X_m)$ is the number of empty bins

Framework

Suppose, we have independent random variables X_1, \ldots, X_n . We want to study the random variable:

$$f(X_1,\ldots,X_n)$$

Some examples:

- 1. $X = X_1 + \ldots + X_n$ (our setting earlier)
- 2. In balls into bins, X_i indicates where ball i is allocated, and $f(X_1, \ldots, X_m)$ is the number of empty bins
- 3. In a randomly generated graph, X_i indicates if the *i*-th edge is present and $f(X_1, \ldots, X_{\binom{n}{2}})$ represents the number of connected components of G

Framework

Suppose, we have independent random variables X_1, \ldots, X_n . We want to study the random variable:

$$f(X_1,\ldots,X_n)$$

Some examples:

- 1. $X = X_1 + ... + X_n$ (our setting earlier)
- 2. In balls into bins, X_i indicates where ball i is allocated, and $f(X_1, \ldots, X_m)$ is the number of empty bins
- 3. In a randomly generated graph, X_i indicates if the *i*-th edge is present and $f(X_1, \ldots, X_{\binom{n}{2}})$ represents the number of connected components of G

In all those cases (and more) we can easily prove concentration of $f(X_1, ..., X_n)$ around its mean by the so-called **Method of Bounded Differences**.

A function f is called Lipschitz with parameters $\mathbf{c} = (c_1, \dots, c_n)$ if for all $i = 1, 2, \dots, n$,

$$|f(x_1, x_2, \ldots, x_{i-1}, \mathbf{x}_i, x_{i+1}, \ldots, x_n) - f(x_1, x_2, \ldots, x_{i-1}, \widetilde{\mathbf{x}}_i, x_{i+1}, \ldots, x_n)| \leq c_i$$

where x_i and \tilde{x}_i are in the domain of the *i*-th coordinate.

A function f is called Lipschitz with parameters $\mathbf{c} = (c_1, \dots, c_n)$ if for all $i = 1, 2, \dots, n$,

$$|f(x_1, x_2, \ldots, x_{i-1}, \mathbf{x}_i, x_{i+1}, \ldots, x_n) - f(x_1, x_2, \ldots, x_{i-1}, \widetilde{\mathbf{x}}_i, x_{i+1}, \ldots, x_n)| \leq c_i,$$

where x_i and \tilde{x}_i are in the domain of the *i*-th coordinate.

McDiarmid's inequality

Let $X_1, ..., X_n$ be independent random variables. Let f be Lipschitz with parameters $\mathbf{c} = (c_1, ..., c_n)$. Let $X = f(X_1, ..., X_n)$. Then for any t > 0,

$$\mathbf{P}[X \ge \mu + t] \le \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right),\,$$

and

$$\mathbf{P}[X \le \mu - t] \le \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right).$$

A function f is called Lipschitz with parameters $\mathbf{c} = (c_1, \dots, c_n)$ if for all $i = 1, 2, \dots, n$,

$$|f(x_1, x_2, \ldots, x_{i-1}, \mathbf{x}_i, x_{i+1}, \ldots, x_n) - f(x_1, x_2, \ldots, x_{i-1}, \mathbf{x}_i, x_{i+1}, \ldots, x_n)| \leq c_i$$

where x_i and \tilde{x}_i are in the domain of the *i*-th coordinate.

McDiarmid's inequality

Let $X_1, ..., X_n$ be independent random variables. Let f be Lipschitz with parameters $\mathbf{c} = (c_1, ..., c_n)$. Let $X = f(X_1, ..., X_n)$. Then for any t > 0,

$$\mathbf{P}[X \ge \mu + t] \le \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right),\,$$

and

$$\mathbf{P}[X \leq \mu - t] \leq \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right).$$

• Notice the similarity with Hoeffding's inequality! [Exercise 2/3.14]

A function f is called Lipschitz with parameters $\mathbf{c} = (c_1, \dots, c_n)$ if for all $i = 1, 2, \dots, n$,

$$|f(x_1, x_2, \ldots, x_{i-1}, \mathbf{x}_i, x_{i+1}, \ldots, x_n) - f(x_1, x_2, \ldots, x_{i-1}, \widetilde{\mathbf{x}}_i, x_{i+1}, \ldots, x_n)| \leq c_i,$$

where x_i and \tilde{x}_i are in the domain of the *i*-th coordinate.

McDiarmid's inequality

Let X_1, \ldots, X_n be independent random variables. Let f be Lipschitz with parameters $\mathbf{c} = (c_1, \ldots, c_n)$. Let $X = f(X_1, \ldots, X_n)$. Then for any t > 0,

$$\mathbf{P}[X \ge \mu + t] \le \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right),\,$$

and

$$\mathbf{P}[X \le \mu - t] \le \exp\left(-\frac{2t^2}{\sum_{i=1}^n c_i^2}\right).$$

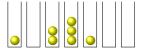
- Notice the similarity with Hoeffding's inequality! [Exercise 2/3.14]
- The proof is omitted here (it requires the concept of martingales).

Outline

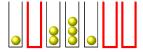
Application 2: Randomised QuickSort

Extensions of Chernoff Bounds

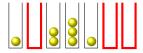
Applications of Method of Bounded Differences



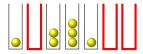
- Consider again m balls assigned uniformly at random into n bins.
- Enumerate the balls from 1 to m. Ball i is assigned to a random bin X_i



- Consider again m balls assigned uniformly at random into n bins.
- Enumerate the balls from 1 to m. Ball i is assigned to a random bin X_i
- Let Z be the number of empty bins (after assigning the m balls)
- $Z = Z(X_1, \dots, X_m)$ and Z is Lipschitz with $\mathbf{c} = (1, \dots, 1)$

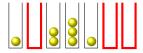


- Consider again *m* balls assigned uniformly at random into *n* bins.
- Enumerate the balls from 1 to m. Ball i is assigned to a random bin X_i
- Let Z be the number of empty bins (after assigning the m balls)
- $Z = Z(X_1, ..., X_m)$ and Z is Lipschitz with $\mathbf{c} = (1, ..., 1)$ (If we move one ball to another bin, number of empty bins changes by ≤ 1 .)



- Consider again *m* balls assigned uniformly at random into *n* bins.
- Enumerate the balls from 1 to m. Ball i is assigned to a random bin X_i
- Let Z be the number of empty bins (after assigning the m balls)
- $Z = Z(X_1, ..., X_m)$ and Z is Lipschitz with $\mathbf{c} = (1, ..., 1)$ (If we move one ball to another bin, number of empty bins changes by ≤ 1 .)
- By McDiarmid's inequality, for any $t \ge 0$,

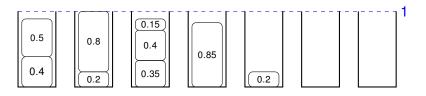
$$P[|Z - E[Z]| > t] \le 2 \cdot e^{-2t^2/m}$$



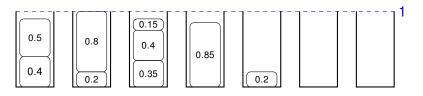
- Consider again m balls assigned uniformly at random into n bins.
- Enumerate the balls from 1 to m. Ball i is assigned to a random bin X_i
- Let Z be the number of empty bins (after assigning the m balls)
- $Z = Z(X_1, ..., X_m)$ and Z is Lipschitz with $\mathbf{c} = (1, ..., 1)$ (If we move one ball to another bin, number of empty bins changes by ≤ 1 .)
- By McDiarmid's inequality, for any $t \ge 0$,

$$P[|Z - E[Z]| > t] \le 2 \cdot e^{-2t^2/m}$$

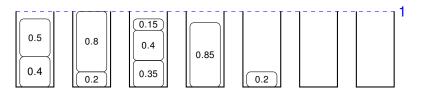
This is a decent bound, but for some values of m it is far from tight and stronger bounds are possible through a refined analysis.



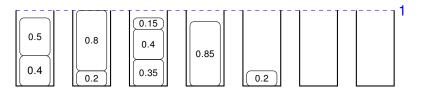
- We are given n items of sizes in the unit interval [0, 1]
- We want to pack those items into the fewest number of unit-capacity bins
- Suppose the item sizes X_i are independent random variables in [0, 1]



- We are given *n* items of sizes in the unit interval [0, 1]
- We want to pack those items into the fewest number of unit-capacity bins
- Suppose the item sizes X_i are independent random variables in [0, 1]
- Let $B = B(X_1, ..., X_n)$ be the optimal number of bins



- We are given *n* items of sizes in the unit interval [0, 1]
- We want to pack those items into the fewest number of unit-capacity bins
- Suppose the item sizes X_i are independent random variables in [0, 1]
- Let $B = B(X_1, ..., X_n)$ be the optimal number of bins
- The Lipschitz conditions holds with c = (1, ..., 1). Why?



- We are given *n* items of sizes in the unit interval [0, 1]
- We want to pack those items into the fewest number of unit-capacity bins
- Suppose the item sizes X_i are independent random variables in [0, 1]
- Let $B = B(X_1, ..., X_n)$ be the optimal number of bins
- The Lipschitz conditions holds with c = (1, ..., 1). Why?
- Therefore

$$P[|B - E[B]| \ge t] \le 2 \cdot e^{-2t^2/n}$$
.

This is a typical example where proving concentration is much easier than calculating (or estimating) the expectation!