Chapter 10

Randomized Algorithms II – High Probability

CS 573: Algorithms, Fall 2013
September 26, 2013

10.1 Movie...

10.2 Understanding the binomial distribution

10.2.0.1 Binomial distribution

X_n = numbers of heads when flipping a coin n times.

Claim

$\mathbf{Pr}\Big[X_n = i\Big] = \frac{\binom{n}{i}}{2^n}$.

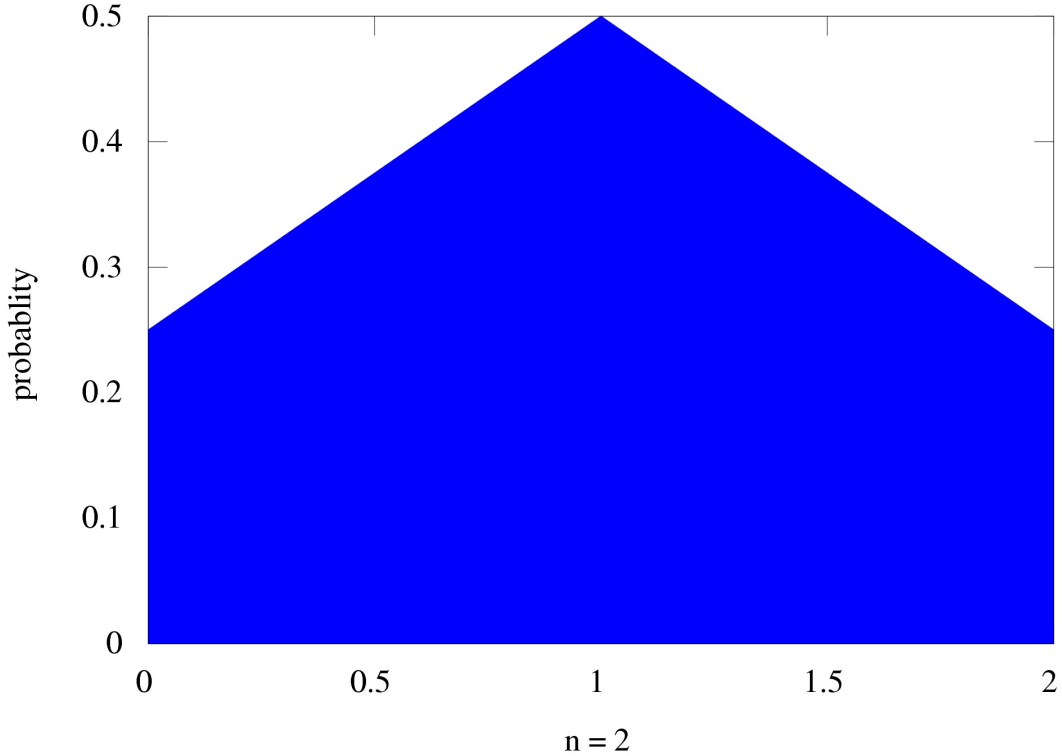
Where: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

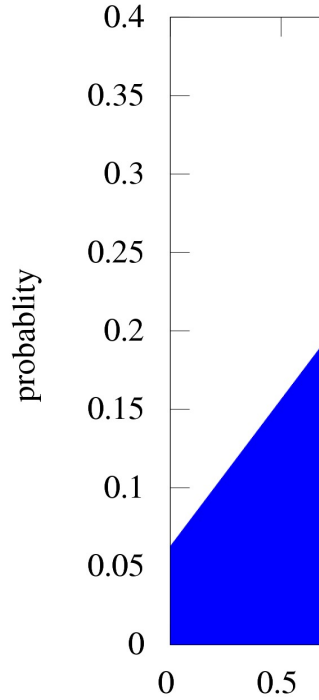
Indeed, $\binom{n}{i}$ is the number of ways to choose i elements out of n elements (i.e., pick which i coin flip come up heads).

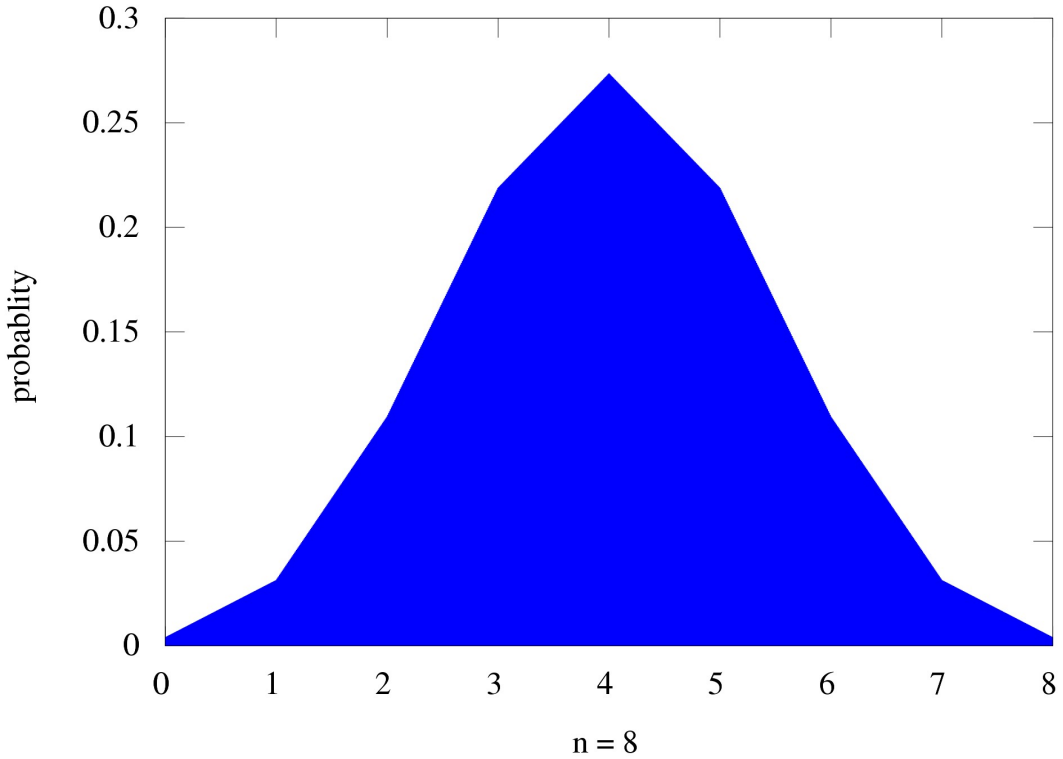
Each specific such possibility (say 0100010...) had probability $1/2^n$.

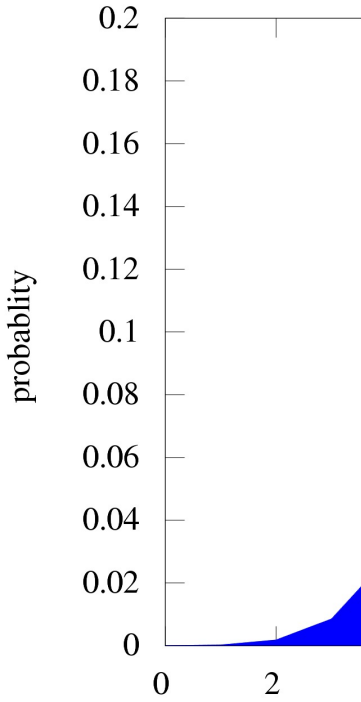
10.2.0.2 Massive randomness.. Is not that random.

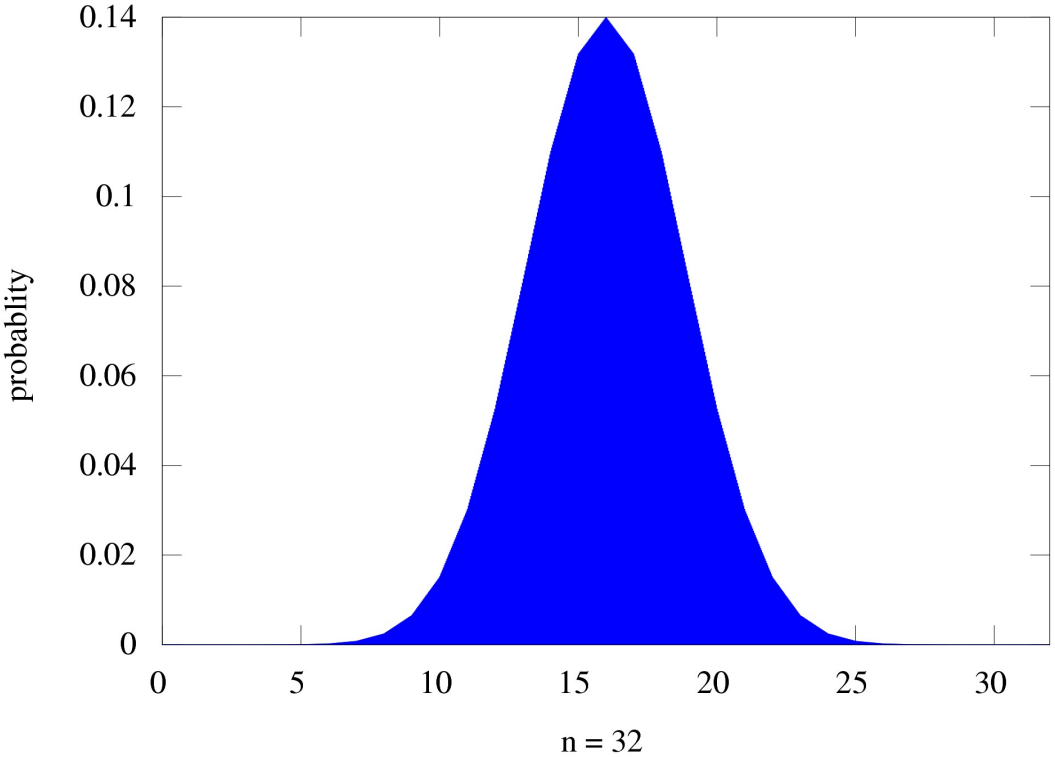
Consider flipping a fair coin n times independently, head given 1, tail gives zero. How many heads? ...we get a binomial distribution.

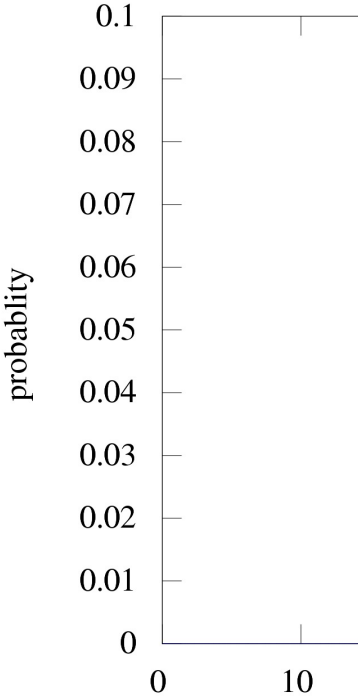

probablity
0.5
0.4
0.3
0.2
0.1
0
0
0.5
1
1.5
2
n = 2

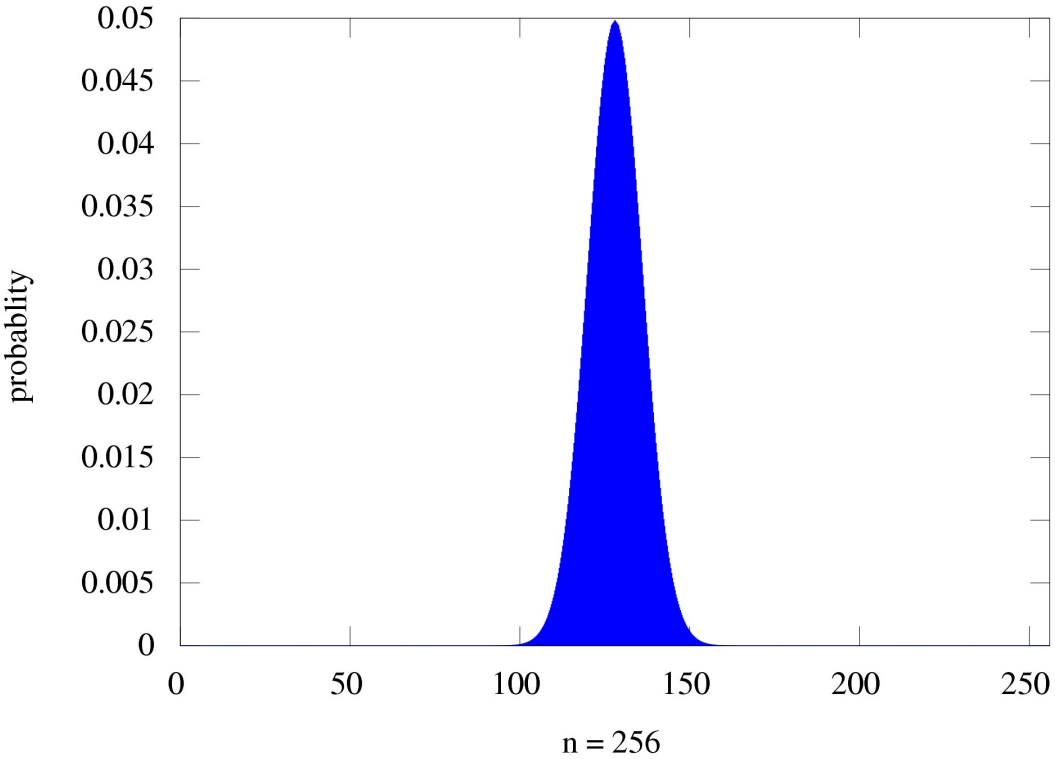

probablity
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
0.5

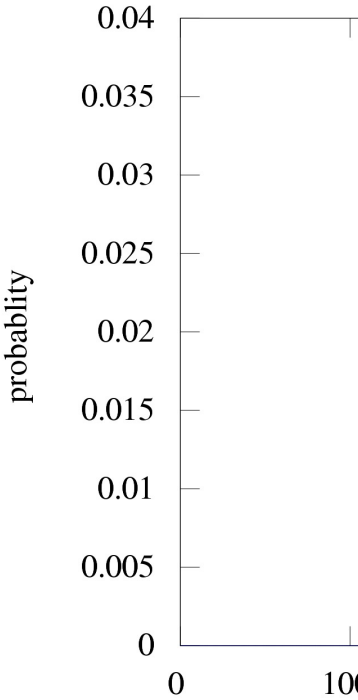

probablity
0.3
0.25
0.2
0.15
0.1
0.05
0
0
1
2
3
4
5
6
7
8
n = 8

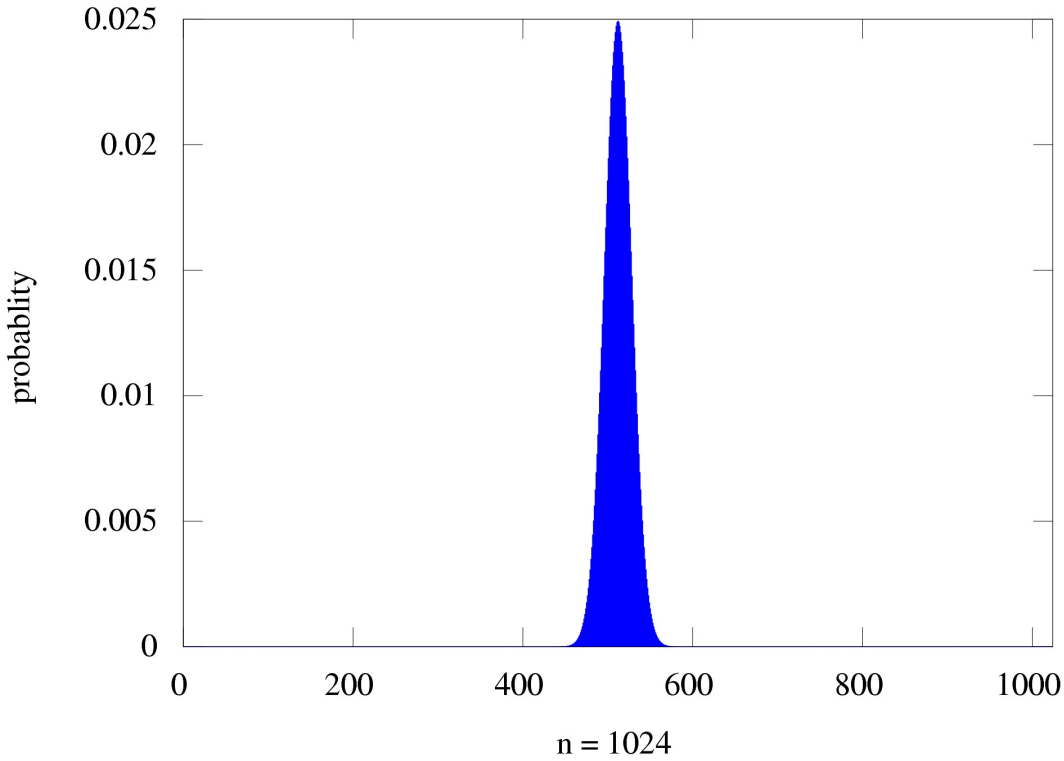

probablity
0.2
0.18
0.16
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
0
2

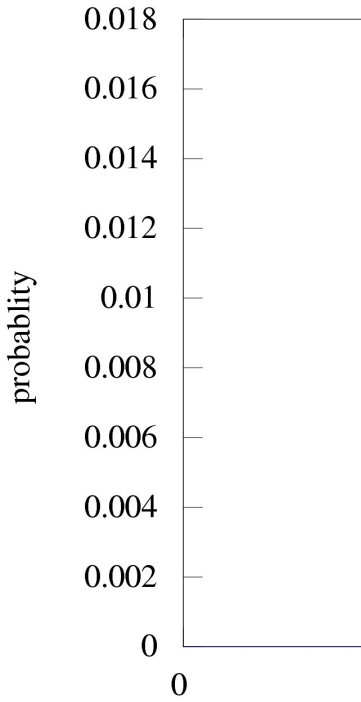

probablity
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
0
5
10
15
20
25
30
n = 32

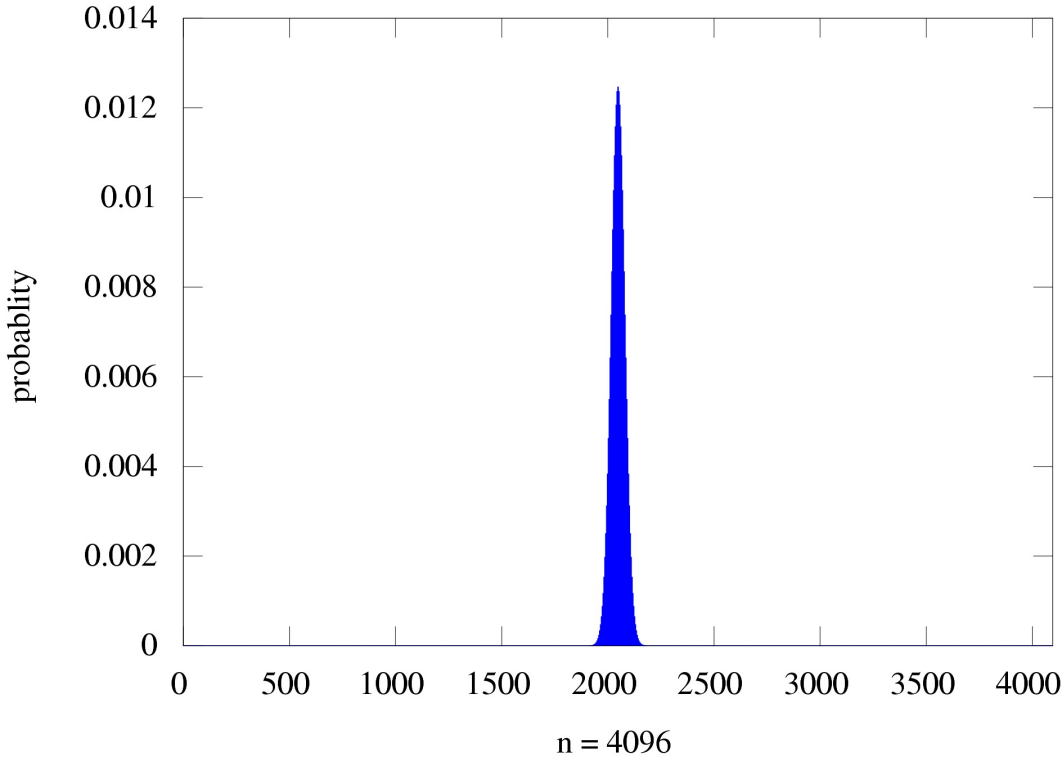

probablity
0.1
0.09
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0
0
10

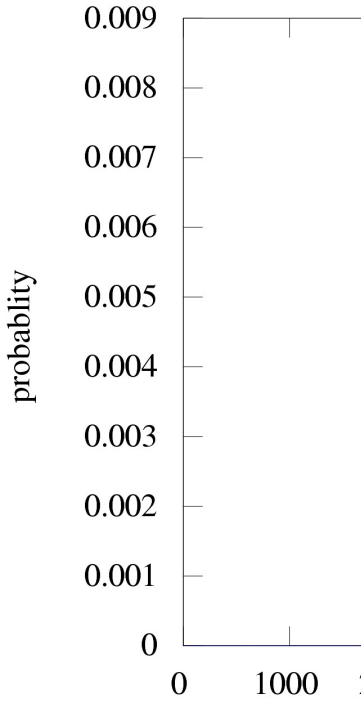

probablity
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
0
50
100
150
200
250
n = 256


probablity
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
0

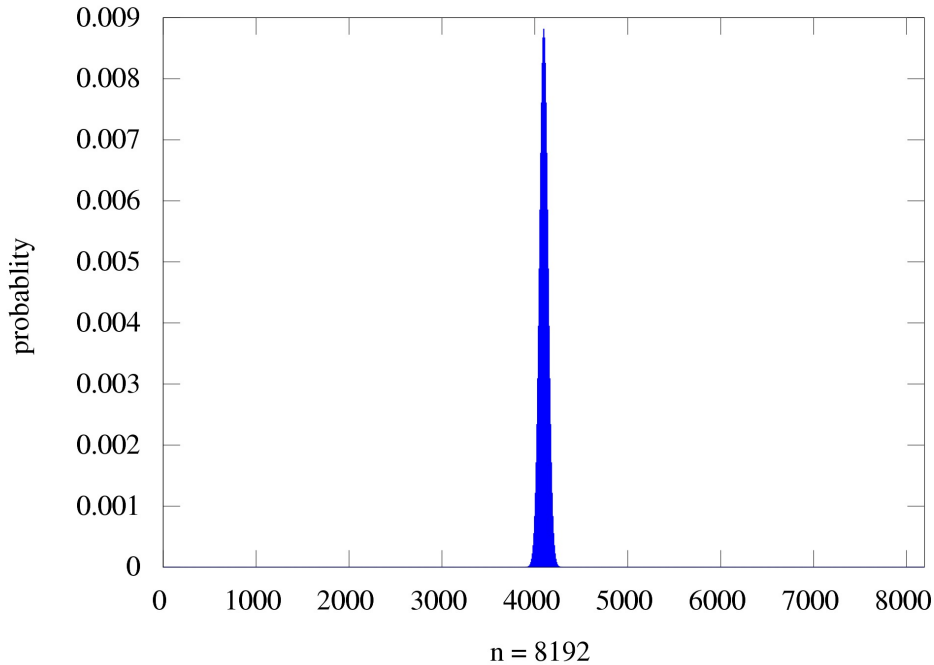

0.025
0.02
0.015
0.01
0.005
0
probablity
0
200
400
600
800
1000
n = 1024


0.018
0.016
0.014
0.012
0.01
0.008
0.006
0.004
0.002
0
probablity
0


0.014
0.012
0.01
0.008
0.006
0.004
0.002
0
probablity
0
500
1000
1500
2000
2500
3000
3500
4000
n = 4096


0.009
0.008
0.007
0.006
0.005
0.004
0.003
0.002
0.001
0
probablity
0
1000

10.2.0.3 Massive randomness.. Is not that random.



This is known as ***concentration of mass***.

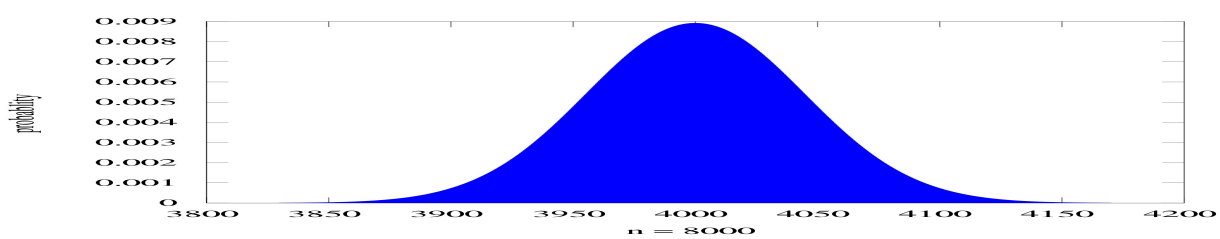
This is a very special case of the ***law of large numbers***.

10.2.1 Side note...

10.2.1.1 Law of large numbers (weakest form)...

Informal statement of law of large numbers

For n large enough, the middle portion of the binomial distribution looks like (converges to) the normal/Gaussian distribution.



10.2.1.2 Massive randomness.. Is not that random.

Intuitive conclusion

Randomized algorithm are unpredictable in the tactical level, but very predictable in the strategic level.

10.3 QuickSort with high probability

10.4 AlgorithmQuickSort and Treaps with High Probability

10.4.0.3 Show that QuickSort running time is $O(n \log n)$

(A) **QuickSort** picks a pivot, splits into two subproblems, and continues recursively.
(B) Track single element in input.
(C) Game ends, when this element is alone in subproblem.
(D) Show every element in input, participates $\leq 32 \ln n$ rounds (with high enough probability).
(E) $\mathcal{E}_i$: event ith element participates $> 32 \ln n$ rounds.
(F) C_{QS}: number of comparisons performed by **QuickSort**.
(G) Running time $O(C_{QS})$.
(H) Probability of failure is $\alpha = \mathbf{Pr}\Big[C_{QS} \geq 32n \ln n\Big] \leq \mathbf{Pr}[\bigcup_i \mathcal{E}_i] \leq \sum_{i=1}^{n} \mathbf{Pr}\Big[\mathcal{E}_i\Big]$.
... by the union bound.

10.4.0.4 Show that QuickSort running time is $O(n \log n)$

(A) Probability of failure is $\alpha = \mathbf{Pr}\Big[C_{QS} \geq 32n \ln n\Big] \leq \mathbf{Pr}[\bigcup_i \mathcal{E}_i] \leq \sum_{i=1}^{n} \mathbf{Pr}\Big[\mathcal{E}_i\Big]$.
(B) ***Union bound***: for any two events A and B: $\mathbf{Pr}[A \cup B] \leq \mathbf{Pr}[A] + \mathbf{Pr}[B]$.
(C) Assume: $\mathbf{Pr}[\mathcal{E}_i] \leq 1/n^3$.
(D) Bad probability... $\alpha \leq \sum_{i=1}^{n} \mathbf{Pr}\Big[\mathcal{E}_i\Big] \leq \sum_{i=1}^{n} \frac{1}{n^3} = \frac{1}{n^2}$.
(E) $\implies$ **QuickSort** performs $\leq 32n \ln n$ comparisons, w.h.p.
(F) $\implies$ **QuickSort** runs in $O(n \log n)$ time, with high probability.

10.4.1 Proving that an element participates in small number of rounds

10.4.2 Proving that an element...

10.4.2.1 ... participates in small number of rounds.

(A) n: number of elements in input for **QuickSort**.
(B) x: Arbitrary element x in input.
(C) S_1: Input.
(D) S_i: input to ith level recursive call that include x.
(E) x ***lucky*** in jth iteration, if balanced split...
$|S_{j+1}| \leq (3/4)\,|S_j|$ and $|S_j \setminus S_{j+1}| \leq (3/4)\,|S_j|$
(F) $Y_j = 1 \iff x$ lucky in jth iteration.
(G) $\mathbf{Pr}\Big[Y_j\Big] = \frac{1}{2}$.
(H) **Observation**: $Y_1, Y_2, \ldots, Y_m$ are independent variables.
(I) x can participate $\leq \rho = \log_{4/3} n \leq 3.5 \ln n$ rounds.
(J) ...since $|S_j| \leq n(3/4)^{\#\text{ of lucky iteration in}1\ldots j}$.
(K) If ρ lucky rounds in first k rounds $\implies |S_k| \leq (3/4)^{\rho} n \leq 1$.

10.4.3 Proving that an element...

10.4.3.1 ... participates in small number of rounds.

(A) Brain reset!

(B) Q: How many rounds x participates in = how many coin flips till one gets ρ heads?
(C) A: In expectation, 2ρ times.

10.4.4 Proving that an element...

10.4.4.1 ... participates in small number of rounds.

(A) Assume the following:

Lemma 10.4.1. *In M coin flips:* $\mathbf{Pr}[\#\ \textit{heads} \leq M/4] \leq \exp(-M/8)$.

(B) Set $M = 32 \ln n \geq 8\rho$.
(C) $\mathbf{Pr}[Y_j = 0] = \mathbf{Pr}[Y_j = 1] = 1/2$.
(D) $Y_1, Y_2, \ldots, Y_M$ are independent.
(E) $\implies$ probability $\leq \rho \leq M/4$ ones in $Y_1, \ldots, Y_M$ is

$$\leq \exp\left(-\frac{M}{8}\right) \leq \exp(-\rho) \leq \frac{1}{n^3}.$$

(F) $\implies$ probability x participates in M recursive calls of **QuickSort** $\leq 1/n^3$.

10.4.5 Proving that an element...

10.4.5.1 ... participates in small number of rounds.

(A) n input elements. Probability depth of recursion in **QuickSort** $> 32 \ln n$ is $\leq (1/n^3) * n = 1/n^2$.
(B) Result:

Theorem 10.4.2. *With high probability (i.e., $1 - 1/n^2$) the depth of the recursion of* **QuickSort** *is $\leq 32 \ln n$. Thus, with high probability, the running time of* **QuickSort** *is $O(n \log n)$.*

(C) Same result holds for **MatchNutsAndBolts**.

10.4.5.2 Alternative proof of high probability of QuickSort

(A) T: n items to be sorted.
(B) $t \in T$: element.
(C) X_i: the size of subproblem in ith level of recursion containing t.
(D) $X_0 = n$, and $\mathbf{E}\left[X_i \,\middle|\, X_{i-1}\right] \leq \frac{1}{2}\frac{3}{4} X_{i-1} + \frac{1}{2} X_{i-1} \leq \frac{7}{8} X_{i-1}$.
(E) $\forall$ random variables $\mathbf{E}\left[X\right] = \mathbf{E}_y\left[\mathbf{E}\left[X \,\middle|\, Y = y\right]\right]$.
(F) $\mathbf{E}\left[X_i\right] = \mathbf{E}_y\left[\mathbf{E}\left[X_i \,\middle|\, X_{i-1} = y\right]\right] \leq \mathbf{E}_{X_{i-1}=y}\left[\frac{7}{8} y\right] = \frac{7}{8}\,\mathbf{E}\left[X_{i-1}\right] \leq \left(\frac{7}{8}\right)^i \mathbf{E}[X_0] = \left(\frac{7}{8}\right)^i n$.

10.4.5.3 Alternative proof of high probability of QuickSort

(A) $M = 8 \log_{8/7} n$: $\mu = \mathbf{E}\left[X_M\right] \leq \left(\frac{7}{8}\right)^M n \leq \frac{1}{n^8} n = \frac{1}{n^7}$.
(B) **Markov's Inequality**: For a non-negative variable X, and $t > 0$, we have:

$$\mathbf{Pr}\left[X \geq t\right] \quad \leq \quad \frac{\mathbf{E}[X]}{t}.$$

(C) By Markov's inequality:

$$\mathbf{Pr}\left[\begin{array}{c} t \text{ participates} \\ > M \text{ recursive calls} \end{array}\right] \leq \mathbf{Pr}\Big[X_M \geq 1\Big] \leq \frac{\mathbf{E}[X_M]}{1} \leq \frac{1}{n^7}.$$

(D) Probability any element of input participates $> M$ recursive calls $\leq n(1/n^7) \leq 1/n^6$.

10.5 Chernoff inequality

10.5.0.4 Preliminaries

(A) X, Y: Random variables are *independent* if $\forall x, y$:

$$\mathbf{Pr}\Big[(X = x) \cap (Y = y)\Big] = \mathbf{Pr}\Big[X = x\Big] \cdot \mathbf{Pr}\Big[Y = y\Big].$$

(B) The following is easy to prove:

Claim 10.5.1. *If X and Y are independent*
$\implies \mathbf{E}[XY] = \mathbf{E}[X]\,\mathbf{E}[Y]$.
$\implies Z = e^X$ *and* $W = e^Y$ *are independent.*

10.5.0.5 Chernoff inequality

Theorem 10.5.2 (Chernoff inequality). *$X_1, \ldots, X_n$: n independent random variables, such that $\mathbf{Pr}[X_i = 1] = \mathbf{Pr}[X_i = -1] = \frac{1}{2}$, for $i = 1, \ldots, n$. Let $Y = \sum_{i=1}^n X_i$. Then, for any $\Delta > 0$, we have*

$$\mathbf{Pr}\Big[Y \geq \Delta\Big] \leq \exp\Big(-\Delta^2/2n\Big).$$

10.5.0.6 Proof of Chernoff inequality

Fix arbitrary $t > 0$:

$$\begin{aligned}\mathbf{Pr}\Big[Y \geq \Delta\Big] &= \mathbf{Pr}\Big[tY \geq t\Delta\Big] = \mathbf{Pr}\Big[\exp(tY) \geq \exp(t\Delta)\Big] \\ &\leq \frac{\mathbf{E}\Big[\exp(tY)\Big]}{\exp(t\Delta)},\end{aligned}$$

10.5.1 Proof of Chernoff inequality

10.5.1.1 Continued...

$$\begin{aligned}\mathbf{E}\Big[\exp(tX_i)\Big] &= \frac{1}{2}e^t + \frac{1}{2}e^{-t} = \frac{e^t + e^{-t}}{2} \\ &= \frac{1}{2}\left(1 + \frac{t}{1!} + \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots\right) \\ &\quad + \frac{1}{2}\left(1 - \frac{t}{1!} + \frac{t^2}{2!} - \frac{t^3}{3!} + \cdots\right) \\ &= 1 + \frac{t^2}{2!} + + \cdots + \frac{t^{2k}}{(2k)!} + \cdots.\end{aligned}$$

However: $(2k)! = k!(k+1)(k+2)\cdots 2k \geq k!2^k$.

$$\mathbf{E}\Big[\exp(tX_i)\Big] = \sum_{i=0}^{\infty} \frac{t^{2i}}{(2i)!} \leq \sum_{i=0}^{\infty} \frac{t^{2i}}{2^i(i!)} =\leq \sum_{i=0}^{\infty} \frac{1}{i!}\left(\frac{t^2}{2}\right)^i =\leq \exp\left(\frac{t^2}{2}\right).$$

$$\mathbf{E}\Big[\exp(tY)\Big] = \mathbf{E}\left[\exp\left(\sum_i tX_i\right)\right] = \mathbf{E}\left[\prod_i \exp(tX_i)\right] = \prod_{i=1}^{n} \mathbf{E}\Big[\exp(tX_i)\Big] \leq \prod_{i=1}^{n} \exp\left(\frac{t^2}{2}\right) =\leq \exp\left(\frac{nt^2}{2}\right).$$

$$\mathbf{Pr}\Big[Y \geq \Delta\Big] \leq \frac{\mathbf{E}\Big[\exp(tY)\Big]}{\exp(t\Delta)} \leq \frac{\exp\left(\frac{nt^2}{2}\right)}{\exp(t\Delta)} = \exp\left(\frac{nt^2}{2} - t\Delta\right).$$

Set $t = \Delta/n$:

$$\mathbf{Pr}\Big[Y \geq \Delta\Big] \leq \exp\left(\frac{n}{2}\left(\frac{\Delta}{n}\right)^2 - \frac{\Delta}{n}\Delta\right) = \exp\left(-\frac{\Delta^2}{2n}\right).$$

■

10.5.2 Chernoff inequality...

10.5.2.1 ...what it really says

By theorem:

$$\mathbf{Pr}\Big[Y \geq \Delta\Big] = \sum_{i=\Delta}^{n} \mathbf{Pr}\Big[Y = i\Big] = \sum_{i=n/2+\Delta/2}^{n} \frac{\binom{n}{i}}{2^n} \leq \exp\left(-\frac{\Delta^2}{2n}\right),$$

10.5.3 Chernoff inequality...

10.5.3.1 symmetry

Corollary 10.5.3. *Let $X_1, \ldots, X_n$ be n independent random variables, such that $\mathbf{Pr}[X_i = 1] = \mathbf{Pr}[X_i = -1] = \frac{1}{2}$, for $i = 1, \ldots, n$. Let $Y = \sum_{i=1}^{n} X_i$. Then, for any $\Delta > 0$, we have*

$$\mathbf{Pr}\Big[|Y| \geq \Delta\Big] \leq 2\exp\left(-\frac{\Delta^2}{2n}\right).$$

10.5.3.2 Chernoff inequality for coin flips

$X_1, \ldots, X_n$ be n independent coin flips, such that $\mathbf{Pr}[X_i = 1] = \mathbf{Pr}[X_i = 0] = \frac{1}{2}$, for $i = 1, \ldots, n$. Let $Y = \sum_{i=1}^{n} X_i$. Then, for any $\Delta > 0$, we have

$$\mathbf{Pr}\left[\frac{n}{2} - Y \geq \Delta\right] \leq \exp\left(-\frac{2\Delta^2}{n}\right) \quad \text{and} \quad \mathbf{Pr}\left[Y - \frac{n}{2} \geq \Delta\right] \leq \exp\left(-\frac{2\Delta^2}{n}\right).$$

In particular, we have $\mathbf{Pr}\left[\left|Y - \frac{n}{2}\right| \geq \Delta\right] \leq 2\exp\left(-\frac{2\Delta^2}{n}\right)$.

10.5.3.3 The special case we needed

Lemma 10.5.4. *In a sequence of M coin flips, the probability that the number of ones is smaller than $L \leq M/4$ is at most* $\exp(-M/8)$.

Proof: Let $Y = \sum_{i=1}^{m} X_i$ the sum of the M coin flips. By the above corollary, we have:

$$\mathbf{Pr}\Big[Y \leq L\Big] = \mathbf{Pr}\Big[\frac{M}{2} - Y \geq \frac{M}{2} - L\Big] = \mathbf{Pr}\Big[\frac{M}{2} - Y \geq \Delta\Big],$$

where $\Delta = M/2 - L \geq M/4$. Using the above Chernoff inequality, we get $\mathbf{Pr}\Big[Y \leq L\Big] \leq \exp\Big(-\frac{2\Delta^2}{M}\Big) \leq \exp(-M/8)$. ■

10.6 The Chernoff Bound — General Case

10.6.1 The Chernoff Bound

10.6.1.1 The general problem

Problem 10.6.1. *Let $X_1, \ldots X_n$ be n independent Bernoulli trials, where*

$$\mathbf{Pr}\Big[X_i = 1\Big] = p_i \qquad \text{and} \qquad \mathbf{Pr}\Big[X_i = 0\Big] = 1 - p_i,$$

and let denote

$$Y = \sum_i X_i \qquad \mu = \mathbf{E}[Y].$$

Question: *what is the probability that $Y \geq (1+\delta)\mu$.*

10.6.2 The Chernoff Bound

10.6.2.1 The general case

Theorem 10.6.2 (Chernoff inequality). *For any $\delta > 0$,*

$$\mathbf{Pr}\Big[Y > (1+\delta)\mu\Big] < \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu}.$$

Or in a more simplified form, for any $\delta \leq 2e - 1$,

$$\mathbf{Pr}\Big[Y > (1+\delta)\mu\Big] < \exp\Big(-\mu\delta^2/4\Big),$$

and

$$\mathbf{Pr}\Big[Y > (1+\delta)\mu\Big] < 2^{-\mu(1+\delta)},$$

for $\delta \geq 2e - 1$.

10.6.2.2 Theorem

Theorem 10.6.3. *Under the same assumptions as the theorem above, we have*

$$\mathbf{Pr}\Big[Y < (1-\delta)\mu\Big] \leq \exp\left(-\mu\frac{\delta^2}{2}\right).$$

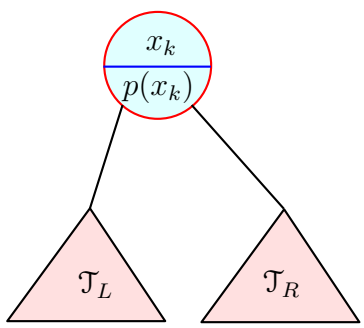
10.7 Treaps

10.8 Treaps

10.8.0.3 Balanced binary search trees...

(A) Work usually by storing additional information.
(B) Idea: For every element x inserted
randomly choose ***priority*** $p(x) \in [0,1]$.
(C) $X = \{x_1, \ldots, x_n\}$
priorities: $p(x_1), \ldots, p(x_n)$.
(D) x_k: lowest priority in X.
(E) Make x_k the root.
(F) partition X in the natural way:
  (A) L: set of all the numbers smaller than x_k in X, and
  (B) R: set of all the numbers larger than x_k in X.

10.8.0.4 Treaps



Continuing recursively, we have:
(A) L: set of all the numbers smaller than x_k in X, and
(B) R: set of all the numbers larger than x_k in X.

Definition 10.8.1. *Resulting tree a* **treap**.
Tree over the elements, and a heap over the priorities; that is,
TREAP = TREE + HEAP.

10.8.0.5 Treaps continued

Lemma 10.8.2. *S: n elements.*
Expected depth of treap T for S is $O(\log(n))$.
Depth of treap T for S is $O(\log(n))$ w.h.p.

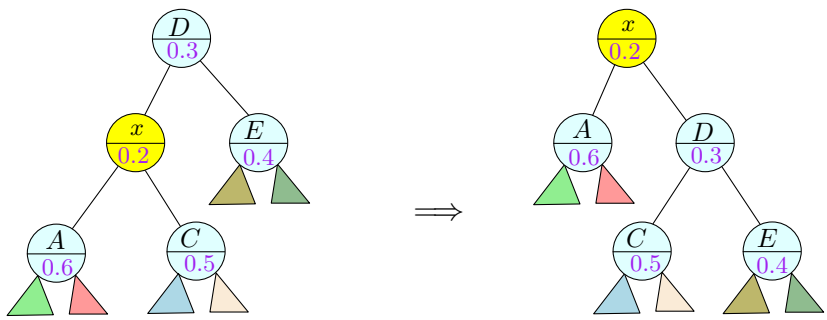
Proof: **QuickSort**... ■

10.8.1 Operations

10.8.1.1 Treaps - implementation

Observation 10.8.3. *Given n distinct elements, and their (distinct) priorities, the treap storing them is uniquely defined.*

10.8.1.2 Rotate right...



10.8.1.3 Insertion

10.8.1.4 Treaps – insertion

(A) x: an element x to insert.
(B) Insert it into T as a regular binary tree.
(C) Takes $O(\text{height}(\mathsf{T}))$.
(D) x is a leaf in the treap.
(E) Pick priority $p(x) \in [0, 1]$.
(F) Valid search tree,.. but priority heap is broken at x.
(G) Fix priority heap around x.

10.8.1.5 Fix treap for a leaf x...

```
RotateUp(x)
  y ← parent(x)
  while p(y) > p(x) do
      if y.left_child = x then
          RotateRight(y)
      else
          RotateLeft(y)
      y ← parent(x)
```

Insertion takes $O(\text{height}(\mathsf{T}))$.

10.8.1.6 Treaps – deletion

(A) Deletion is just an insertion done in reverse.
(B) x: element to delete.
(C) Set $p(x) \leftarrow +\infty$,
(D) rotate x down till its a leaf.
(E) Rotate so that child with lower priority becomes new parent.
(F) x is now leaf – deleting is easy...

10.8.1.7 Split

(A) x: element stored in treap T.
(B) split T into two treaps – one treap $\mathsf{T}_{\leq x}$ and treap $\mathsf{T}_{>}$ for all the elements larger than x.
(C) Set $p(x) \leftarrow -\infty$,

(D) fix priorities by rotation.
(E) x item is now the root.
(F) Splitting is now easy....
(G) Restore x to its original priority. Fix by rotations.

10.8.1.8 Meld

(A) T_L and T_R: treaps.
(B) all elements in T_L ¡ all elements in T_R.
(C) Want to merge them into a single treap...

10.8.1.9 Treap – summary

Theorem 10.8.4. *Let T be an empty treap, after a sequence of $m = n^c$ insertions, where c is some constant.*

d: arbitrary constant.

The probability depth T ever exceed $d \log n$ is $\leq 1/n^{O(1)}$.

A treap can handle insertion/deletion in $O(\log n)$ time with high probability.

10.8.1.10 Proof

Proof:
(A) $\mathsf{T}_1, \ldots, \mathsf{T}_m$: sequence of treaps.
(B) T_i is treap after ith operation.
(C) $\alpha_i = \mathbf{Pr}\Big[\mathrm{depth}(\mathsf{T}_i) > tc' \log n\Big] = \mathbf{Pr}\Big[\mathrm{depth}(\mathsf{T}_i) > c't\Big(\frac{\log n}{\log|\mathsf{T}_i|}\Big) \cdot \log|\mathsf{T}_i|\Big] \leq \frac{1}{n^{O(1)}}$,
(D) Use union bound...

■

10.8.1.11 Bibliographical Notes

(A) Chernoff inequality was a rediscovery of Bernstein inequality.
(B) ...published in 1924 by Sergei Bernstein.
(C) Treaps were invented by Siedel and Aragon Seidel and Aragon [1996].
(D) Experimental evidence suggests that Treaps performs reasonably well in practice see Cho and Sahni [2000].
(E) Old implementation of treaps I wrote in `C` is available here: `http://valis.cs.uiuc.edu/blog/?p=6060`.

Bibliography

S. Cho and S. Sahni. A new weight balanced binary search tree. *Int. J. Found. Comput. Sci.*, 11(3): 485–513, 2000.

R. Seidel and C. R. Aragon. Randomized search trees. *Algorithmica*, 16:464–497, 1996.