Theorem 1. *If X and Y are independent r.v.'s then:*

$$E[XY] = E[X]E[Y]$$

$$Var[X + Y] = Var[X] + Var[Y]$$

Example

What is the probability of getting more than $3N/4$ heads in N independent coin flips?

$X_i = 1$ if the ith flip was a head else $X_i = 0$.

$E[X_i] = 1/2$; $Var[X_i] = 1/4$

$\Pr(X \geq 3N/4) \leq \Pr(|X - E[X]| \geq N/4)$

$= \Pr(|X - E[X]| \geq E[X]/2) \leq 4/N$

Chernoff Bound

Theorem 2. *Let* $X_1, X_2, \ldots, X_n$ *be independent indicator random variables such that, for* $1 \leq i \leq n$, $\Pr[X_i = 1] = p_i$, *where* $0 < p_i < 1$. *Then, for* $X = \sum_{i=1}^{n} X_i$, $\mu = E[X] = \sum_{i=1}^{n} p_i$, *and any* $\delta > 0$,

$$\Pr\left(X > (1+\delta)\mu\right) < \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}$$

For $0 < \delta < 1$,

$$\Pr\left(X > (1+\delta)\mu\right) \leq e^{-\mu\delta^2/3}$$

For $0 < \delta < 1$,

$$\Pr(X < (1-\delta)\mu) < e^{-\mu\delta^2/2}$$

Proof. Upper tail: For any positive real t,

$$\Pr\left(X > (1+\delta)\mu\right) = \Pr(e^{tX} > e^{t(1+\delta)\mu})$$

By Markov's inequality,

$$\Pr\left(X > (1+\delta)\mu\right) < \frac{E[e^{tX}]}{e^{t(1+\delta)\mu}}$$

$$\begin{aligned}
&= \frac{E[e^{t\sum_{i=1}^{n} X_i}]}{e^{t(1+\delta)\mu}} = \frac{E[\Pi_{i=1}^{n} e^{tX_i}]}{e^{t(1+\delta)\mu}} = \frac{\Pi_{i=1}^{n} E[e^{tX_i}]}{e^{t(1+\delta)\mu}} \\
&= \frac{\Pi_{i=1}^{n}(p_i e^t + 1 - p_i)}{e^{t(1+\delta)\mu)}} = \frac{\Pi_{i=1}^{n}(1 + p_i(e^t - 1))}{e^{t(1+\delta)\mu}} \\
&< \frac{\Pi_{i=1}^{n} e^{p_i(e^t-1)}}{e^{t(1+\delta)\mu}} = \frac{e^{\sum_{i=1}^{n} p_i(e^t-1)}}{e^{t(1+\delta)\mu}} = \frac{e^{(e^t-1)\mu}}{e^{t(1+\delta)\mu}} \\
&\leq \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}
\end{aligned}$$

for $t = \ln(1+\delta)$

Using $\delta - (1+\delta)\ln(1+\delta) \leq -\delta^2/3$ for $0 < \delta < 1$ we get

$$\Pr\left(X > (1+\delta)\mu\right) \leq e^{-\mu\delta^2/3}$$

Lower tail:

$$\Pr\left(X < (1-\delta)\mu\right) = \Pr(e^{-tX} > e^{-t(1-\delta)\mu})$$

By Markov's inequality,

$$\Pr\left(X < (1-\delta)\mu\right) < \frac{E[e^{-tX}]}{e^{-t(1-\delta)\mu}}$$

Similar calculations yield

$$< \frac{e^{(e^{-t}-1)\mu}}{e^{-t(1-\delta)\mu}}$$

For $t = \ln(1/(1-\delta))$

$$\leq \left(\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}\right)^{\mu}$$

Since $(1-\delta)^{(1-\delta)} > e^{-\delta+\delta^2/2}$ we have

$$\Pr(X < (1-\delta)\mu) < e^{-\mu\delta^2/2}$$

□

Example

Theorem 3. *Consider n coin flips, let X be the number of heads,*

$$\Pr(|X - \frac{n}{2}| > \frac{1}{2}\sqrt{6n \log n}) \leq \frac{2}{n}$$

Proof.

$$E[X] = n/2$$

We need

$$\frac{n}{2} - \frac{1}{2}\sqrt{6n \log n} \leq X \leq \frac{n}{2} + \frac{1}{2}\sqrt{6n \log n}$$

or

$$X = \frac{n}{2}(1 \pm \sqrt{\frac{6 \log n}{n}})$$

Fixing $\delta = \sqrt{\frac{6 \log n}{n}}$

$$\Pr(X < (1-\delta)n/2) \leq e^{-\frac{n}{2}\frac{\delta^2}{2}} \leq 1/n$$

$$\Pr(X > (1+\delta)n/2) \leq e^{-\frac{n}{2}\frac{\delta^2}{3}} \leq 1/n$$

□

Randomized Quicksort Revisited

View an execution of the randomized quicksort algorithm (for sorting a set of $n > 1$ distinct numbers) as the following binary tree of (sub-)problems. An internal node of this tree is a subproblem of sorting a set S (of size greater than 1) and its left child (if any) is the subproblem of sorting a set $S_1 \subset S$ consisting of elements smaller than the pivot and its right child (if any) is the subproblem of sorting a set $S_2 \subset S$ consisting of elements larger than the pivot (the pivot is chosen uniformly at random in S). The root of this tree is the (initial) problem of sorting a given set of n distinct numbers; and a leaf is a subproblem of sorting a singleton set. Thus, a run of a quicksort algorithm is described by the above *execution tree*.

Theorem 4. *Randomized Quicksort runs in* $O(n \log n)$ *time with high probability , i.e., with probability at least* $1 - 1/n^b$*, for some constant* $b > 1$*.*

Proof. Suppose the size of the set to be sorted at a particular node is S. A node in the execution tree is labeled **good** if the pivot element divides the set into two parts, each of size not exceeding $2S/3$. Otherwise the node is called **bad**.

Then we can show that:

1. The probability of a node being labeled good is $1/3$.

2. The number of good nodes in any root to leaf path is bounded by $\log_{3/2} n < c \log n$ for some constant c.

What is the probability that a path of length $ac\log n$ (for some constant $a > 1$) will have at most $c\log n$ good nodes?

The mean $\mu = 1/3(ac\log n)$. Using the Chernoff bound

$$\Pr(X < c\log n) = \Pr(X < (1 - (1 - \frac{3}{a}))\mu)$$

$$\leq e^{-\mu(1-3/a)^2(1/2)} \leq 1/n^2$$

for a suitably large constant a.

Thus with probability at least $1 - 1/n^2$ the longest path (the above argument holds for any path, in particular the longest path) is at most $ac\log n$. Since the total work done at each level of the tree is $O(n)$, the running time is bounded by $O(n\log n)$ with high probability.

□

Computer Communication

* Parallel switches - communication network for parallel computers - tightly coupled machines (fast, reliable, almost synchronized).

* Communication networks for distributed systems - loosely coupled machines.

Local area networks - Ethernet, Token Ring

* Wide area networks - Internet.

Communication Layers

1. Physical Layer - wire, radio, optic ..

2. Data Link Layer - Moving data between two nodes: breaking message into frames, adding error correction, flow control.

3. Network/Transport Layer - Moving the data from source to destination: routing, addressing, ..

4. Application Layer - security, network management, applications (mail, web, etc.).