
$\qquad$
$\qquad$
$\qquad$
$\qquad$
$\qquad$
Randomization

- Randomized Algorithms: Uses values
generated by random number generator to
decide next step
- Often easier to implement and/or more
efficient
- Applications
- Used in protocol in "Ethernet Cards" to decide
when it next tries to access the shared medium
- Primality testing \& cryptography
- Monte Carlo simulations
1/12/10
cor 6936


## QuickSort vs Randomized QuickSort

QuickSort

- Pick a fixed pivot
- Partition input based on pivot into two sets
$\qquad$
- Recursively sort the two partitions

Randomized QuickSort

- Pick a random pivot
- Partition input based on pivot into two sets
- Recursively sort the two partitions

1/12/10
COT 6936

| QuickSort: Probabilistic Analysis |
| :--- |
| - Expected rank of pivot $=n / 2(W h y ?)$ |
| - Thus expected size of sublists after |
| partition $=n / 2$ |
| - Hence the recurrence $T(n)=2 T(n / 2)+O(n)$ |
| - Average time complexity $=T(n)=O(n \log n)$ |
|  |

$\qquad$
$\qquad$
$\qquad$
$\qquad$
$\qquad$
$\qquad$
$\qquad$

## New Quicksort: Randomized Analysis

- Let $X_{i j}$ be a random variable representing the number of times items $i$ and $j$ are compared by the algorithm.
- Expected time complexity = expected value of sum of all random variables $X_{i j}$.
- $\operatorname{Pr}\left(X_{i j}=1\right)=2 /(j-i+1) \quad$ (Why?)
$T(n)=$ ? $\qquad$
$\qquad$

1/12/10
COT 6936
5


$\qquad$

$\qquad$
$\qquad$
$\qquad$
$\qquad$
$\qquad$
$\qquad$

## Edge Contractions and Min-Cuts

$\qquad$

- Lemma: If you are not contracting an edge from the cut-set, edge contractions do no $\dagger$
$\qquad$ affect the size of min-cuts.
Observation: Most edges are not part of the min-cut.
- Idea: Use randomization
$\qquad$
$\qquad$
$\qquad$

| Randomized Algorithms: Min-Cut |
| :--- |
| - Assume that the Min-cut is of size k |
| - Pick a random edge |
| - Prob $\{$ edge is not in Min-cut $\} \geq 1-2 / n$ (why?) |
| - Prob $\{$ Min-cut is output $\} \geq 2 / n(n-1)$ (why?) |

$\qquad$

## Monte Carlo vs Las Vegas

$\qquad$
Monte Carlo algorithms: sometimes incorrect, but with bounded probability $\qquad$

- One-sided versus two-sided errors

Las Vegas algorithms: always correct, but with variable run times

## Chain Hashing

$\qquad$

- Balls and Bins Model
- Throw m balls into $n$ bins
$\qquad$
- Location of each ball chosen independently and uniformly at random
$\qquad$
Interesting questions to ask
- How many balls in a bin on the average?
$\qquad$
- How many bins are empty?
- How many balls in the fullest bin?
- If $m=n$, how many bins are expected to have > 1 ball in it?

COT 6936

## Power of Two Choices

## - Hashing with two hash functions

- Dramatically reduces the expected size of the $\qquad$ largest bin while doubling the average search cost.
- Dynamic Resource Allocation
- Multiple identical resources to choose from
- Find load of each one and pick least loaded
- Pick random resource
- Sample 2 random resources and pick less loaded one


## Bloom Filters

- Used to test set membership by using bit arrays to indicate which positions have been hashed to.

| 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |

- Use $k$ hash functions instead of 1.
- How large should $k$ be for given error bound?


## Breaking symmetry

$\qquad$
Many users want to share a resource

- Want to pick a permutation quickly
$\qquad$
- Hash to $2^{b}$ bits and sort them
- If $b=3 \log _{2} n$ then two users will have distinct hash values with probability $1-1 / n$

