



eCOMMONS

Loyola University Chicago
Loyola eCommons

Computer Science: Faculty Publications and
Other Works

Faculty Publications and Other Works by
Department

8-11-1996

Some Applications of Sophisticated Mathematics to Randomized Computing

Ronald I. Greenberg
Rgreen@luc.edu

Follow this and additional works at: https://ecommons.luc.edu/cs_facpubs

 Part of the [Computer Sciences Commons](#), [Other Mathematics Commons](#), and the [Probability Commons](#)

Recommended Citation

Greenberg, Ronald I.. Some Applications of Sophisticated Mathematics to Randomized Computing. Conference in Honor of the 90th Birthday of Professor Arnold Ross at Ohio State University, Columbus, OH, , , 1996. Retrieved from Loyola eCommons, Computer Science: Faculty Publications and Other Works,

This Presentation is brought to you for free and open access by the Faculty Publications and Other Works by Department at Loyola eCommons. It has been accepted for inclusion in Computer Science: Faculty Publications and Other Works by an authorized administrator of Loyola eCommons. For more information, please contact ecommons@luc.edu.



This work is licensed under a [Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 License](#).

Mathematics and Randomized Computing

Ronald Greenberg
U. of Maryland



Loyola U.
rig@math.luc.edu

Randomized Algorithms

Use random bits (typically pseudorandom no. generator in practice) to make decisions about what to do.

Two types of randomized alg.:

- Las Vegas
- Monte Carlo

Randomized Alg. Example

Primality Testing

Input: p

Output: "prime" or "composite"

Idea: Repeatedly pick random a such that $0 < a < p$, and compute $a^{p-1} \bmod p$. If result is ever $\neq 1$, then p is composite. If always 1, then p is probably prime.

Three Mathematical Results

- Chernoff bound on sums of random variables
- Lovász Local Lemma
- Weil's Theorem

Chernoff Bound

Very general.

Let S be the sum of k independent observations of a random variable X .

Let $m(a) = \inf_{t \in \mathbb{R}} E(e^{t(X-a)})$.

Then, for $a \geq E(X)$,

$$P(S_k \geq ka) \leq [m(a)]^k.$$

Special Case of Chernoff Bound

S_k is a binomial distribution
= sum of Bernoulli trials.

$$P(X=1) = q$$

$$P(X=0) = 1-q$$

$$E(e^{t(X-a)}) = (1-q)e^{-at} + qe^{t(1-a)}$$

Find inf by computing $\frac{d}{dt}$, etc.

After more work,

$$P(S_k \geq ka) \leq e^{-\left(\frac{a}{q} - 1\right)^2 kq/2}$$

for $a \geq q$.

An Application

A variation of Sample Sort parallel sorting alg. Begins w. each of p processors holding $\frac{n}{p}$ elements. Each proc. sends each elt. to a random one of the p procs. Expect i th proc. P_i to send $\approx \frac{n}{p^2}$ elts. to $P_j \forall i, j$.

What prob. of imbalance (degrading running time)? Prob. P_i sends $c \frac{n}{p^2}$ elts. to P_j is $\leq e^{-(c-1)^2 n / (2p^2)}$.

($k = n/p$, $q = 1/p$, $a = c/p$)

Very small for e.g. $c=2$ & n large.

Lovász Local Lemma

8

Let A_1, \dots, A_m be events each of which depends on $\leq b$ others,

If $P(A_i) \leq p \forall i$ and $4pb < 1$,
then $P(A_1 \cup A_2 \cup \dots \cup A_m) < 1$.

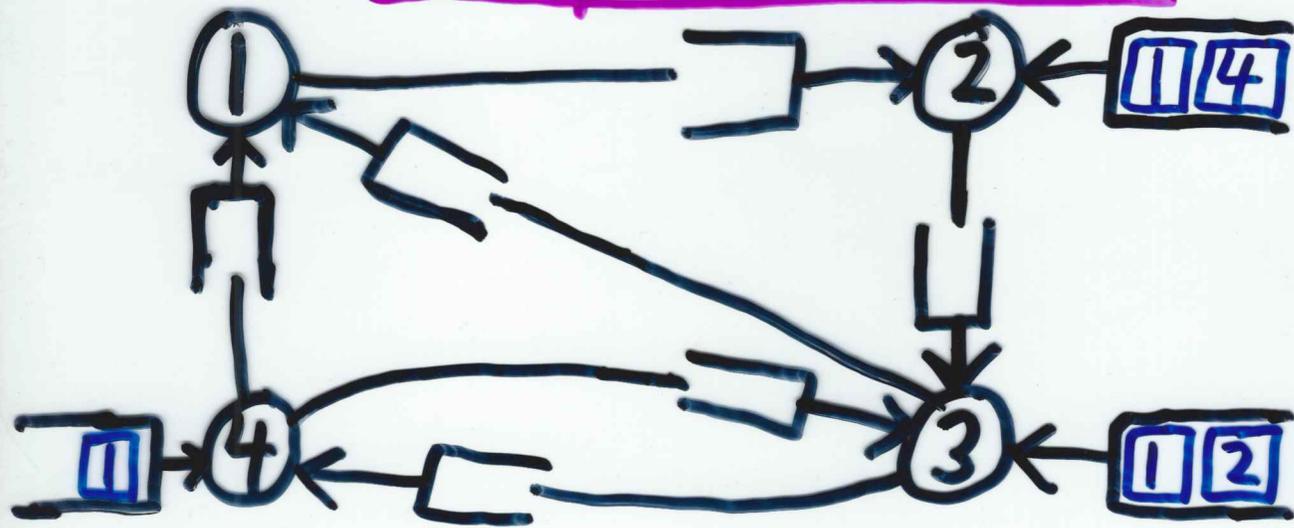
An Application

Used repeatedly to show that any set of packet paths in a network w. congestion c and dilation d can be realized in $O(c+d)$ time steps.

$c = \max.$ over edges of no. of packets that cross.

$d = \max.$ no. of edges traversed by a packet.

Graph Model



- Before routing, packets in initial queues at nodes (processors) where generated.
- Packet can traverse edge and enter queue at end when edge queue not full
- d_e time to traverse edge e

One step in the $O(c+d)$ Proof

WLOG, assume $c=d$.

Give each packet an initial delay from $[1, ac]$, and let packets go w/o further delay.

Claim: \exists a choice of delay such that $\leq lgc$ packets traverse any given edge during any given interval of lgc time steps.

Pf: Consider random delays.

Bad event for each edge: $> lgc$ packets during some interval of lgc time steps.

Pf. Cont.'d

$$p \leq (1+\alpha)c \binom{c}{lgc} \left(\frac{lgc}{\alpha c} \right)^{lgc}$$

$$b \leq cd = c^2$$

$4pb < 1$ for large enough const. α .

(Note: $\binom{n}{k} \leq \left(\frac{en}{k} \right)^k$.)

Weil Application

Variation of Lehmer's alg. for $\sqrt{} \pmod{p}$

Idea: Find x s.t. $\Delta = x^2 - a$ is a non-square mod p . Let $u = x + \sqrt{\Delta}$. In $\mathbb{Z}_p[\sqrt{\Delta}] = \mathbb{Z}_{p^2}$, compute and return $v = u^{(p+1)/2}$.

(\mathbb{Z}_{p^2} is the field of elts. of the form $x + y\sqrt{\Delta}$ w. $x, y \in \mathbb{Z}_p$ and Δ a nonsquare in \mathbb{Z}_p .)

Works because $v^2 = (u^{(p+1)/2})^2 = u^{p+1} \equiv u\bar{u} = x^2 - \Delta = a$.

Exer. (Note: $u^{(p+1)/2} \in \mathbb{Z}_p$. Exer.)

Choosing x

Make random picks. Prob. = $\frac{1}{2}$ that $x^2 - a$ is square (failure). With k indep. random picks, failure prob. = $\frac{1}{2^k}$.

But typical computation better modeled as random x_1 , then

$$x_2 = ax_1 + b \pmod{c}, x_3 = ax_2 + b \pmod{c}, \text{ etc.}$$

Actually can get good results w.

$x, x+1, x+2, \dots, x+k-1$. Fail only if

$\exists y_1, \dots, y_k$ such that

$$x^2 - a = y_1^2; (x+1)^2 - a = y_2^2; \dots;$$

$$(x+k-1)^2 - a = y_k^2.$$

Bounding Failure Prob.

Can show failure unlikely by bounding no. of solutions on curve.

Weil's Theorem: Let $\bar{\mathbb{F}}_p$ denote the algebraic closure of \mathbb{F}_p . Let C be a curve, def. by eqns. whose coefficients lie in \mathbb{F}_p , whose projective closure \bar{C} (over $\bar{\mathbb{F}}_p$) is nonsingular. Then N , the no. of pts. in \bar{C} w. coordinates in \mathbb{F}_p satisfies $|p+1-N| \leq 2g\sqrt{p}$, where g is the genus of C .