ERRATUM: OPTIMAL PARALLEL RANDOMIZED ALGORITHMS FOR THREE-DIMENSIONAL CONVEX HULLS AND RELATED PROBLEMS*

JOHN H. REIF† AND SANDEEP SEN‡

A portion of the appendix to "Optimal Parallel Randomized Algorithms for Three-Dimensional Convex Hulls and Related Problems," by John H. Reif and Sandeep Sen [SIAM J. Comput., 21 (1992), pp. 466–485] was inadvertently deleted when the article was printed. The appendix appears here in its entirety.

A. Appendix. We say a random variable X upper-bounds another random variable Y (equivalently Y lower bounds X) if for all x such that $0 \leq x \leq 1$, $\text{Prob}(X \leq x) \leq \text{Prob}(Y \leq x)$.

A Bernoulli trial is an experiment with two possible outcomes, success and failure. The probability of success is p.

A binomial variable X with parameters (n, p) is the number of successes in n independent Bernoulli trials, the probability of success in each trial being p. The *probability mass function* of X can be easily seen to be

$$\text{Prob}(X \leq x) = \sum_{k=0}^{x} \binom{n}{k} p^k (1-p)^{n-k}.$$

The tail end of the binomial distribution can be bounded by *Chernoff* bounds. In particular the following approximations due to Angluin and Valiant are frequently used:

$$\text{Prob}(X \geq m) \leq \left(\frac{np}{m}\right)^m e^{m-np} \tag{1}$$

$$\text{Prob}(X \leq m) \leq \left(\frac{np}{m}\right)^m e^{-np+m} \tag{2}$$

$$\text{Prob}(X \leq (1-\epsilon)pn) \leq \exp(-\epsilon^2 np/2) \tag{3}$$

$$\text{Prob}(X \geq (1+\epsilon)np) \leq \exp(-\epsilon^2 np/3) \tag{4}$$

for all $0 < \epsilon < 1$. The last two bounds actually follow from the Chernoff bounds, which (for a discrete distribution) can be stated as

$$\text{Prob}[A \geq x] \leq z^{-x} G_A(z)$$

where $G_A(z)$ is the probability generating function.

To minimize the bound we substitute $z = z_o$, which minimizes the right side expression.

Proof. (Lemma 10): Consider the generalized Chebychev's inequality

$$\text{Prob}\{|X| \geq t\} \leq \frac{E(\phi(X))}{\phi(t)}.$$

Using $\phi(t) = t^{2k}$ and substituting $X - E[X]$ for X and setting t to be equal to μ, we get

$$\text{Prob}\{|X - E[X]| \geq E[X]\} \leq \frac{E[(X - E[X])^{2k}]}{E^{2k}[X]}.$$

†Department of Computer Science, Duke University, Durham, North Carolina, 27706.

‡Department of Computer Science, Duke University, Durham, North Carolina, 27706. Present address, Department of Computer Science and Engineering, Indian University of Technology, New Delhi, 110016, India.

Preprint of paper appearing in SIAM Journal on Computing, 23(2): 447-448, April 1994.

Let us focus on the numerator. We shall show that it is $O(\mu^k)$ and the lemma follows. Since $E[X] = \sum_{i=1}^{n} E[X_i]$, we can write $(X - E[X])^{2k}$ as $(\sum_{i=1}^{n} X_i - E[X_i])^{2k}$. In the multinomial expansion, all the terms containing $X_i - E[X_i]$ (for any i) as a factor vanish because of the $2k$-way independence property.

There are $\binom{n}{c} \cdot \binom{2k-1}{c-1}$ terms that have c distinct non-unit product terms of the form $(X_j - E[X_j])^i$ such that $i > 0$ and $\sum i = 2k$. Also note that

$$\begin{aligned} E[(X_j - E[X_j])^i] &= (1-p)(-p)^i + p(1-p)^i \\ &\leq p^i + p \\ &= p(1 + p^{i-1}) \\ &\leq 2p. \end{aligned}$$

We can factor out p so that we can write the coefficient of n^c as $p^c \cdot f(k)$, where f is a function independent of n and can be absorbed in the big-O notation. From our observation about the first-order terms (which vanish), the maximum value of c is k. The numerator can be bound by the asymptotically dominating term $O(n^k \cdot p^k) = O(\mu^k)$. Since the denominator is μ^{2k}, the lemma follows. $\square$