Randomized Algorithms in "Primitive" Cultures or What is the Oracle Complexity of a Dead Chicken?

Jeffrey Shallit*
Department of Computer Science
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1
shallit@graceland.uwaterloo.ca

1 Introduction

Newton said, "If I have seen further it is by standing upon the shoulders of Giants."[1] But too often in the theoretical computer science community, we see ourselves as pioneers, covering untrod territory, without realizing that others may have gone before us.

It is my point in this note to kneel down for a moment in the wilderness of discovery, and note the outlines of ancient foundations buried under our frontier outpost. I will show that some of the concepts of randomized algorithms can quite legitimately be said to have their origins in the beliefs of two "primitive"[2] societies: namely, the Naskapi and the Azande.

Randomized algorithms are of great interest in theoretical computer science. Although some of the basic ideas can be traced back as far as Laplace's 1812 analysis of the Buffon needle problem [6] and Lord Kelvin's randomized simulation techniques [5], they did not gain wide acceptance until the papers of Solovay and Strassen [9], Rabin [8], and the thesis of Gill [4].

*A grant from NSERC had very little to do with the preparation of this paper.

[1]However, see Boller and George [2, pp. 100–101], where it is pointed out that the sentiment appeared previously in a 1624 book of Richard Burton. A more appropriate epigram for this paper might be the following excuse: "If I have failed to see very far, it is because Giants were standing on my shoulders!"

[2]"Primitive" is used here, of course, in the technical anthropological sense of the word, meaning a society that possesses neither insurance salesmen nor plastic slipcovers.

2 The Naskapi

The *Naskapi* people live in Labrador and northern Quebec; they speak Algonquian and are similar to the Montagnais people. They subsist on caribou, fish, and small game. According to the *Columbia Concise Encyclopedia*, there are about 7,000 Montagnais and Naskapi Indians alive today. Like the tribes of central Asia, they practice *scapulimancy:* the practice of roasting an animal's shoulder blade in order to obtain the answer to a question.

This practice is used most often to help find wild game. To quote Speck [10, p. 142],

> The use of the shoulder blades of game and fur-bearing animals is the outstanding phenomenon in divination here. In the rite of consultation this tablet-like bone is subjected to heat, and the burnings, in the form of blackened spots, cracks and breaks, are then interpreted by the cunning and ingeniousness of the practitioner. Imagination suggests the likeness of the marks produced by the heat, to rivers, lakes, mountains, trails, camps and various animals–the latter either single or in groups. The direction of the burnt marks and their respective locations are also significant.

An anthropologist with the unlikely name of Omar Khayyam Moore [7] observed in 1957,

> One class of questions for which shoulder-blade augury provides answers is: What direction should hunters take in locating game? This is a critical matter, for the failure of a hunt may bring privation or even death.

Moore suggests that the practice of scapulimancy is actually a form of randomization:

> If it may be assumed that there is some interplay between the animals [the Naskapi] seek and the hunts they undertake, such that the hunted and the hunters act and react to the other's actions and potential actions, then there may be a marked advantage in avoiding a fixed pattern in hunting. Unwitting regularities in behavior provide a basis for anticipatory response. For instance, animals that are "overhunted" are likely to become sensitized to human beings and hence quick to take evasive action. Because the occurrence of cracks and spots in the shoulder blade and the distribution of game are in all likelihood independent events, i.e., the former is unrelated to the outcome of past hunts, it would seem that a certain amount of irregularity would be introduced into the Naskapi hunting patterns by this mechanism ...
>
> It should be remembered that it is difficult for human beings to avoid patterning their behavior in a regular way. Without the aid of a table of random numbers or some other randomizing instrument, it is very unlikely that a human being or group would be able to make random choices even if an attempt were made to do so.

To summarize, Moore suggests that scapulimancy works because it suggests to the hunter a "random" place to hunt for game, one that might not necessarily have occurred to the hunter otherwise. Scapulimancy is a primitive form of randomized algorithm!

3 The Azande

The *Azande* (sing. *Zande*) are a tribe occupying parts of the Central African Republic and the Sudan. They consult a "poison oracle", or *benge*, in seeking advice on important matters.[3] The manner in which the oracle is consulted is described by Evans-Pritchard [3, p. 260]:

> The poison used is a red powder manufactured from a forest creeper and mixed with water to a paste. The liquid is squeezed out of the paste into the beaks of small domestic fowls which are compelled to swallow it. Generally violent spasms follow. The doses sometimes prove fatal, but as often the fowls recover. Sometimes they are even unaffected by the poison. From the behaviour of fowls under this ordeal, especially by their death or survival, Azande receive answers to the questions they place before the oracle.

The oracle is believed to speak through the poison, and when properly consulted is never wrong. However, since the question may not always have been framed properly, or too much or too little poison may have been administered, there is an element of randomness involved. To handle this problem, the Azande have devised the following clever method [3, pp. 299–302]:

> There are two tests, the *bambata sima*, or first test, and the *gingo*, or second test. If a fowl dies in the first test, then another fowl must survive the second test, and if a fowl survives the first test another fowl must die in the second test for the judgement to be accepted as valid. Generally the question is so framed that the oracle will have to kill a fowl in the first test and spare another fowl in the corroborative test to give a negative reply; but this is not invariably the case, and questions are sometimes framed in an opposite manner ...
>
> In the two tests one fowl must die and the other must live if the verdict is to be accepted as valid. If both live or both die the verdict is invalid and the oracle must be consulted on the matter a second time on another occasion ...
>
> Often Azande consider a single test sufficient, especially if the oracle gives its answer decisively by killing the fowl without hesitation. They are able to economize their oracle poison by this means ... Sometimes a single fowl is used to confirm different questions. If in answer to two different questions the oracle killed two fowls it may then be asked to spare a third fowl to confirm both its verdicts at the same time.

A footnote in [7] says

> Incidentally, their manner of framing questions–they use complex conditionals–so as to obtain as many definitive answers while sacrificing as few fowls as possible, would do credit to a logician.[4]

[3] Too bad the Azande did not know of the vastly superior modern technique of consulting one's horoscope, notably practiced by a recent US president.

[4] Moore does not elaborate, but one could imagine, for example, choosing among eight alternatives by feeding poison to three chickens, and employing binary search.

Thus we see that the Azande have anticipated at least two modern techniques associated with randomized algorithms: amplifying confidence in a result by repeating the algorithm on independent trials, and the re-use of random bits, treating randomness (or, more properly, chickens) as a scarce resource. (For this latter technique in a modern context, see, for example, Bach [1].)

At the risk of hearing the reader cry, "Fowl!", one might even say that the Azande anticipated the field of *oracle complexity*,[5] in which one studies resource-bounded computation with a restricted number of oracle queries–hence the question in the title of this paper.

References

[1] E. Bach. Realistic analysis of some randomized algorithms. *J. Comput. System Sci.*, 42:30–53, 1991.

[2] Paul F. Boller, Jr. and John George. *They Never Said It: A Book of Fake Quotes, Misquotes, and Misleading Attributions*. Oxford University Press, New York, 1989.

[3] E. E. Evans-Pritchard. *Witchcraft, Oracles, and Magic Among the Azande*. Oxford University Press, London, 1937.

[4] J. Gill. Computational complexity of probabilistic Turing machines. *SIAM J. Comput.*, 6:675–695, 1977.

[5] Lord Kelvin. Nineteenth century clouds over the dynamical theory of heat and light. *Philosophical Magazine*, 2:1–40, 1901.

[6] Pierre Simon Laplace. *Théorie Analytique des Probabilités*. Paris, 1812.

[7] Omar Khayyam Moore. Divination–a new perspective. *American Anthropologist*, 59:69–74, 1957.

[8] M. O. Rabin. Probabilistic algorithms. In J. F. Traub, editor, *Algorithms and Complexity: New Directions and Recent Results*, pages 21–39. Academic Press, New York, 1976.

[9] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Comput.*, 6:84–85, 1977. Also see erratum 7:118, 1978.

[10] Frank G. Speck. *Naskapi: The Savage Hunters of the Labrador Peninsula*. University of Oklahoma Press, Norman, 1977. New edition; originally published 1935.

[11] K. Wagner. Bounded query computations. In *Proc. 3rd Structure in Complexity Theory Annual Conference*, pages 260–277. IEEE Press, 1988.

[5] See the survey of Wagner [11]. I am grateful to Judy Goldsmith for supplying this reference.

Randomised algorithms oer simple and ecient solutions to a number of prob-lems, though it can be a complex task to prove that a specic randomised algo-rithm has a desired property. This note describes a simple technique for bounding the expected running time of randomised algorithms, namely analysis by indicator variables combined with linearity of expectation. The technique is applied to quicksort, to randomised dictionaries and to two selected geometric algorithms: construction of a binary planar autopartition and construction of a convex hull in the plane. All algorithms are simple, but wit...Â gorithm, but one of the rst modern examples of a randomised algorithm, the. Rabin-Miller. primality. Randomized algorithms and data structures are often analyzed under the assumption of access to a perfect source of randomness. The most fundamental metric used to measure how â€œrandomâ€ a hash function or a random number generator is, is its independence: a sequence of random variables is said to be k-independent if every variable is uniform and every size k subset is independent.Â This paper presents a method to analyze the powers of a given trilinear form (a special kind of algebraic constructions also called a tensor) and obtain upper bounds on the asymptotic complexity of matrix multiplication. Compared with existing approaches, this method is based on convex optimization, and thus has polynomial-time complexity. Another subclass of randomized algorithms is randomized rounding of linear programming relaxation. Many problems (Min cut, Set Cover, Vertex Cover, TSP) can be expressed as an Integer Programming problem. In order to get a solution, we formulate the relaxed Linear Programming problem, solve it and perform randomized rounding on the solution to obtain the final solution. 1.1k views Â· View 5 Upvoters. Jack Gindi, Math and CS undergrad, have TAed both subjects.Â If n is sufficiently large, this may not be feasible. With a randomized procedure, we can reduce the communication complexity to [math]O(\log n)[/math] â€" only introducing a small probability of failure. I write about it here: The file comparison problem. Counting distinct elements in a data stream.