

FingerPrinting and its Geometric Implications

Jeff M Phillips

11.24.2003

Abstract

The technique of FingerPrinting uses a randomly chosen map, $F(x)$ or often $F_p(x)$, on elements from a large, possibly infinite set S , to a smaller finite set of buckets B . Some important characteristic of the relationship between elements $x \in S$ must be preserved over the map $F(S)$. This characteristic should then be assured with high probability for $F(x) \in B$. By analyzing only the finite number of buckets, much faster run times can be achieved.

I will attempt to show two simple examples of the technique. The first [1] verifies matrix multiplication in $O(n^2)$ time, and is the earliest instance of this type of algorithm I have found. The second [2] securely verifies length n bit strings in $O(\log n)$ time. This citation is often referenced as the first formalized use of the technique, although it references a tech report by Rabin [4] which clearly predates it. A nice survey of fingerprinting applications is available in [3].

After a basic flavor of the approach is taken in from the examples, I will attempt to characterize the set of problems which can benefit from this technique. (I will attempt to wield my reluctant knowledge of Number Theory and Abstract Algebra.) Possibly we may realize more applications for this powerful randomized tool.

If time permits, I will describe a novel use of FingerPrinting, in a geometric setting. John Reif and I are investigating the class of geometric objects for which intersections can be detected in faster than an all-pairs, $O(n^2)$ check. I may give the algorithm and analysis for some of the most simple geometric applications and allude to some more interesting ones.

References

- [1] R. Freivalds. Probabilistic machines can use less running time. *Information Processing 77, Proceedings of IFIP Congress*, 77:839–842, 1977.
- [2] R. M. Karp and M. O. Rabin. Efficient randomized pattern-matching algorithms. *IBM Journal of Research and Development*, 31:249–260, March 1987.
- [3] R. Motwani and P. Raghavan. *Randomized Algorithms*, chapter 7, pages 161–188. Cambridge.
- [4] M. O. Rabin. Fingerprinting by random polynomials. Technical Report TR-15-81, Harvard University Center for Research in Computing Technology, 1981.