Derandomization via small sample spaces

Noga Alon[⋆]

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 69978, Israel. E-mail: noga@math.tau.ac.il.

Abstract

Many randomized algorithms run successfully even when the random choices they utilize are not fully independent. For the analysis some limited amount of independence, like *k-wise independence* for some fixed k, often suffices. In these cases, it is possible to replace the appropriate exponentially large sample spaces required to simulate all random choices of the algorithms by ones of polynomial size. This enables one to *derandomize* the algorithms, that is, convert them into deterministic ones, by searching the relatively small sample spaces deterministically. If a random variable attains a certain value with positive probability, then we can actually search and find a point in which it attains such a value.

The observation that $n-1$ *pairwise independent* nontrivial random variables can be defined over a sample space of size n has been mentioned already long ago, see [11], [23]. The pairwise independent case has been a crucial ingredient in the construction of efficient hashing schemes in [14], [17]. A more general construction, of small sample spaces supporting k-wise independent random variables, appeared in [19]. For the case of binary, uniform random variables this is treated under the name *orthogonal arrays* in the Coding Theory literature, see, e.g., [27]. Most constructions are based on some simple properties of polynomials over a finite field or on certain explicit error correcting codes.

Several researchers realized that constructions of this type are useful for derandomizing *parallel* algorithms, since one may simply check all points of the sample space in parallel. Papers pursuing this idea include [1], [22], [24], and papers dealing with the properties of the constructions in which the sample spaces are not necessarily uniform include [20], [21]. It can be shown that for fixed k, the minimum size of a sample space supporting n k-wise independent random variables is $\Omega(n^{\lfloor k/2 \rfloor})$. For the binary uniform case this is essentially the Rao bound [30] (see also [12], [16]), whereas for the general case it is shown in [1], where it is also observed this is tight for the binary uniform case. It follows that polynomial size sample spaces suffice only for handling k-wise independence for fixed k. There are, however, several ways to achieve a higher amount of independence. One method, developed in [9] and [26], (see also [25] for related ideas), starts with a construction of relatively small spaces which support k-wise

[⋆] Research supported in part by a USA Israeli BSF grant.

independent random variables for $k = (\log n)^{O(1)}$, and proceeds by searching in these spaces using the *conditional expectations* method of [32], [29]. Another method, suggested in [31], is based on constructing spaces in which only certain prescribed sets of random choices are independent. The third method, initiated in [28] and improved in [3] (see also [2], [8], [13], [15]) constructs sample spaces that support random variables any k of which are *nearly* independent.

The above techniques have been applied in numerous papers dealing with derandomization, and we make no attempt to list all of them here. Examples include parallelization of derandomized geometric algorithms in [10], [18], and various parallel graph algorithms [1], [9], [22], [24], [28]. It turned out that some variants of the techniques are also useful in derandomizing *sequential* algorithms [5], [7] and in designing space efficient on-line algorithms for estimating some statistical properties of a given input sequence [4].

In the talk I will survey the basic ideas in the constructions of small sample spaces and discuss some of the applications, focusing on various recent results that illustrate the somewhat surprising relevance of the techniques to the solutions of several algorithmic problems.

References

1. N. Alon, L. Babai and A. Itai. A fast and simple randomized parallel algorithm for the maximal independent set problem. *J. Alg.*, 7:567–583, 1986.
2. N. Alon, J. Bruck, J. Naor, M. Naor and R. Roth. Construction of asymptotically good, low-rate error-correcting codes through pseudo-random graphs. *IEEE Trans. Info. Theory*, 38:509–516, 1992.
3. N. Alon, O. Goldreich, J. Håstad and R. Peralta. Simple constructions of almost k–wise independent random variables. *Random Structures and Algorithms*, 3(3):289–303, 1992.
4. N. Alon, Y. Matias and M. Szegedy. The space complexity of approximating the frequency moments. In *Proc. of the 28th ACM Symp. on Theory of Computing*, 1996, in press.
5. N. Alon and M. Naor. Derandomization, witnesses for Boolean matrix multiplication and construction of perfect hash functions. To appear in *Algorithmica*.
6. N. Alon and J. H. Spencer. *The Probabilistic Method.* Wiley, 1992.
7. N. Alon, R. Yuster and U. Zwick. Color-coding. *J. ACM* 42:844–856, 1995.
8. Y. Azar, R. Motwani and J. Naor. Approximating arbitrary probability distributions using small sample spaces. Manuscript, 1990.
9. B. Berger and J. Rompel. Simulating $(\log^c n)$-wise independence in NC. *Journal of the ACM*, 38:1026–1046, 1991.
10. B. Berger, J. Rompel and P. W. Shor. Efficient NC algorithms for set cover with applications to learning and geometry. In *Proc. 30th IEEE Symposium on Foundations of Computer Science*, pages 54-59, 1989.
11. S. Bernstein. *Theory of Probability (3rd Edition).* GTTI, Moscow, 1945.
12. B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich and R. Smolensky. The Bit Extraction Problem or t-Resilient Functions. In 26^{th} *Annual Symposium on Foundations of Computer Science, Portland, Oregon*, pages 396–407, 1985.

13. S. Chari, P. Rohatgi and A. Srinivasan. Improved algorithms via approximations of probability distributions. In *Proc. 26th ACM Symposium on Theory of Computing*, pages 584–592, 1994.
14. L. Carter and M. Wegman. Universal classes of Hash functions. *J. Computer System Sciences*, 18:143-154, 1979.
15. G. Even, O. Goldreich, M. Luby, N. Nisan and B. Velićković. Approximations of general independent distributions. In *Proc. 24th ACM Symposium on Theory of Computing*, pages 10–16, 1992.
16. J. Friedman. On the bit extraction problem. In *Proc. 33rd IEEE Symposium on Foundations of Computer Science*, pages 314–319, 1992.
17. M. Fredman, J. Komlos and E. Szemerédi. Storing a sparse table with $O(1)$ worst-case access time. In *Proc. 23rd IEEE Symposium on Foundations of Computer Science*, pages 165–169, 1982.
18. M. T. Goodrich. Geometric partitioning made easier, even in parallel. In *Proc. 9th ACM Symp. Comput. Geom.*, pages 73–82, 1993.
19. A. Joffe. On a set of almost deterministic k-independent random variables. *Annals of Probability*, 2:161–162, 1974.
20. D. Koller and N. Megiddo. Constructing small sample spaces satisfying given constraints. In *Proc. of the* 25^{th} *Annual ACM Symposium on Theory of Computing*, pages 268–277, 1993.
21. H. Karloff and Y. Mansour. On construction of k-wise independent random variables. In *Proc. of the 26th Annual ACM Symposium on Theory of Computing*, pages 564–573, 1994.
22. R. Karp and A. Wigderson. A fast parallel algorithm for the maximum independent set problem. *J. ACM*, 32: 762–773, 1985.
23. H. O. Lancaster. Pairwise statistical independence. *Ann. Math. Stat.* 36: 1313-1317, 1965.
24. M. Luby. A simple parallel algorithm for the maximal independent set problem. *SIAM J. Comput.*, 15(4):1036–1053, 1986.
25. M. Luby. Removing randomness in parallel computation without a processor penalty. *J. Comput. Syst. Sci.*, 47(2):250–286, 1993.
26. R. Motwani, J. Naor and M. Naor. The probabilistic method yields deterministic parallel algorithms. *J. Comput. Syst. Sci.*, 49:478–516, 1994.
27. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North Holland, Amsterdam, 1977.
28. J. Naor and M. Naor. Small–bias probability spaces: efficient constructions and applications. *SIAM J. Comput.*, 22(4):838–856, 1993.
29. P. Raghavan. Probabilistic construction of deterministic algorithms: approximating packing integer programs. *J. Comput. Syst. Sci.*, 37:130–143, 1988.
30. C. R. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *J. Royal Stat. Soc.* 9: 128–139, 1947.
31. L. J. Schulman. Sample spaces uniform on neighborhoods. In *Proceedings of the* 24^{th} *Annual ACM Symposium on Theory of Computing*, pages 17–25, 1992.
32. J. Spencer. *Ten Lectures on the Probabilistic Method.* SIAM, 1987.