**Goldreich, Oded**

**A sample of samplers: a computational perspective on sampling.** (English) Zbl 1343.68297

Goldreich, Oded (ed.), Studies in complexity and cryptography. Miscellanea on the interplay between randomness and computation. In collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman. Berlin: Springer (ISBN 978-3-642-22669-4/pbk). Lecture Notes in Computer Science 6650, 302-332 (2011).

Summary: We consider the problem of estimating the average of a huge set of values. That is, given oracle access to an arbitrary function $f : \{0,1\}^n \to [0,1]$, we wish to estimate $2^{-n} \sum_{x \in \{0,1\}^n} f(x)$ upto an additive error of $\epsilon$. We are allowed to employ a randomized algorithm that may err with probability at most $\delta$.

We survey known algorithms for this problem and focus on the ideas underlying their construction. In particular, we present an algorithm that makes $O(\epsilon^{-2} \cdot \log(1/\delta))$ queries and uses $n + O(\log(1/\epsilon)) + O(\log(1/\delta))$ coin tosses, both complexities being very close to the corresponding lower bounds.

For the entire collection see [Zbl 1220.68005].

**MSC:**

68W20 Randomized algorithms
05C81 Random walks on graphs
68Q87 Probability in computer science (algorithm analysis, random structures, phase transitions, etc.)
94A20 Sampling theory in information and communication theory



**Keywords:**

sampling; randomness complexity; saving randomness; pairwise independent random variables; expander graphs; random walks on graphs; information-theoretic lower bounds

**Full Text:** DOI

**References:**

[1] Ajtai, M., Komlos, J., Szemerédi, E.: Deterministic Simulation in LogSpace. In: Proc. 19th STOC, pp. 132–140 (1987)· doi:10.1145/28395.28410

[2] Alon, N.: Eigenvalues, Geometric Expanders, Sorting in Rounds and Ramsey Theory. Combinatorica˜6, 231–243 (1986) · Zbl 0625.05026

[3] Alon, N., Bruck, J., Naor, J., Naor, M., Roth, R.: Construction of Asymptotically Good, Low-Rate Error-Correcting Codes through Pseudo-Random Graphs. IEEE Transactions on Information Theory˜38, 509–516 (1992) · Zbl 0744.94023 · doi:10.1109/18.119713

[4] Alon, N., Milman, V.D.: {\(\lambda\)} 1, Isoperimetric Inequalities for Graphs and Superconcentrators. J. Combinatorial Theory, Ser. B˜38, 73–88 (1985) · Zbl 0549.05051 · doi:10.1016/0095-8956(85)90092-9

[5] Alon, N., Spencer, J.H.: The Probabilistic Method. John Wiley & Sons, Inc., Chichester (1992) · Zbl 0767.05001

[6] Bar-Yossef, Z., Kumar, R., Sivakumar, D.: Sampling Algorithms: Lower Bounds and Applications. In: 33rd STOC, pp. 266–275 (2001) · Zbl 1323.68292

[7] Bellare, M., Goldreich, O., Goldwasser, S.: Randomness in Interactive Proofs. Computational Complexity˜4(4), 319–354 (1993); Extended abstract in 31st FOCS, pp. 318–326 (1990) · Zbl 0802.68053 · doi:10.1007/BF01275487

[8] Bellare, M., Goldreich, O., Goldwasser, S.: Addendum to [7]. (May 1997), http://theory.lcs.mit.edu/˜oded/papers.html · Zbl 0916.94005

[9] Bellare, M., Rompel, J.: Randomness-efficient oblivious sampling. In: 35th FOCS (1994)· doi:10.1109/SFCS.1994.365687

[10] Canetti, R., Even, G., Goldreich, O.: Lower Bounds for Sampling Algorithms for Estimating the Average. In: IPL, vol.˜53, pp. 17–25 (1995) · Zbl 0875.68529

[11] Carter, L., Wegman, M.: Universal Classes of Hash Functions. J. Computer and System Sciences˜18, 143–154 (1979) · Zbl 0412.68090 · doi:10.1016/0022-0000(79)90044-8

[12] Chor, B., Goldreich, O.: On the Power of Two–Point Based Sampling. Jour. of Complexity˜5, 96–106 (1989) · Zbl 0672.60105 · doi:10.1016/0885-064X(89)90015-0

[13] Cohen, A., Wigderson, A.: Dispensers, Deterministic Amplification, and Weak Random Sources. In: 30th FOCS, pp. 14–19

(1989)

[14] Gaber, O., Galil, Z.: Explicit Constructions of Linear Size Superconcentrators. JCSS˜22, 407–420 (1981) · Zbl 0487.05045

[15] Goldreich, O., Impagliazzo, R., Levin, L.A., Venkatesan, R., Zuckerman, D.: Security Preserving Amplification of Hardness. In: 31st FOCS, pp. 318–326 (1990)· doi:10.1109/FSCS.1990.89550

[16] Goldreich, O., Wigderson, A.: Tiny Families of Functions with Random Properties: A Quality–Size Trade–off for Hashing. Journal of Random structures and Algorithms˜11(4), 315–343 (1997) · Zbl 0891.60010 · doi:10.1002/(SICI)1098-2418(199712)11:4<315::AID-RSA3>3.0.CO;2-1

[17] Golomb, S.W.: Shift Register Sequences. Aegean Park Press, (1982) (revised edition) · Zbl 1152.94383

[18] Guruswami, V., Umans, C., Vadhan, S.: Unbalanced Expanders and Randomness Extractors from Parvaresh-Vardy Codes. JACM˜56(4) (2009); Preliminary version in 22nd CCC 2007 · Zbl 1325.68169

[19] Hoory, S., Linial, N., Wigderson, A.: Expander Graphs and their Applications. Bull. AMS˜43(4), 439–561 (2006) · Zbl 1147.68608 · doi:10.1090/S0273-0979-06-01126-8

[20] Impagliazzo, R., Zuckerman, D.: How to Recycle Random Bits. In: 30th FOCS, pp. 248–253 (1989)· doi:10.1109/SFCS.1989.63486

[21] Kahale, N.: Eigenvalues and Expansion of Regular Graphs. Journal of the ACM˜42(5), 1091–1106 (1995) · Zbl 0885.68117 · doi:10.1145/210118.210136

[22] Karp, R.M., Pippinger, N., Sipser, M.: A Time-Randomness Tradeoff. In: AMS Conference on Probabilistic Computational Complexity, Durham, New Hampshire (1985)

[23] Lubotzky, A., Phillips, R., Sarnak, P.: Explicit Expanders and the Ramanujan Conjectures. In: Proc. 18th STOC, pp. 240–246 (1986)· doi:10.1145/12130.12154

[24] Margulis, G.A.: Explicit Construction of Concentrators. Prob. Per. Infor.˜9(4), 71–80 (1973); In Russian, English translation in Problems of Infor. Trans., 325–332 (1975) · Zbl 0312.22011

[25] Radhakrishnan, J., Ta-Shma, A.: Bounds for Dispersers, Extractors, and Depth-Two Superconcentrators. SIAM J. Discrete Math.˜13(1), 2–24 (2000) · Zbl 1023.94025 · doi:10.1137/S0895480197329508

[26] Reingold, O., Vadhan, S., Wigderson, A.: Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors. ECCC, TR01-018, 2001; Preliminary version in 41st FOCS, pp. 3–13 (2000)

[27] Sipser, M.: Expanders, Randomness or Time vs Space, Proceedings of the Structure in Complexity Theory (1986) · Zbl 0606.68042 · doi:10.1007/3-540-16486-3$_1$08

[28] Shaltiel, R.: Recent Developments in Explicit Constructions of Extractors. In: Paun, G., Rozenberg, G., Salomaa, A. (eds.) Current Trends in Theoretical Computer Science: The Challenge of the New Century. Algorithms and Complexity, vol.˜1, pp. 67–95. World scietific (2004); Preliminary version in Bulletin of the EATCS 77, pages 67–95, 2002 · Zbl 1051.68070

[29] Trevisan, L.: When Hamming meets Euclid: The Approximability of Geometric TSP and MST. In: 29th STOC, pp. 21–29 (1997) · Zbl 0962.68164

[30] Zuckerman, D.: Randomness-Optimal Oblivious Sampling. In: Journal of Random Structures and Algorithms, vol.˜11(4), pp. 345–367 (1997); Preliminary version in 28th STOC, pages 286–295, 1996 · Zbl 0891.60100