Goldreich, Oded; **Vadhan, Salil**

On the complexity of computational problems regarding distributions. (English)

Zbl 1343.68115

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, 390-405 (2011).

Summary: We consider two basic computational problems regarding discrete probability distributions: (1) approximating the statistical difference (aka variation distance) between two given distributions, and (2) approximating the entropy of a given distribution. Both problems are considered in two different settings. In the first setting the approximation algorithm is only given samples from the distributions in question, whereas in the second setting the algorithm is given the "code" of a sampling device (for the distributions in question).

We survey the know results regarding both settings, noting that they are fundamentally different: The first setting is concerned with the number of samples required for determining the quantity in question, and is thus essentially information theoretic. In the second setting the quantities in question are determined by the input, and the question is merely one of computational complexity. The focus of this survey is actually on the latter setting. In particular, the survey includes proof sketches of three central results regarding the latter setting, where one of these proofs has only appeared before in the second author's PhD Thesis.

For the entire collection see [Zbl 1220.68005].

MSC:

68Q25	Analysis of algorithms and problem complexity
62E99	Statistical distribution theory
68Q87	Probability in computer science (algorithm analysis, random structures, phase transitions, etc.)
94A17	Measures of information, entropy

Keywords:

approximation; reductions; entropy; statistical difference; variation distance; sampleable distributions; zero-knowledge; promise problems

Full Text: DOI

References:

[1] Aiello, W., Håstad, J.: Perfect Zero-Knowledge Languages can be Recognized in Two Rounds. In: 28th FOCS, pp. 439–448 (1987) · Zbl 0732.68038 · doi:10.1109/SFCS.1987.47

[2] Barak, B.: Non-Black-Box Techniques in Cryptography. Ph.D. Thesis, Weizmann Institute of Science (January 2004)

[3] Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S.P., Yang, K.: On the (Im)possibility of obfuscating programs. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol.˜2139, pp. 1–18. Springer, Heidelberg (2001) · Zbl 1001.68511 · doi:10.1007/3-540-44647-8$_1$

[4] Batu, T., Dasgupta, S., Kumar, R., Rubinfeld, R.: The Complexity of Approximating the Entropy. In: 34th STOC (2002) · Zbl 1192.94074

[5] Batu, T., Fischer, E., Fortnow, L., Kumar, R., Rubinfeld, R., White, P.: Testing random variables for independence and identity. In: 42nd FOCS (2001)· doi:10.1109/SFCS.2001.959920

[6] Batu, T., Fortnow, L., Rubinfeld, R., Smith, W.D., White, P.: Testing that distributions are close. In: 41st FOCS, pp. 259–269 (2000)· doi:10.1109/SFCS.2000.892113

[7] Bellare, M., Goldreich, O., Sudan, M.: Free Bits, PCPs and Non-Approximability – Towards Tight Results. SICOMP˜27(3), 804–915 (1998) · Zbl 0912.68041 · doi:10.1137/S0097539796302531

[8] Carter, L., Wegman, M.: Universal Hash Functions. JCSS˜18, 143–154 (1979) · Zbl 0412.68090

[9] Ergun, F., Kannan, S., Kumar, S.R., Rubinfeld, R., Viswanathan, M.: Spot-checkers. JCSS˜60(3), 717–751 (2000) · Zbl

0961.68036

[10] Even, S., Selman, A.L., Yacobi, Y.: The Complexity of Promise Problems with Applications to Public-Key Cryptography. Inform. and Control˜61, 159–173 (1984) · Zbl 0592.94012 · doi:10.1016/S0019-9958(84)80056-X

[11] Fortnow, L.: The Complexity of Perfect Zero-Knowledge. In: 19th STOC, pp. 204–209 (1987)· doi:10.1145/28395.28418

[12] Goldreich, O., Goldwasser, S., Ron, D.: Property testing and its connection to learning and approximation. JACM, 653–750 (July 1998) · Zbl 1065.68575 · doi:10.1145/285055.285060

[13] Goldreich, O.V., Kushilevitz, E.V.: A Perfect Zero-Knowledge Proof for a Decision Problem Equivalent to Discrete Logarithm. JofC˜6(2), 97–116 (1993) · Zbl 0783.68039

[14] Goldreich, O., Micali, S., Wigderson, A.: Proofs that Yield Nothing but their Validity or All Languages in NP Have Zero-Knowledge Proof Systems. JACM˜38(1), 691–729 (1991); Preliminary version in 27th FOCS (1986) · Zbl 0799.68101

[15] Goldreich, O., Sahai, A., Vadhan, S.: Honest-Verifier Statistical Zero-Knowledge equals general Statistical Zero-Knowledge. In: 30th STOC, pp. 399–408 (1998) · Zbl 1027.68695 · doi:10.1145/276698.276852

[16] Goldreich, O., Sahai, A., Vadhan, S.P.: Can Statistical Zero-Knowledge be Made Non-Interactive? or On the Relationship of SZK and NISZK. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol.˜1666, pp. 467–484. Springer, Heidelberg (1999) · Zbl 0942.68046 · doi:10.1007/3-540-48405-1$_3$0

[17] Goldreich, O., Vadhan, S.: Comparing Entropies in Statistical Zero-Knowledge with Applications to the Structure of SZK. In: 14th IEEE Conference on Computational Complexity, pp. 54–73 (1999)· doi:10.1109/CCC.1999.766262

[18] Goldwasser, S., Micali, S., Rackoff, C.: The Knowledge Complexity of Interactive Proof Systems. SICOMP˜18, 186–208 (1989); Preliminary version in 17th STOC (1985); Earlier versions date to (1982) · Zbl 0677.68062 · doi:10.1137/0218012

[19] Okamoto, T.: On relationships between statistical zero-knowledge proofs. In: 28th STOC, pp. 649–658 (1996) · Zbl 0922.68049 · doi:10.1145/237814.238016

[20] Rubinfeld, R., Sudan, M.: Robust Characterizations of Polynomials with Applications to Program Checking. SICOMP˜25(2), 252–271 (1996); Preliminary version in 3rd SODA (1992) · Zbl 0844.68062 · doi:10.1137/S0097539793255151

[21] Sahai, A., Vadhan, S.: A Complete Promise Problem for Statistical Zero-Knowledge. In: 38th FOCS, pp. 448–457 (1997)· doi:10.1109/SFCS.1997.646133

[22] Vadhan, S.: A Study of Statistical Zero-Knowledge Proofs. PhD Thesis, Department of Mathematics, MIT (1999)

[23] Valiant, G., Valiant, P.: A CLT and tight lower bounds for estimating entropy. In: ECCC, TR10-179 (2010)

[24] Valiant, G., Valiant, P.: Estimating the unseen: A sublinear-sample canonical estimator of distributions.In: ECCC, TR10-180 (2010)

[25] Valiant, P.: Testing symmetric properties of distributions. In: ECCC, TR07-135 (2007)

[26] Wyner, A.D.: The wire-tap channel. Bell System Technical Journal˜54(8), 1355–1387 (1975) · Zbl 0316.94017 · doi:10.1002/j.1538-7305.1975.tb02040.x