Goldreich, Oded

Short locally testable codes and proofs. (English) Zbl 1309.68220

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, 333-372 (2011).

Summary: We survey known results regarding locally testable codes and locally testable proofs (known as PCPs), with emphasis on the length of these constructs. Local testability refers to approximately testing large objects based on a very small number of probes, each retrieving a single bit in the representation of the object. This yields super-fast approximate-testing of the corresponding property (i.e., be a codeword or a valid proof). We also review the related concept of local decodable codes.

The survey consists of two independent (i.e., self-contained) parts that cover the same material at different levels of rigor and detail. Still, in spite of the repetitions, there may be a benefit in reading both parts.

For the entire collection see [Zbl 1220.68005].

MSC:

68W20	Randomized algorithms
68P30	Coding and information theory (compaction, compression, models of communication, encoding schemes, etc.) (aspects in computer science)
68Q25	Analysis of algorithms and problem complexity
68Q60	Specification and verification (program logics, model checking, etc.)
94B60	Other types of codes

Keywords:

error-correcting codes; probabilistically checkable proofs; locally testable codes; locally decodable codes; self-correction; low-degree tests; derandomization; private information retrieval

Full Text: DOI

References:

[1] Alon, N., Kaufman, T., Krivelevich, M., Litsyn, S.N., Ron, D.: Testing low-degree polynomials over GF(2). In: Arora, S., Jansen, K., Rolim, J.D.P., Sahai, A. (eds.) RANDOM 2003 and APPROX 2003. LNCS, vol.˜2764, pp. 188–199. Springer, Heidelberg (2003) · Zbl 1247.94058 · doi:10.1007/978-3-540-45198-3$_1$7

[2] Ambainis, A.: An upper bound on the communication complexity of private information retrieval. In: Degano, P., Gorrieri, R., Marchetti-Spaccamela, A. (eds.) ICALP 1997. LNCS, vol.˜1256, pp. 401–407. Springer, Heidelberg (1997) · Zbl 1401.68065 · doi:10.1007/3-540-63165-8$_1$96

[3] Arora, S.: Probabilistic checking of proofs and the hardness of approximation problems. PhD thesis, UC Berkeley (1994)

[4] Arora, S., Lund, C., Motwani, R., Sudan, M., Szegedy, M.: Proof verification and the hardness of approximation problems. JACM˜45,3, 501–555 (1998); Preliminary Version in 33rd FOCS, 1992 · Zbl 1065.68570

[5] Arora, S., Safra, S.: Probabilistic checking of proofs: A new characterization of˜NP. JACM˜45(1), 70–122 (1998): Preliminary Version in 33rd FOCS 1992 · Zbl 0903.68076 · doi:10.1145/273865.273901

[6] Babai, L., Fortnow, L., Lund, C.: Non-deterministic exponential time has two-prover interactive protocols. Computational Complexity˜1(1), 3–40 (1991) · Zbl 0774.68041 · doi:10.1007/BF01200056

[7] Babai, L., Fortnow, L., Levin, L.A., Szegedy, M.: Checking computations in polylogarithmic time. In: Proc. 23rd ACM Symposium on the Theory of Computing, pp. 21–31. D, F (1991)

[8] Barak, B.: How to go beyond the black-box simulation barrier. In: Proc. 42nd IEEE Symposium on Foundations of Computer Science , pp. 106–115 (October 2001)· doi:10.1109/SFCS.2001.959885

[9] Beimel, A., Ishai, Y., Kushilevitz, E., Raymond, J.F.: Breaking the O(n 1/(2k\ -\ 1)) barrier for information-theoretic private information retrieval. In: Proc. 43rd FOCS, pp. 261–270 (November 2002)

[10] Bellare, M., Coppersmith, D., Håstad, J., Kiwi, M., Sudan, M.: Linearity testing in characteristic two. In: Proceedings of the 36th FOCS, pp. 432–441 (1995) · Zbl 0938.68926

[11] Bellare, M., Goldreich, O., Sudan, M.: Free bits, PCPs, and nonapproximability–towards tight results. In: SICOMP, vol.˜27,

3, pp. 804–915 (1998); Preliminary Version in 36th FOCS 1995 · Zbl 0912.68041

[12] Bellare, M., Goldwasser, S., Lund, C., Russell, A.: Efficient probabilistically checkable proofs and applications to approximation. In: Proc. 25th STOC, pp. 294–304 (May 1993) · Zbl 1310.68083 · doi:10.1145/167088.167174

[13] Bellare, M., Sudan, M.: Improved non-approximability results. In: Proceedings of the 26th Annual ACM Symposium on the Theory of Computing, pp. 184–193 (1994) · Zbl 1344.68094 · doi:10.1145/195058.195129

[14] Ben-Sasson, E., Goldreich, O., Sudan, M.: Bounds on 2-Query Codeword Testing. In: Arora, S., Jansen, K., Rolim, J.D.P., Sahai, A. (eds.) RANDOM 2003 and APPROX 2003. LNCS, vol.˜2764, pp. 216–227. Springer, Heidelberg (2003) · Zbl 1279.94142 · doi:10.1007/978-3-540-45198-3$_1$9

[15] Ben-Sasson, E., Goldreich, O., Harsha, P., Sudan, M., Vadhan, S.: Robust PCPs of proximity, shorter PCPs and applications to coding. In: Proc. 36th STOC, pp. 1–10 (June 2004); See ECCC Technical Report TR04-021, March 2004 · Zbl 1118.68071

[16] Ben-Sasson, E., Goldreich, O., Harsha, P., Sudan, M., Vadhan, S.: Short PCPs verifiable in polylogarithmic time. In: 20th IEEE Conference on Computational Complexity, pp. 120–134 (2005)· doi:10.1109/CCC.2005.27

[17] Ben-Sasson, E., Guruswami, V., Kaufman, T., Sudan, M., Viderman, M.: Locally testable codes require redundant testers. In: IEEE Conference on Computational Complexity, pp. 52–61 (2009) · Zbl 1209.68265

[18] Ben-Sasson, E., Harsha, P., Raskhodnikova, S.: Some 3CNF properties are hard to test. In: Proc. 35th STOC, pp. 345–354. s, f (2003) · Zbl 1192.68347 · doi:10.1145/780542.780594

[19] Ben-Sasson, E., Sudan, M.: Robust Locally Testable Codes and Products of Codes. In: Jansen, K., Khanna, S., Rolim, J.D.P., Ron, D. (eds.) RANDOM 2004 and APPROX 2004. LNCS, vol.˜3122, pp. 286–297. Springer, Heidelberg (2004) · Zbl 1105.68346 · doi:10.1007/978-3-540-27821-4$_2$6

[20] Ben-Sasson, E., Sudan, M.: Short PCPs with polylog query complexity. In: SICOMP, vol.˜38(2), pp. 551–607 (2008); Preliminary Version in 37th STOC 2005) · Zbl 1172.68025

[21] Ben-Sasson, E., Sudan, M., Vadhan, S., Wigderson, A.: Randomness-efficient low degree tests and short PCPs via epsilon-biased sets. In: Proc. 35th STOC, pp. 612–621 (June 2003) · Zbl 1192.94089 · doi:10.1145/780542.780631

[22] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. JCSS˜47, 3 (December 1993), 549–595. (Preliminary Version in 22nd STOC, 1990). · Zbl 0795.68131

[23] Buhrman, H., de Wolf, R.: On relaxed locally decodable codes(July 2004) Unpublished manuscript

[24] Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology. In: Proc. 30th STOC, pp. 209–218 (May 1998) (revisited) · Zbl 1027.68603

[25] Chor, B., Goldreich, O., Kushilevitz, E., Sudan, M.: Private Information Retrieval. Journal of the ACM˜45(6), 965–982 (1998) · Zbl 1065.68524 · doi:10.1145/293347.293350

[26] Dinur, I.: The PCP theorem by gap amplification. JACM˜54(3) Art. 12 (2007); Extended abstract in 38th STOC 2006 · Zbl 1301.68133

[27] Dinur, I., Harsha, P.: Composition of low-error 2-query PCPs using decodable PCPs. In: 50th FOCS, pp. 472–481 (2009) · Zbl 1292.68083 · doi:10.1109/FOCS.2009.8

[28] Dinur, I., Reingold, O.: Assignment-testers: Towards a combinatorial proof of the PCP-Theorem. SICOMP˜36(4), 975–1024 (2006); Extended abstract in 45th FOCS 2004 · Zbl 1127.68031 · doi:10.1137/S0097539705446962

[29] Efremenko, K.: 3-query locally decodable codes of subexponential length. In: 41st STOC, pp. 39–44 (2009) · Zbl 1304.94124 · doi:10.1145/1536414.1536422

[30] Ergün, F., Kumar, R., Rubinfeld, R.: Fast approximate PCPs. In: Proc. 31st STOC, pp. 41–50 (May 1999) · Zbl 1346.68097 · doi:10.1145/301250.301267

[31] Feige, U., Goldwasser, S., Lovász, L., Safra, S., Szegedy, M.: Interactive proofs and the hardness of approximating cliques. JACM˜43(2), 268–292 (1996); Preliminary version in 32nd FOCS 1991 · Zbl 0882.68129 · doi:10.1145/226643.226652

[32] Forney, G.D.: Concatenated Codes. MIT Press, Cambridge (1966) · Zbl 0264.94006

[33] Fortnow, L., Rompel, J., Sipser, M.: On the power of multi-prover interactive protocols. Theoretical Computer Science˜134, 2, 545–557 (November 1994) · Zbl 0938.68824 · doi:10.1016/0304-3975(94)90251-8

[34] Friedl, K., Sudan, M.: Some improvements to total degree tests. In: Proc. 3rd Israel Symposium on Theoretical and Computing Systems, Tel Aviv, Israel, January 4–6, pp. 190–198 (1995)· doi:10.1109/ISTCS.1995.377032

[35] Gemmell, P., Lipton, R., Rubinfeld, R., Sudan, M., Wigderson, A.: Self-testing/correcting for polynomials and for approximate functions. In: Proc. 23rd STOC, pp. 32–42 (1991)· doi:10.1145/103418.103429

[36] Goldreich, O.: Short locally testable codes and proofs (survey). ECCC Technical Report TR05-014 (January 2005) · Zbl 1309.68220

[37] Goldreich, O.: Computational Complexity: A Conceptual Perspective. Cambridge University Press, Cambridge (2008) · Zbl 1154.68056 · doi:10.1017/CBO9780511804106

[38] Newman, I.: Property testing of massively parametrized problems - A survey. In: Goldreich, O. (ed.) Property Testing. LNCS, vol.˜6390, pp. 142–157. Springer, Heidelberg (2010) · Zbl 1309.68227 · doi:10.1007/978-3-642-16367-8$_8$

[39] Goldreich, O., Goldwasser, S., Ron, D.: Property testing and its connection to learning and approximation. JACM˜45(4), 653–750 (1998); Preliminary Version in 37th FOCS 1996 · Zbl 1065.68575 · doi:10.1145/285055.285060

[40] Goldreich, O., Ron, D.: On proximity oblivious testing. ECCC, TR08-041, 2008. Also in the proceedings of the 41st STOC (2009)

[41] Goldreich, O., Karloff, H., Schulman, L., Trevisan, L.: Lower bounds for linear locally decodable codes and private information

retrieval. In: Proc. 17th Conference on Computational Complexity, Montréal, Québec, Canada, May 21–24, pp. 175–183 (2002) · Zbl 1113.68049 · doi:10.1109/CCC.2002.1004353

[42] Goldreich, O., Sudan, M.: Locally testable codes and PCPs of almost linear length. In: Proc.43rd FOCS, pp. 13–22 (November 2002); See ECCC Report TR02-050 2002 · Zbl 1315.94144

[43] Harsha, P., Sudan, M.: Small PCPs with low query complexity. Computational Complexity˜9 (3–4), 157–201 (2001); Preliminary Version in 18th STACS 2001 · Zbl 0986.68134

[44] Håstad, J.: Clique is hard to approximate within n 1\ -\ {\(\epsilon\)} . Acta Mathematica˜182, 105–142 (1999); Preliminary Versions in 28th STOC 1996 and 37th FOCS 1997 · Zbl 0989.68060

[45] Håstad, J.: Some optimal inapproximability results. Journal of the ACM˜48(4), 798–859 (2001); Preliminary Version in 29th STOC 1997 · Zbl 1127.68405 · doi:10.1145/502090.502098

[46] Katz, J., Trevisan, L.: On the efficiency of local decoding procedures for error-correcting codes. In: Proc. 32nd STOC, pp. 80–86 (2000) · Zbl 1296.94171 · doi:10.1145/335305.335315

[47] Kaufman, T., Litsyn, S., Xie, N.: Breaking the {\(\epsilon\)}-soundness bound of the linearity test over GF(2). SICOMP˜39(5), 1988–2003 (2009) · Zbl 1202.68178 · doi:10.1137/080715548

[48] Kerenidis, I., de Wolf, R.: Exponential lower bound for 2-query locally decodable codes via a quantum argument. In: Proc. 35th STOC, pp. 106–115 (June 2003) · Zbl 1192.81082 · doi:10.1145/780542.780560

[49] Kilian, J.: A note on efficient zero-knowledge proofs and arguments (extended abstract). In: Proc. 24th STOC, pp. 723–732 (May 1992)· doi:10.1145/129712.129782

[50] Lapidot, D., Shamir, A.: Fully parallelized multi prover protocols for NEXP-time (extended abstract). In: Proc. 32nd FOCS, pp. 13–18 (October 1991) · Zbl 0877.68078

[51] Lund, C., Fortnow, L., Karloff, H., Nisan, N.: Algebraic methods for interactive proof systems. JACM˜39(4), 859–868 (1992) · Zbl 0799.68097 · doi:10.1145/146585.146605

[52] Meir, O.: Combinatorial construction of locally testable codes. SICOMP˜39(2), 491–544 (2009); Extended abstrat in 40th STOC 2008 · Zbl 1202.68235 · doi:10.1137/080729967

[53] Meir, O.: Combinatorial PCPs with efficient verifiers. In: 50th FOCS, pp. 463–471 (2009) · Zbl 1292.68078 · doi:10.1109/FOCS.2009.10

[54] Micali, S.: Computationally sound proofs. SICOMP˜30(4), 1253–1298 (2000); Preliminary Version in 35th FOCS 1994 · Zbl 1009.68053 · doi:10.1137/S0097539795284959

[55] Moshkovitz, D., Raz, R.: Two query PCP with sub-constant error. In: 49th FOCS, pp. 314–323 (2008)· doi:10.1109/FOCS.2008.60

[56] Polishchuk, A., Spielman, D.A.: Nearly-linear size holographic proofs. In: Proc. 26th STOC, pp. 194–203 (May 1994) · Zbl 1345.68180 · doi:10.1145/195058.195132

[57] Raz, R.: A parallel repetition theorem. SIAM Journal of Computing˜27(3), 763–803 (1998); Preliminary Version in 27th STOC 1995 · Zbl 0911.68082 · doi:10.1137/S0097539795280895

[58] Rubinfeld, R., Sudan, M.: Robust characterizations of polynomials with applications to program testing. SICOMP˜25(2), 252–271 (1996); Preliminary Version in 3rd SODA 1992 · Zbl 0844.68062 · doi:10.1137/S0097539793255151

[59] Spielman, D.: Computationally efficient error-correcting codes and holographic proofs. PhD thesis, Massachusetts Institute of Technology (June 1995)

[60] Sudan, M.: Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems. LNCS, vol.˜1001. Springer, Heidelberg (1995) · Zbl 0861.68042 · doi:10.1007/3-540-60615-7

[61] Szegedy, M.: Many-valued logics and holographic proofs. In: Wiedermann, J., Van Emde Boas, P., Nielsen, M. (eds.) ICALP 1999. LNCS, vol.˜1644, pp. 676–686. Springer, Heidelberg (1999) · Zbl 0938.03022 · doi:10.1007/3-540-48523-6$_64$

[62] Yekhanin, S.: Towards 3-Query locally decodable codes of subexponential length. In: 39th STOC, pp. 266–274 (2007) · Zbl 1232.94020