Arora, Sanjeev; **Ge, Rong**

New algorithms for learning in presence of errors. (English) Zbl 1332.68099

Aceto, Luca (ed.) et al., Automata, languages and programming. 38th international colloquium, ICALP 2011, Zurich, Switzerland, July 4–8, 2011. Proceedings, Part I. Berlin: Springer (ISBN 978-3-642-22005-0/pbk). Lecture Notes in Computer Science 6755, 403-415 (2011).

Summary: We give new algorithms for a variety of randomly-generated instances of computational problems using a linearization technique that reduces to solving a system of linear equations.

These algorithms are derived in the context of learning with structured noise, a notion introduced in this paper. This notion is best illustrated with the learning parities with noise (LPN) problem – well-studied in learning theory and cryptography. In the standard version, we have access to an oracle that, each time we press a button, returns a random vector $a \in \mathrm{GF}(2)^n$ together with a bit $b \in \mathrm{GF}(2)$ that was computed as $a \cdot u + \eta$, where $u \in \mathrm{GF}(2)^n$ is a secret vector, and $\eta \in \mathrm{GF}(2)$ is a noise bit that is 1 with some probability p. Say $p = 1/3$. The goal is to recover u. This task is conjectured to be intractable.

In the structured noise setting we introduce a slight (?) variation of the model: upon pressing a button, we receive (say) 10 random vectors $a_1, a_2, \ldots, a_{10} \in \mathrm{GF}(2)^n$, and corresponding bits $b_1, b_2, \cdots, b_{10}$, of which at most 3 are noisy. The oracle may arbitrarily decide which of the 10 bits to make noisy. We exhibit a polynomial-time algorithm to recover the secret vector u given such an oracle. We think this structured noise model may be of independent interest in machine learning.

We discuss generalizations of our result, including learning with more general noise patterns. We also give the first nontrivial algorithms for two problems, which we show fit in our structured noise framework.

We give a slightly subexponential algorithm for the well-known learning with errors (LWE) problem over $\mathrm{GF}(q)$ introduced by *O. Regev* [J. ACM 56, No. 6, Article No. 34, 40 p. (2009; Zbl 1325.68101)] for cryptographic uses. Our algorithm works for the case when the Gaussian noise is small; which was an open problem. Our result also clarifies why existing hardness results fail at this particular noise rate.

We also give polynomial-time algorithms for learning the MAJORITY OF PARITIES function of *B. Applebaum* et al. [in: Proceedings of the 42nd annual ACM symposium on theory of computing, STOC '10. New York, NY: Association for Computing Machinery (ACM). 171–180 (2010; Zbl 1293.94052)] for certain parameter values. This function is a special case of Goldreich's pseudorandom generator.

The full version is available at http://www.eccc.uni-trier.de/report/2010/066/.

For the entire collection see [Zbl 1217.68003].

MSC:

68Q32 Computational learning theory
68T05 Learning and adaptive systems in artificial intelligence
94A60 Cryptography

Full Text: DOI

References:

[1] Ajtai, M.: Generating hard instances of lattice problems (extended abstract). In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing (1996) · Zbl 0921.11071 · doi:10.1145/237814.237838

[2] Ajtai, M., Dwork, C.: A public-key cryptosystem with worst-case/average-case equivalence. In: Proceedings of the 29th Annual ACM Symposium on Theory of Computing (1997) · Zbl 0962.68055 · doi:10.1145/258533.258604

[3] Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol.˜5444, pp. 474–495. Springer, Heidelberg (2009) · Zbl 1213.94075 · doi:10.1007/978-3-642-00457-5_28

[4] Alekhnovich, M.: More on average case vs approximation complexity. In: Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (2003) · Zbl 1242.68109 · doi:10.1109/SFCS.2003.1238204

[5] Applebaum, B., Barak, B., Wigderson, A.: Public key cryptography from different assumptions. In: Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (2010) · Zbl 1293.94052 · doi:10.1145/1806689.1806715

[6] Bard, G.V.: Algebraic Cryptanalysis. Springer, Heidelberg (2009) · Zbl 1183.94019 · doi:10.1007/978-0-387-88757-9

[7] Blum, A., Furst, M.L., Kearns, M.J., Lipton, R.J.: Cryptographic primitives based on hard learning problems. In: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology (1994) · Zbl 0870.94021 · doi:10.1007/3-540-48329-2_24

[8] Blum, A., Kalai, A., Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model. Journal of ACM (2003) · Zbl 1325.68114 · doi:10.1145/792538.792543

[9] Bogdanov, A., Qiao, Y.: On the security of goldreich's one-way function. In: Dinur, I., Jansen, K., Naor, J., Rolim, J. (eds.) APPROX 2009. LNCS, vol.˜5687, pp. 392–405. Springer, Heidelberg (2009) · Zbl 1255.94053 · doi:10.1007/978-3-642-03685-9_30

[10] Feldman, V., Gopalan, P., Khot, S., Ponnuswami, A.K.: New results for learning noisy parities and halfspaces. In: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (2006) · Zbl 1198.68156 · doi:10.1109/FOCS.2006.51

[11] Friedl, K., Ivanyos, G., Magniez, F., Santha, M., Sen, P.: Hidden translation and orbit coset in quantum computing. In: Proceedings of the 35th Annual ACM Symposium on Theory of Computing (2003) · Zbl 1192.81066 · doi:10.1145/780542.780544

[12] Goldreich, O.: Candidate one-way functions based on expander graphs. technical report. TR00-090, Electronic Colloquium on Computational Complexity, ECCC (2000) · Zbl 1306.94056

[13] Hopper, N.J., Blum, M.: Secure human identification protocols. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol.˜2248, p. 52. Springer, Heidelberg (2001) · Zbl 1062.94549 · doi:10.1007/3-540-45682-1_4

[14] Kearns, M.: Efficient noise-tolerant learning from statistical queries. Journal of ACM (1998) · Zbl 1065.68605 · doi:10.1145/293347.293351

[15] Micciancio, D., Regev, O.: Lattice-based cryptography. In: Post Quantum Cryptography (2009) · Zbl 1161.81324 · doi:10.1007/978-3-540-88702-7_5

[16] Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of 41st ACM Symposium on Theory of Computing (2009) · Zbl 1304.94079 · doi:10.1145/1536414.1536461

[17] Peikert, C., Vaikuntanathan, V., Waters, B.: A framework for efficient and composable oblivious transfer. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol.˜5157, pp. 554–571. Springer, Heidelberg (2008) · Zbl 1183.94046 · doi:10.1007/978-3-540-85174-5_31

[18] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of ACM (2009) · Zbl 1325.68101 · doi:10.1145/1568318.1568324