Proceedings of Machine Learning Research vol 291:1–3, 2025 38th Annual Conference on Learning Theory

Algorithms for Sparse LPN and LSPN Against Low-noise

Xue Chen[*] XUECHEN1989@USTC.EDU.CN
University of Science and Technology of China, Hefei 230026, China & Hefei National Laboratory, Hefei 230088, China

Wenxuan Shu WXSHU@MAIL.USTC.EDU.CN
University of Science and Technology of China, Hefei 230026, China

Zhaienhe Zhou ZHAIENHEZHOU@GMAIL.COM
University of Science and Technology of China, Hefei 230026, China

Editors: Nika Haghtalab and Ankur Moitra

Abstract

We consider sparse variants of the classical Learning Parities with random Noise (LPN) problem. Our main contribution is a new algorithmic framework that provides learning algorithms against low-noise for both Learning Sparse Parities (LSPN) problem and sparse LPN problem. Different from previous approaches for LSPN and sparse LPN (Grigorescu et al., 2011; Valiant, 2015; Karppa et al., 2018; Raghavendra et al., 2017; Guruswami et al., 2022), this framework has a simple structure without fast matrix multiplication or tensor methods such that its algorithms are easy to implement and run in polynomial space. Let n be the dimension, k denote the sparsity, and η be the noise rate such that each label gets flipped with probability η.

As a fundamental problem in computational learning theory (Feldman et al., 2009), Learning Sparse Parities with Noise (LSPN) assumes the hidden parity is k-sparse instead of a potentially dense vector. While the simple enumeration algorithm takes $\binom{n}{k} = O(n/k)^k$ time, previously known results stills need at least $\binom{n}{k/2} = \Omega(n/k)^{k/2}$ time for any noise rate η (Grigorescu et al., 2011; Valiant, 2015; Karppa et al., 2018). Our framework provides a LSPN algorithm runs in time $O(\eta \cdot n/k)^k$ for any noise rate η, which improves the state-of-the-art of LSPN whenever $\eta \in (k/n, \sqrt{k/n})$.

The sparse LPN problem is closely related to the classical problem of refuting random k-CSP (Feige et al., 2006; Raghavendra et al., 2017; Guruswami et al., 2022) and has been widely used in cryptography as the hardness assumption (e.g., Alekhnovich, 2003; Applebaum et al., 2010, 2017; Dao et al., 2023). Different from the standard LPN that samples random vectors in $\mathbf{F}_2^n$, it samples random k-sparse vectors. Because the number of k-sparse vectors is $\binom{n}{k} < n^k$, sparse LPN has learning algorithms in polynomial time when $m > n^{k/2}$. However, much less is known about learning algorithms for a constant k like 3 and $m < n^{k/2}$ samples, except the Gaussian elimination algorithm and sum-of-squares algorithms (Barak et al., 2014; Barak and Moitra, 2022; Raghavendra et al., 2017). Our framework provides a learning algorithm in $e^{\tilde{O}(\eta \cdot n^{\frac{\delta+1}{2}})}$ time given $\delta \in (0,1)$ and $m = \max\{1, \frac{\eta \cdot n^{\frac{\delta+1}{2}}}{k^2}\} \cdot n^{1+(1-\delta)\cdot\frac{k-1}{2}}$ samples. This improves previous learning algorithms. For example, in the classical setting of $k = 3$ and $m = n^{1.4}$ (Feige et al., 2006; Applebaum et al., 2010), our algorithm would be faster than previous approaches for any $\eta < n^{-0.7}$.

Keywords: computational learning theory, Learning Parities with Noise (LPN), Learning Sparse Parities with Noise (LSPN), sparse LPN

[*] Extended abstract. Full version appears as [arXiv:2407.19215, v8]

Acknowledgments

Xue Chen is supported by Innovation Program for Quantum Science and Technology 2021ZD0302901, NSFC 62372424, and CCF-HuaweiLK2023006.

References

Michael Alekhnovich. More on average case vs approximation complexity. FOCS '03, page 298. IEEE Computer Society, 2003. ISBN 0769520405.

Benny Applebaum, Boaz Barak, and Avi Wigderson. Public-key cryptography from different assumptions. In *Proceedings of the Forty-Second ACM Symposium on Theory of Computing*, STOC '10, page 171–180. Association for Computing Machinery, 2010. ISBN 9781450300506. doi: 10.1145/1806689.1806715.

Benny Applebaum, Ivan Damgård, Yuval Ishai, Michael Nielsen, and Lior Zichron. Secure arithmetic computation with constant computational overhead. In *Advances in Cryptology – CRYPTO 2017*, pages 223–254. Springer International Publishing, 2017. ISBN 978-3-319-63688-7.

Boaz Barak and Ankur Moitra. Noisy tensor completion via the sum-of-squares hierarchy. *Math. Program.*, 193(2):513–548, June 2022. ISSN 0025-5610. doi: 10.1007/s10107-022-01793-9. URL https://doi.org/10.1007/s10107-022-01793-9.

Boaz Barak, Jonathan A. Kelner, and David Steurer. Rounding sum-of-squares relaxations. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '14, page 31–40, New York, NY, USA, 2014. Association for Computing Machinery. ISBN 9781450327107. doi: 10.1145/2591796.2591886. URL https://doi.org/10.1145/2591796.2591886.

Quang Dao, Yuval Ishai, Aayush Jain, and Huijia Lin. Multi-party homomorphic secret sharing and sublinear mpc from sparse LPN. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023*, page 315–348. Springer-Verlag, 2023. ISBN 978-3-031-38544-5. doi: 10.1007/978-3-031-38545-2_11.

Uriel Feige, Jeong Han Kim, and Eran Ofek. Witnesses for non-satisfiability of dense random 3CNF formulas. In *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, pages 497–508, 2006. doi: 10.1109/FOCS.2006.78.

Vitaly Feldman, Parikshit Gopalan, Subhash Khot, and Ashok Kumar Ponnuswami. On agnostic learning of parities, monomials, and halfspaces. *SIAM J. Comput.*, 39(2):606–645, jul 2009. ISSN 0097-5397. doi: 10.1137/070684914.

Elena Grigorescu, Lev Reyzin, and Santosh Vempala. On noise-tolerant learning of sparse parities and related problems. In *Proceedings of the 22nd International Conference on Algorithmic Learning Theory*, ALT'11, page 413–424, 2011. ISBN 9783642244117.

Venkatesan Guruswami, Pravesh K. Kothari, and Peter Manohar. Algorithms and certificates for boolean CSP refutation: Smoothed is no harder than random. *SIAM Journal on Computing*, 0(0): STOC22–282–STOC22–337, 2022. doi: 10.1137/22M1537771.

Matti Karppa, Petteri Kaski, and Jukka Kohonen. A faster subquadratic algorithm for finding outlier correlations. *ACM Trans. Algorithms*, 14(3), jun 2018. ISSN 1549-6325. doi: 10.1145/3174804.

Prasad Raghavendra, Satish Rao, and Tselil Schramm. Strongly refuting random CSPs below the spectral threshold. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, page 121–131. ACM, 2017. ISBN 9781450345286. doi: 10.1145/3055399.3055417.

Gregory Valiant. Finding correlations in subquadratic time, with applications to learning parities and the closest pair problem. *J. ACM*, 62(2), may 2015. ISSN 0004-5411. doi: 10.1145/2728167.