Title: Parity learning

URL: https://en.wikipedia.org/wiki/Parity_learning

PageID: 23864280

Categories: Category:Applied mathematics stubs, Category:Machine learning, Category:Machine learning stubs

---

Parity learning is a problem in machine learning . An algorithm that solves this problem must find a function f , given some samples (x , f (x)) and the assurance that f computes the parity of bits at some fixed locations. The samples are generated using some distribution over the input. The problem is easy to solve using Gaussian elimination provided that a sufficient number of samples (from a distribution which is not too skewed) are provided to the algorithm.

Noisy version ("Learning Parity with Noise")

In Learning Parity with Noise (LPN), the samples may contain some error. Instead of samples (x , f (x)), the algorithm is provided with (x , y), where for random boolean $b \in \{ 0 , 1 \}$ {\displaystyle b\in \{0,1\}}

y = { f (x) , if b 1 – f (x) , otherwise {\displaystyle y={\begin{cases}f(x),&{\text{if }}b\\1-f(x),&{\text{otherwise}}\end{cases}}}

The noisy version of the parity learning problem is conjectured to be hard [1] and is widely used in cryptography. [2]

See also

Learning with errors

References

Avrim Blum, Adam Kalai, and Hal Wasserman, “Noise-tolerant learning, the parity problem, and the statistical query model,” J. ACM 50, no. 4 (2003): 506–519.

Adam Tauman Kalai, Yishay Mansour, and Elad Verbin, “On agnostic boosting and parity learning,” in Proceedings of the 40th annual ACM symposium on Theory of computing (Victoria, British Columbia, Canada: ACM, 2008), 629–638, http://portal.acm.org/citation.cfm?id=1374466 .

Oded Regev, “On lattices, learning with errors, random linear codes, and cryptography,” in Proceedings of the thirty-seventh annual ACM symposium on Theory of computing (Baltimore, MD, USA: ACM, 2005), 84–93, http://portal.acm.org/citation.cfm?id=1060590.1060603 .

This applied mathematics –related article is a stub . You can help Wikipedia by expanding it .

v

t

e

This machine learning -related article is a stub . You can help Wikipedia by expanding it .

v

t

e