

# Learnability Beyond $AC^0$

Jeffrey C. Jackson\*  
Duquesne University  
Pittsburgh, PA 15282  
jackson@mathcs.duq.edu

Adam R. Klivans†  
MIT  
Cambridge, MA 02139  
klivans@math.mit.edu

Rocco A. Servedio‡  
Harvard University  
Cambridge, MA 02138  
rocco@cs.harvard.edu

In a celebrated result Linial *et al.* [3] gave an algorithm which learns size- $s$  depth- $d$  AND/OR/NOT circuits in time  $n^{(\log s)^d}$  from uniformly distributed random examples on the Boolean cube  $\{0, 1\}^n$ . Kharitonov [2] subsequently gave compelling evidence that the Linial *et al.* algorithm is essentially optimal, by showing that an  $n^{(\log s)^{o(d)}}$ -time algorithm for learning size- $s$  depth- $d$  circuits under uniform would contradict a plausible cryptographic assumption about the hardness of integer factorization.

We give the first algorithm for learning a more expressive circuit class than the class  $AC^0$  considered by Linial *et al.* and Kharitonov. The new algorithm learns constant-depth AND/OR/NOT circuits augmented with (a limited number of) majority gates. Our main positive result for these circuits can be stated informally as follows (a precise statement is given in [1]):

**Theorem 1** *Quasipolynomial ( $n^{\text{polylog } n}$ ) size constant-depth circuits which contain a polylogarithmic number of majority gates can be learned under the uniform distribution in quasipolynomial time from random examples only.*

As we allow constant depth circuits to contain more and more majority gates we move toward the circuit complexity class  $TC^0$  which can be viewed as  $AC^0$  augmented with a polynomial number of majority gates.  $TC^0$  is a highly expressive class which is not likely to be efficiently learnable. We establish the following lower bound for learning augmented  $AC^0$  circuits which holds under Kharitonov's plausible cryptographic assumption (a precise statement is given in [1]):

**Theorem 2** *Any algorithm that even weakly learns depth-5 circuits containing more than a polylogarithmic number of majority gates under the uniform distribution must run in more than quasipolynomial time, even if membership queries are allowed.*

\*This material is based upon work supported by the National Science Foundation under Grant No. CCR-9877079.

†Supported in part by NSF grant CCR-97-01304.

‡Supported by NSF Grant CCR-98-77049 and by an NSF Mathematical Sciences Postdoctoral Research Fellowship.

Thus our new algorithm is essentially optimal with respect to both running time and expressiveness (number of majority gates) of the circuits being learned.

Our new algorithm uses hypothesis boosting, a well known technique in computational learning theory which can be used to transform a weak learning algorithm (which constructs an approximator to the function being learned which has error only slightly less than  $1/2$ ) into a strong learning algorithm which generates a high accuracy hypothesis. We show that for any function  $f$  in our class and any near-uniform distribution  $\mathcal{D}$ , there exists a low-order parity function which is weakly correlated with  $f$ . Since this parity depends on only a small number of variables it can be found using exhaustive search. We show that the size bound for this parity – and hence the running time of our algorithm – depends directly on the extent of  $\mathcal{D}$ 's deviation from the uniform distribution. Fortunately, there exist known boosting algorithms with the property that if the initial distribution is uniform, then all distributions constructed by the boosting algorithm will remain close to uniform. Using such a boosting algorithm we obtain from our weak learning algorithm a strong learning algorithm which generates a highly accurate approximator to the unknown target function.

We also provide evidence that other augmentations of  $AC^0$  using expressive gates such as PARITY,  $MOD_p$  and arbitrary threshold gates may be difficult to learn using known techniques.

## References

- [1] J. Jackson, A. Klivans, and R. Servedio. Learnability beyond  $AC^0$ . In *Proceedings of the 34th Annual Symposium on Theory of Computing*, 2002.
- [2] M. Kharitonov. Cryptographic hardness of distribution-specific learning. In *Proceedings of the 28th Annual Symposium on Theory of Computing*, pages 372-381, 1993.
- [3] N. Linial, Y. Mansour, and N. Nisan. Constant depth circuits, Fourier transform and learnability. *Journal of the ACM*, 40(3):607-620, 1993.