

# Agnostically Learning Juntas from Random Walks

Jan Arpe\* Elchanan Mossel†

June 25, 2008

## Abstract

We prove that the class of functions  $g : \{-1, +1\}^n \rightarrow \{-1, +1\}$  that only depend on an unknown subset of  $k \ll n$  variables (so-called  $k$ -juntas) is agnostically learnable from a random walk in time polynomial in  $n$ ,  $2^{k^2}$ ,  $\epsilon^{-k}$ , and  $\log(1/\delta)$ . In other words, there is an algorithm with the claimed running time that, given  $\epsilon, \delta > 0$  and access to a random walk on  $\{-1, +1\}^n$  labeled by an arbitrary function  $f : \{-1, +1\}^n \rightarrow \{-1, +1\}$ , finds with probability at least  $1 - \delta$  a  $k$ -junta that is  $(\text{opt}(f) + \epsilon)$ -close to  $f$ , where  $\text{opt}(f)$  denotes the distance of a closest  $k$ -junta to  $f$ .

**Keywords:** agnostic learning, random walks, juntas

## 1 Introduction

### 1.1 Motivation

In supervised learning, the learner is provided with a *training set* of *labeled examples*

$$(x^1, f(x^1)), (x^2, f(x^2)), \dots,$$

and the goal is to find a *hypothesis*  $h$  that is a good approximation to  $f$ , i.e., that gives good estimates for  $f(x)$  also on the points that are not present in the training set. In many applications, the points  $x$  correspond to particular *states* of a system and the labels  $f(x)$  correspond to *classifications* of these states. If the underlying system evolves over time and thus  $(x^t, f(x^t))$  corresponds to a measurement of the current state and its classification at time  $t$ , it is often reasonable to assume that state changes only occur *locally*, i.e., at each time  $t$ ,  $x^t$  differs only “locally” from  $x^{t-1}$ . Such phenomena occur for instance in physics or biology: e.g., in a fixed time interval, a particle can only travel a finite distance and the mutation of a DNA sequence can be assumed to happen in a single position at a time. In discrete settings, such processes are often modeled as *random walks* on graphs, in which the nodes represent the states of the system, and edges indicate possible local state changes.

We are interested in studying the special case that the underlying graph is a hypercube, i.e., the node set is  $\{-1, 1\}^n$  and two nodes are adjacent if and only if they differ in exactly one coordinate. Furthermore, we restrict the setting to *Boolean classifications*. This *random walk learning model* has attracted a lot of attention since the nineties [1, 3, 7, 6, 15], mainly because of its interesting

---

\*U.C. Berkeley. Email: [arpe@stat.berkeley.edu](mailto:arpe@stat.berkeley.edu). Supported by the Postdoc-Program of the German Academic Exchange Service (DAAD) and in part by NSF Career Award DMS 0548249 and BSF 2004105.

†U.C. Berkeley. Email: [mossel@stat.berkeley.edu](mailto:mossel@stat.berkeley.edu). Supported by NSF Career Award DMS 0548249, BSF 2004105, and DOD ONR grant N0014-07-1-05-06.

learning theoretic properties. The model is weaker than the *membership query model* in which the learner is allowed to ask the classifications of specific points, and it is stronger than the *uniform-distribution model* in which the learner observes points that are drawn independently of each other from the uniform distribution on  $\{-1, 1\}^n$ . Moreover, the latter relation is known to be *strict*: under a standard complexity theoretic assumption (existence of one-way functions) there is a class that is efficiently learnable from labeled random walks, but not from independent uniformly distributed examples [6, Proposition 2].

The random walk learning model shares some similarities with both other models mentioned above: as in the uniform-distribution model, the examples are generated at random (so that the learner has no influence on the given examples) and points of the random walk that correspond to time points that are sufficiently far apart roughly behave like independent uniformly distributed points. On the other hand, some learning problems that appear to be infeasible in the uniform distribution model but are known to be easy to solve in the membership query model have turned out to be easy in the random walk model as well. Among them is the problem of learning DNFs with polynomially many terms [6] (even under random classification noise) and the problem of learning parity functions in the presence of random classification noise. The former result relies on an efficient algorithm performing the *Bounded Sieve* [6] introduced in [5]. The latter result follows from the fact that the (noise-less) random walk model admits an efficient approximation of variable influences, and the effect of *random* classification noise can be easily dealt with by drawing a sufficiently larger amount of examples.

Given this success of the random walk model in learning large classes in the presence of random classification noise, it is natural to ask whether it can also cope with even more severe noise models. One elegant, albeit challenging, noise model is the *agnostic learning model* introduced by Kearns et al. [11]. In this model, no assumption whatsoever is made about the labels. Instead of asking for a hypothesis that is close to the classification function, the goal in agnostic learning is to produce a hypothesis that agrees with the labels on nearly as many points as the *best* fitting function from the target class. More formally, given a class  $\mathcal{C}$  of Boolean functions on  $\{-1, 1\}^n$  and an arbitrary function  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ , let  $\text{opt}_{\mathcal{C}}(f) = \min_{g \in \mathcal{C}} \Pr[g(x) \neq f(x)]$ . The class  $\mathcal{C}$  is *agnostically learnable* if there is an algorithm that, for any  $\epsilon, \delta > 0$ , produces a hypothesis  $h$  that, with probability at least  $1 - \delta$ , satisfies  $\Pr[h(x) \neq f(x)] \leq \text{opt}_{\mathcal{C}}(f) + \epsilon$ .

Recently, Gopalan et al. [9] have shown that the class of Boolean functions that can be represented by decision trees of polynomial size (in the number of variables) can be learned agnostically from *membership queries* in polynomial time. Their main result combines the Kushilevitz-Mansour algorithm for finding large Fourier coefficients [12] with a gradient-descent algorithm [16] to solve an  $\ell^1$ -regression problem for sparse polynomials. They also present a simpler algorithm (with slightly worse running time) that *properly* agnostically learns the class of *k-juntas*. These are functions  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$  that depend on an a priori unknown subset of at most  $k$  variables. The term *proper* learning refers to the requirement that only hypotheses from the target class (here: *k-juntas*) are produced.

The investigation of the learnability of this class has both practical and theoretical motivation. Practically, the junta learning problem serves as a clean model of learning in the presence of irrelevant information, a core problem in data mining [4]. From a theoretical perspective, the problem is interesting due to its close relationship to learning DNF formulas, decision trees, and noisy parity functions [14].

## 1.2 Our Results and Techniques

The main result of this paper is that the class of  $k$ -juntas on  $n$  variables is properly agnostically learnable in the random walk model in time polynomial in  $n$  (times some function in  $k$  and the accuracy parameter  $\epsilon$ ). More precisely, we show

**Theorem 1.** *Let  $\mathcal{C}$  be the class of  $k$ -juntas on  $n$  variables. There is an algorithm that, given  $\epsilon, \delta > 0$  and access to a random walk  $x^1, x^2, \dots$  on  $\{-1, 1\}^n$  that is labeled by an arbitrary function  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ , returns a  $k$ -junta  $h$  that, with probability at least  $1 - \delta$ , satisfies*

$$\Pr[h(x) \neq f(x)] \leq \text{opt}_{\mathcal{C}}(f) + \epsilon.$$

*The running time of this algorithm is polynomial in  $n$ ,  $2^{k^2}$ ,  $(1/\epsilon)^k$ , and  $\log(1/\delta)$ .*

We thus prove the first efficient learning result for agnostically learning juntas (even properly) in a *passive* learning model.

Our main technical lemma (Lemma 3) shows that for an arbitrary function  $f$  and a  $k$ -junta  $g$ , there exists another  $k$ -junta  $g'$  that is almost as correlated with  $f$  as  $g$  is and whose relevant variables can be inferred from all low-level Fourier coefficients of  $f$  of a certain size. These Fourier coefficients can in turn be detected using the Bounded Sieve algorithm of Bshouty et al. [6] given a random walk labeled by  $f$ . Once a superset  $R$  of the relevant variables of  $g'$  is found, it is easy to derive a hypothesis that only depends on at most  $k$  variables from  $R$  and that best matches the given labels: For each  $k$ -element subset  $J \subseteq R$ , the best matching function with relevant variables in  $J$  is obtained by taking majority votes on points that coincide in these coordinates. Similarly to the classical result of Angluin and Laird [2] that a (proper) hypothesis that minimizes the number of disagreements with the labels is close to the target function (in the PAC learning model with random classification noise), we show that such a hypothesis is also a good candidate to satisfy the agnostic learning goal in the random walk model (see Proposition 1). A similar statement has implicitly been shown in the agnostic PAC learning model (see the proof of Theorem 1 in [11]).

## 1.3 Related Work

Our algorithm for agnostically learning juntas in the random walk model has some similarities to Gopalan et al.'s recent algorithm for properly agnostically learning juntas in the membership query model [9]. The main differences between the approaches are in two respects: first, we do not explicitly calculate the quantities  $I_i^{\leq k} = \sum_{S: i \in S, |S| \leq k} \hat{f}(S)^2$  but instead use our technical lemma mentioned above, which may be of independent interest. Second, instead of using their characterization of the best fitting junta with a fixed set of relevant variables in terms of the Fourier spectrum of  $f$  ([9, Lemma 13]), we directly construct such a best fitting hypothesis by taking majority votes in ambiguous situations.

Even though we became aware of Gopalan et al.'s result only *after* devising our junta learning algorithm we have decided to adopt much of their notation to the benefit of the readers.

It should also be noted that a generalization of Gopalan et al.'s decision tree learning algorithm cannot be adapted for the random walk model in a straightforward manner: The running time of the only known analogue of the Kushilevitz-Mansour subroutine for the random walk model (i.e., the Bounded Sieve) is exponential in the *level* up to which the large Fourier coefficients are sought. In general, however, sparse polynomials can be concentrated on high levels. It would be interesting to see if the results in [9] can also be derived for the restriction of the class of all  $t$ -sparse polynomials to  $t$ -sparse polynomials of degree roughly  $\log(t)$  since for every decision tree of size  $t$ , there is an  $\epsilon$ -close decision tree of depth  $O(\log(t/\epsilon))$  (cf. [5]). In this case, the same result should hold for the random walk model.

## 1.4 Organization of This Paper

We briefly introduce notational and technical prerequisites in Section 2. The random walk learning model and its agnostic variant are introduced in Section 3. Section 4 contains a concentration for random walks and the result on disagreement minimization in the random walk model. The main result on agnostically learning juntas is presented in Section 5. The Appendix contains a formal statement and proof of a result concerning the independence of points in a random walk (Section A) and an elementary proof of the concentration bound (Section B).

## 2 Preliminaries

Let  $\mathbb{N} = \{0, 1, 2, \dots\}$ . For  $n \in \mathbb{N}$ , let  $[n] = \{1, \dots, n\}$ . For  $x, x' \in \{-1, 1\}^n$ , let  $x \odot x'$  denote the vector obtained by coordinate-wise multiplication of  $x$  and  $x'$ . For  $i \in [n]$ , let  $e_i$  denote the vector in which all entries are equal to  $+1$  except in the  $i$ th position, where the entry is  $-1$ . For  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ , a variable  $x_i$  is said to be *relevant to  $f$*  (and  $f$  *depends* on  $x_i$ ) if there is an  $x \in \{-1, 1\}^n$  such that  $f(x \odot e_i) \neq f(x)$ . For  $i \in [n]$  and  $a \in \{-1, 1\}$ , denote by  $f_{x_i=a} : \{-1, 1\}^n \rightarrow \{-1, 1\}$  the sub-function of  $f$  obtained by letting  $f_{x_i=a}(x) = f(x')$  with  $x'_j = x_j$  if  $j \neq i$  and  $x'_i = a$ . Thus,  $x_i$  is relevant to  $f$  if and only if  $f_{x_i=1} \neq f_{x_i=-1}$ . The restriction of a vector  $x \in \{-1, 1\}^n$  to a subset of coordinates  $J \subseteq [n]$  is denoted by  $x|_J \in \{-1, 1\}^{|J|}$ . All probabilities and expectations in this paper are taken with respect to the uniform distribution (except when indicated differently).

For  $f, g : \{-1, 1\}^n \rightarrow \mathbb{R}$ , define the inner product

$$\langle f, g \rangle = \mathbb{E}_x[f(x)g(x)] = 2^{-n} \sum_{x \in \{-1, 1\}^n} f(x)g(x).$$

It is well-known that the functions  $\chi_S : \{-1, 1\}^n \rightarrow \{-1, 1\}$ ,  $S \subseteq [n]$ , defined by  $\chi_S(x) = \prod_{i \in S} x_i$  form an orthonormal basis of the space of real-valued functions on  $\{-1, 1\}^n$ . Thus, every function  $f : \{-1, 1\}^n \rightarrow \mathbb{R}$  has the unique *Fourier expansion*

$$f = \sum_{S \subseteq [n]} \hat{f}(S) \chi_S$$

where  $\hat{f}(S) = \langle f, \chi_S \rangle$  are the *Fourier coefficients* of  $f$ . Let  $\|f\|_2 = \langle f, f \rangle^{1/2} = \mathbb{E}[f(x)^2]^{1/2}$ . Plancherel's equation states that

$$\langle f, g \rangle = \sum_{S \subseteq [n]} \hat{f}(S) \hat{g}(S), \tag{1}$$

and from this, Parseval's equation  $\|f\|_2^2 = \sum_{S \subseteq [n]} \hat{f}(S)^2$  follows as the special case  $f = g$ .

For  $f, g : \{-1, 1\}^n \rightarrow \{-1, 1\}$ , define the *distance* between  $f$  and  $g$  by

$$\Delta(f, g) = \Pr[f(x) \neq g(x)],$$

and for a class  $\mathcal{C} = \mathcal{C}_n$  of functions from  $\{-1, 1\}^n$  to  $\{-1, 1\}$ , let  $\text{opt}_{\mathcal{C}}(f) = \min_{g \in \mathcal{C}} \Delta(f, g)$  be the distance of  $f$  to a nearest function in  $\mathcal{C}$ . It is easily seen that  $\Delta(f, g) = (1 - \langle f, g \rangle)/2$ . Furthermore, for a *sample*  $\mathcal{S} = (x^i, y^i)_{i=1, \dots, m}$  with  $x^i \in \{-1, 1\}^n$  and  $y^i \in \{-1, 1\}$ , let

$$\Delta(f, \mathcal{S}) = \frac{1}{m} |\{i \in \{1, \dots, m\} \mid f(x^i) \neq y^i\}|$$

be the fraction of examples in  $\mathcal{S}$  for which the labels disagree with the labeling function  $f$ .

### 3 The Random Walk Learning Model

#### 3.1 Learning from Noiseless Examples

Let  $\mathcal{C} = \bigcup_{n \in \mathbb{N}} \mathcal{C}_n$  be a class of functions, where each  $\mathcal{C}_n$  contains functions  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ . In the *random walk learning model*, a learning algorithm has access to the oracle  $\text{RW}(f)$  for some unknown function  $f \in \mathcal{C}_n$ . On the first request,  $\text{RW}(f)$  generates a *point*  $x \in \{-1, 1\}^n$  according to the uniform distribution on  $\{-1, 1\}^n$  and returns the *example*  $(x, f(x))$ , where we refer to  $f(x)$  as the *label* or the *classification* of the example. On subsequent requests, it selects a random coordinate  $i \in [n]$  and returns  $(x \odot e_i, f(x \odot e_i))$ , where  $x$  is the point returned in the last query. The goal of a learning algorithm  $\mathcal{A}$  is, given inputs  $\delta, \epsilon > 0$ , to output a hypothesis  $h : \{-1, 1\}^n \rightarrow \{-1, 1\}$  such that with probability at least  $1 - \delta$  (taken over all possible random walks of the requested length),  $\Pr[h(x) \neq f(x)] \leq \epsilon$ . In this case,  $\mathcal{A}$  is said to *learn*  $f$  with *accuracy*  $\epsilon$  and *confidence*  $1 - \delta$ .

The class  $\mathcal{C}$  is *learnable from random walks* if there is an algorithm  $\mathcal{A}$  that for every  $n$ , every  $f \in \mathcal{C}_n$ , every  $\delta > 0$ , and every  $\epsilon > 0$  learns  $f$  with access to  $\text{RW}(f)$  with accuracy  $\epsilon$  and confidence  $1 - \delta$ . The class  $\mathcal{C}$  is said to be learnable in time equal to the running time of  $\mathcal{A}$ , which is a function of  $n$ ,  $\epsilon$ ,  $\delta$ , and possibly other parameters involved in the parameterization of the class  $\mathcal{C}$ .

If a learning algorithm only outputs hypotheses  $h \in \mathcal{C}_n$ , it is called a *proper learning algorithm*. In this case,  $\mathcal{C}$  is *properly learnable*.

The random walk model is a *passive* learning model in the sense that a learning algorithm has no direct control on which examples it receives (as opposed to the *membership query model* in which the learner is allowed to ask for the labels of specific points  $x$ ). For passive learning models, we may assume without loss of generality that all examples are requested at once.

#### 3.2 Agnostic Learning

In the model of *agnostic learning from random walks*, we make no assumption whatsoever on the nature of the labels. Following the model of Gopalan et al. [9], we assume that there is an *arbitrary* function  $f : \{-1, 1\}^n$  according to which the examples are labeled, i.e., a learner observes pairs  $(x, f(x))$ , with the points coming from a random walk. In other words, the learner has access to  $\text{RW}(f)$ , but now  $f$  is no longer required to belong to  $\mathcal{C}$ . We can think of the labels as originating from a concept  $g \in \mathcal{C}$ , with an  $\text{opt}_{\mathcal{C}}(f)$  fraction of labels flipped by an adversary.

The goal of a learning algorithm is to output a hypothesis  $h$  that performs nearly as well as the best function of  $\mathcal{C}$ . Let  $\text{opt}_{\mathcal{C}}(f) = \min_{g \in \mathcal{C}} \Pr_x[g(x) \neq f(x)]$ , where  $x \in \{-1, 1\}^n$  is drawn according to the uniform distribution. An algorithm *agnostically learns*  $\mathcal{C}$  if, for any  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ , given  $\delta, \epsilon > 0$ , it outputs a hypothesis  $h : \{-1, 1\}^n$  such that with probability at least  $1 - \delta$ ,  $\Pr_x[h(x) \neq f(x)] \leq \text{opt}_{\mathcal{C}}(f) + \epsilon$ . Again, if the algorithm always outputs a hypothesis  $h \in \mathcal{C}$ , then it is called a *proper learning algorithm*, and  $\mathcal{C}$  is said to be *properly agnostically learnable*.

Although all learning algorithms in this paper are proper, we believe that a word is in order concerning the formulation of the learning goal in *improper agnostic learning*. Namely, it could well happen that we can find a hypothesis that satisfies  $\Pr_x[h(x) \neq f(x)] \leq \text{opt}_{\mathcal{C}}(f)$ , but such an  $h$  could be as far as  $2 \text{opt}_{\mathcal{C}}(f)$  from all concepts in  $\mathcal{C}$ , which can definitely not be considered a sensible solution if, say,  $\text{opt}_{\mathcal{C}}(f) \geq 1/4$ . Instead, a hypothesis should rather be required to be  $\epsilon$ -close to *some* function  $g \in \mathcal{C}$  that performs best (or almost best):  $\Pr[h(x) \neq g(x)] \leq \epsilon$  for some  $g \in \mathcal{C}$  with  $\Pr[g(x) \neq f(x)] = \text{opt}_{\mathcal{C}}(f)$  (or for some near-optimal  $g \in \mathcal{C}$  with  $\Pr[g(x) \neq f(x)] \leq \text{opt}_{\mathcal{C}}(f) + \epsilon'$ ). Alternatively, one can require  $h$  to belong to some reasonably chosen *hypothesis class*  $\mathcal{H} \supseteq \mathcal{C}$ , e.g., the hypotheses output by the algorithm in [9] for learning decision trees of size  $t$  are  *$t$ -sparse polynomials*. In fact, that algorithm *properly* agnostically learns the latter class.

## 4 A Concentration Bound for Labeled Random Walks

The following lemma estimates the probability that, after drawing a random walk  $x^0, \dots, x^\ell$ , the points  $x^0$  and  $x^\ell$  are independent. The proof (and a more formal statement) are deferred to the Appendix (see Lemma 4 in Section A).

**Lemma 1.** *Let  $\delta > 0$ ,  $\ell \geq n \ln(n/\delta)$  and  $x^0, \dots, x^\ell$  be a random walk on  $\{-1, 1\}^n$ . Then, with probability at least  $1 - \delta$ ,  $x^0$  and  $x^\ell$  are independent<sup>1</sup> and uniformly distributed.*

**Lemma 2.** *Let  $g : \{-1, 1\}^n \rightarrow [-1, 1]$  and  $\delta, \epsilon > 0$ . Let  $N = \lceil n \ln(n/\delta) \rceil$ ,*

$$m \geq \frac{2N}{\epsilon^2} \ln \left( \frac{2N}{\delta} \right) ,$$

*and  $x^1, \dots, x^m$  be a random walk on  $\{-1, 1\}^n$ . Then, with probability at least  $1 - \delta$ ,*

$$\left| \frac{1}{m} \sum_{i=1}^m g(x^i) - \mathbb{E}_x[g(x)] \right| \leq \epsilon ,$$

*where the expectation is taken over a uniformly distributed  $x$ .*

Although a similar result can be obtained from the more general works on concentration bounds for random walks by Gillman [8] and for finite Markov Chains by Lézaud [13], we give an elementary proof for Lemma 2 in the Appendix (see Section B).

As an immediate consequence, the fraction of disagreements between the labels  $f(x^i)$  and the values  $h(x^i)$  on a random walk converge quickly to the total fraction of disagreements on all of  $\{-1, 1\}^n$ :

**Corollary 1.** *Let  $\mathcal{C} = \mathcal{C}_n$  be a class of functions from  $\{-1, 1\}^n$  to  $\{-1, 1\}$ . Let  $\epsilon, \delta > 0$ ,  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ , and  $(x^i, f(x^i))_{i=1, \dots, m}$  be a labeled random walk of length*

$$m \geq \frac{2N}{\epsilon^2} \ln \left( \frac{2N|\mathcal{C}|}{\delta} \right) ,$$

*where  $N = \lceil n \ln(n|\mathcal{C}|/\delta) \rceil$ . Then, with probability at least  $1 - \delta$ , for every  $h \in \mathcal{C}$ ,*

$$|\Delta(h, \mathcal{S}) - \Delta(h, f)| \leq \epsilon . \tag{2}$$

*Proof.* Let  $h \in \mathcal{C}$ . Taking  $g(x) = \frac{1}{2}|h(x) - f(x)|$ , we obtain  $\Delta(h, \mathcal{S}) = \frac{1}{m}g(x)$  and  $\Delta(h, f) = \mathbb{E}_x[g(x)]$ , so that by Lemma 2,  $|\Delta(h, \mathcal{S}) - \Delta(h, f)| \leq \epsilon$  with probability at least  $1 - \delta/|\mathcal{C}|$ . Thus, with probability at least  $1 - \delta$ , (2) holds for all  $h \in \mathcal{C}$ .  $\square$

The following proposition shows that, similarly to the classical result by Angluin and Laird [2] for distribution-free PAC-learning and the analogue by Kearns et al. [11] for agnostic PAC-learning, also in the random walk model agnostic learning is achieved by finding a hypothesis that minimizes the number of disagreements with a labeled random walk of sufficient length.

---

<sup>1</sup>More precisely, we can perform an additional experiment such that conditional to some event that occurs with probability at least  $1 - \delta$  (taken over the draw of the random walk and the outcome of the additional experiment),  $x^0$  and  $x^\ell$  are independent. For more details, see Section A in the Appendix.

**Proposition 1.** Let  $\mathcal{C} = \mathcal{C}_n$  be a class of functions from  $\{-1, 1\}^n$  to  $\{-1, 1\}$ . Let  $\epsilon, \delta > 0$ ,  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ , and  $\mathcal{S} = (x^i, f(x^i))_{i=1, \dots, m}$  be a labeled random walk of length  $m \geq (8N/\epsilon^2) \ln(2N|\mathcal{C}|/\delta)$ , where  $N = \lceil n \ln(2n|\mathcal{C}|/\delta) \rceil$ . Let  $h_{\text{opt}} \in \mathcal{C}$  minimize  $\Delta(h, \mathcal{S})$ . Then, with probability at least  $1 - \delta$ ,  $\Delta(h_{\text{opt}}, f) \leq \text{opt}_{\mathcal{C}}(f) + \epsilon$ . In particular, the required sample size is polynomial in  $n$ ,  $\log |\mathcal{C}|$ ,  $1/\epsilon$ , and  $\log(1/\delta)$ .

*Proof.* By Corollary 1,  $|\Delta(h, \mathcal{S}) - \Delta(h, f)| \leq \epsilon/2$  for all  $h \in \mathcal{C}$ . In particular, all functions  $h \in \mathcal{C}$  with  $\Delta(h, f) > \text{opt}_{\mathcal{C}}(f) + \epsilon$  have  $\Delta(h, \mathcal{S}) > \text{opt}_{\mathcal{C}}(f) + \epsilon/2$ , whereas all functions  $h \in \mathcal{C}$  with  $\Delta(h, f) = \text{opt}_{\mathcal{C}}(f)$  have  $\Delta(h, \mathcal{S}) \leq \text{opt}_{\mathcal{C}}(f) + \epsilon/2$ . Consequently,  $\Delta(h_{\text{opt}}, \mathcal{S}) \leq \text{opt}_{\mathcal{C}}(f) + \epsilon/2$ , and thus  $\Delta(h_{\text{opt}}, f) \leq \text{opt}_{\mathcal{C}}(f) + \epsilon$ .  $\square$

## 5 Agnostically Learning Juntas

We start with our main technical lemma that shows that whenever there is a  $k$ -junta  $g$  at distance  $\Delta(f, g)$  to some function  $f$ , then there is another  $k$ -junta  $g'$  (in fact, a subfunction of  $g$ ) at distance  $\Delta(f, g) + \epsilon$  such that the relevant variables of  $g'$  can be detected by finding all low-level Fourier coefficients that are of a certain minimum size.

**Lemma 3.** Let  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$  be an arbitrary function and  $g : \{-1, 1\}^n \rightarrow \{-1, 1\}$  be a  $k$ -junta. Then, for every  $\epsilon > 0$ , there exists a  $k$ -junta  $g'$  such that  $\langle f, g' \rangle \geq \langle f, g \rangle - \epsilon$  and for all relevant variables  $x_i$  of  $g'$ , there exists  $S \subseteq [n]$  with  $|S| \leq k$ ,  $i \in S$ , and

$$|\hat{f}(S)| \geq C \cdot 2^{-(k-1)/2} \cdot \epsilon, \quad (3)$$

where  $C = 1 - 1/\sqrt{2} \approx 0.293$ .

*Proof.* The proof is by induction on  $k$ . For  $k = 0$ , there is nothing to show since there are no relevant variables. For the induction step, let  $k > 0$ . Assume that taking  $g'$  to be  $g$  does not satisfy the conclusion, i.e., for some relevant variable  $x_i$  of  $g$ ,  $|\hat{f}(S)| < C 2^{-(k-1)/2} \epsilon$  for all  $S \subseteq [n]$  with  $|S| \leq k$  and  $i \in S$ . Our goal is to show that in this case, either  $g_{x_i=1}$  or  $g_{x_i=-1}$  is well correlated with  $f$  and thus asserts the existence of an appropriate  $(k-1)$ -junta  $g'$ .

Let  $\mathcal{T} = \{S \subseteq [n] \mid \hat{g}(S) \neq 0\}$ . Then  $|\mathcal{T}| \leq 2^k$ . It follows that

$$\begin{aligned} \langle f, g \rangle &= \sum_{S \in \mathcal{T}} \hat{f}(S) \hat{g}(S) = \sum_{S \in \mathcal{T}: i \in S} \hat{f}(S) \hat{g}(S) + \sum_{S \in \mathcal{T}: i \notin S} \hat{f}(S) \hat{g}(S) \\ &\leq \sum_{S \in \mathcal{T}: i \in S} |\hat{g}(S)| \cdot C \cdot 2^{-(k-1)/2} \cdot \epsilon + \sum_{S \in \mathcal{T}: i \notin S} \hat{f}(S) \hat{g}(S) \\ &\leq 2^{(k-1)/2} \cdot C \cdot 2^{-(k-1)/2} \epsilon + \sum_{S \in \mathcal{T}: i \notin S} \hat{f}(S) \hat{g}(S) = C \cdot \epsilon + \sum_{S \in \mathcal{T}: i \notin S} \hat{f}(S) \hat{g}(S), \end{aligned}$$

where the first equation is Plancherel's equation (1) and the second inequality follows by Cauchy-Schwartz (note that  $\hat{g}(S)$  is supported on at most  $2^{k-1}$  sets  $S$  with  $i \in S$ ). Consequently,

$$\sum_{S \in \mathcal{T}: i \notin S} \hat{f}(S) \hat{g}(S) \geq \langle f, g \rangle - C \cdot \epsilon.$$

Since for  $S \subseteq [n]$ ,

$$(\widehat{g_{x_i=1}}(S) + \widehat{g_{x_i=-1}}(S)) / 2 = \begin{cases} 0 & \text{if } i \in S \\ \hat{g}(S) & \text{if } i \notin S \end{cases},$$

it follows that

$$\langle f, g_{x_i=a} \rangle \geq \langle f, g \rangle - C \cdot \epsilon$$

for  $a = 1$  or for  $a = -1$ . Now  $g_{x_i=a}$  is a  $(k-1)$ -junta, so by induction hypothesis, there exists some  $(k-1)$ -junta  $g'$  such that

$$\langle f, g' \rangle \geq \langle f, g_{x_i=a} \rangle - \epsilon/\sqrt{2} \geq \langle f, g \rangle - C \cdot \epsilon - \epsilon/\sqrt{2} = \langle f, g \rangle - \epsilon$$

and for all  $x_i$  relevant to  $g'$ , there exists  $S \subseteq [n]$  with  $|S| \leq k-1$ ,  $i \in S$ , and

$$|\hat{f}(S)| \geq C \cdot 2^{-(k-2)/2} \cdot \epsilon/\sqrt{2} = C \cdot 2^{-(k-1)/2} \cdot \epsilon.$$

□

One might wonder if for  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$  and a  $k$ -junta  $g : \{-1, 1\}^n \rightarrow \{-1, 1\}$ ,  $\langle f, g \rangle \geq \epsilon$  does not imply that for every relevant variable  $x_i$  of  $g$ , there exists  $S \subseteq [n]$  with  $|S| \leq k$ ,  $i \in S$ , such that (3) holds. First of all, if  $f(x) = x_1 \wedge \dots \wedge x_k$  (interpreting  $-1$  as true and  $+1$  as false), then for all  $S \subseteq [n]$  with  $S \neq \emptyset$ ,  $|\hat{f}(S)| \leq 2^{-k+1}$ . So taking  $g = f$ , the prior statement cannot hold.

Still, one might at least hope for a similar statement with the right-hand side of (3) replaced by something of the form  $2^{-\text{poly}(k)} \cdot \text{poly}(\epsilon)$ . However, if we take  $f$  as above and  $g(x) = x_2 \wedge \dots \wedge x_{k+1}$ , then  $\langle f, g \rangle = 1 - 2^{-k+1}$  but for all  $S \subseteq [n]$  with  $k+1 \in S$ ,  $\hat{f}(S) = 0$  (since  $x_{k+1}$  is not relevant to  $f$ ).

Next, we need a tool for finding large low-degree Fourier coefficients of an arbitrary Boolean function, having access to a labeled random walk. Such an algorithm is said to perform the *Bounded Sieve* (see [6, Definition 3]). Bshouty et al. [6] have shown that such an algorithm exists for the random walk model. More precisely, Theorems 7 and 9 in [6] imply:

**Theorem 2** (Bounded Sieve, [6]). *There is an algorithm  $\text{BoundedSieve}(f, \theta, \ell, \delta)$  that on input  $\theta > 0$ ,  $\ell \in [n]$ , and  $\delta > 0$ , given access to  $\text{RW}(f)$  for some  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$ , outputs a list of  $S \subseteq [n]$  with  $|\hat{f}(S)|^2 \geq \theta/2$  such that with probability at least  $1 - \delta$ , every  $S \subseteq [n]$  with  $|S| \leq \ell$  and  $|\hat{f}(S)|^2 \geq \theta$  appears in it. The algorithm runs in time  $\text{poly}(n, 2^\ell, 1/\theta, \log(1/\delta))$ , and the list contains at most  $2/\theta$  sets  $S$ .*

For a sample  $\mathcal{S} = (x^i, f(x^i))_{i=0, \dots, m}$ , a set  $J \subseteq [n]$  of size  $k$ , and an assignment  $\alpha \in \{-1, 1\}^{|J|}$ , let  $s_\alpha^+ = |\{i \in [m] \mid x^i|_J = \alpha \wedge f(x^i) = +1\}|$  and  $s_\alpha^- = |\{i \in [m] \mid x^i|_J = \alpha \wedge f(x^i) = -1\}|$ . Obviously, a  $J$ -junta  $h_J$  that best agrees with  $f$  on the points in  $\mathcal{S}$  is given by  $h_J(x) = \text{sgn}(s_{x|_J}^+ - s_{x|_J}^-)$ . In other words,  $h(x)$  takes on the value  $a \in \{-1, 1\}$  that is taken on by the majority of labels in the sub-cube that fixes the coordinates in  $J$  to  $\alpha$ . This function is unique except for the choice of  $h_J(x)$  at points  $x$  with  $s_{x|_J}^+ = s_{x|_J}^-$ . The function  $h_J$  differs from the labels of  $\mathcal{S}$  in  $\text{err}(J) = \sum_{\alpha \in \{-1, 1\}^{|J|}} \text{err}(\alpha)$  points, where  $\text{err}(\alpha) = \min\{s_\alpha^+, s_\alpha^-\}$ . By Proposition 1, if  $\mathcal{S}$  is sufficiently large, then with high probability, the function  $h_J$  approximately minimizes  $\Delta(h, f)$  among all  $J$ -juntas  $h$ .

We are now ready to show our main result:

**Theorem 3** (Restatement of Theorem 1). *The class of  $k$ -juntas  $g : \{-1, 1\}^n \rightarrow \{-1, 1\}$  is properly agnostically learnable with accuracy  $\epsilon$  and confidence  $1 - \delta$  in the random walk model in time  $\text{poly}(n, 2^{k^2}, (1/\epsilon)^k, \log(1/\delta))$ .*

*Proof.* In the following, we show that Algorithm 1 below is an agnostic learning algorithm with the desired running time bound.



---

**Algorithm 1** LearnJuntas

---

- 1: **Input**  $k, \epsilon, \delta$
  - 2: **Access to**  $\text{RW}(f)$  for some  $f : \{-1, 1\}^n \rightarrow \{-1, 1\}$
  - 3: Run  $\text{BoundedSieve}(f, (1 - 1/\sqrt{2})^2 \cdot 2^{-k+1} \cdot \epsilon^2, k, \delta/2)$  and let  $\mathcal{T}$  be the returned list.
  - 4: Let  $R = \bigcup \{S \mid S \in \mathcal{T}\}$ .
  - 5: For all  $J \subseteq R$  with  $|J| = k$ :
  - 6:   Compute  $\text{err}(J)$ .
  - 7: **Return**  $h_{J_{\text{opt}}}$  for some  $J_{\text{opt}}$  that minimizes  $\text{err}(J)$ .
- 

Denote the class of  $n$ -variate  $k$ -juntas by  $\mathcal{C}$  and let  $\gamma = \text{opt}_{\mathcal{C}}(f)$ . We prove that, with probability at least  $1 - \delta$ ,

$$\Delta(h_{J_{\text{opt}}}, f) \leq \gamma + \epsilon.$$

Let  $g \in \mathcal{C}$  with  $\Delta(f, g) = \gamma$ , so that  $\langle f, g \rangle = 1 - 2\gamma$ . By Lemma 3, there exists  $g' \in \mathcal{C}$  such that  $\langle f, g' \rangle \geq 1 - 2\gamma - \epsilon$  (equivalently,  $\Delta(f, g') \leq \gamma + \epsilon/2$ ) and for all relevant variables  $x_i$  of  $g'$ , there exists  $S \subseteq [n]$  with  $|S| \leq k$ ,  $i \in S$ , and

$$\hat{f}(S)^2 \geq (1 - 1/\sqrt{2})^2 \cdot 2^{-(k-1)} \cdot \epsilon^2.$$

Consequently, with probability at least  $1 - \delta/2$ , the list  $\mathcal{T}$  returned in Step 3 of the algorithm contains all of these sets  $S$ , and thus  $R$  contains all relevant variables of  $g'$ . The Bounded Sieve subroutine runs in time  $\text{poly}(n, 2^k, 1/\epsilon, \log(1/\delta))$ .

The set  $J_{\text{opt}}$  is chosen such that the corresponding  $J_{\text{opt}}$ -junta  $h_{J_{\text{opt}}}$  minimizes the number of disagreements with the labels among all  $k$ -juntas with relevant variables in  $R$ . Denote the class of these juntas by  $\mathcal{C}(R)$ . Since  $|\mathcal{T}| \leq 2 \cdot (1 - 1/\sqrt{2})^{-2} 2^{k-1} / \epsilon^2 \leq 12 \cdot 2^k / \epsilon^2$ , we have  $|R| \leq k|\mathcal{T}| \leq 12 \cdot k \cdot 2^k / \epsilon^2$ . Consequently,  $R$  contains

$$\binom{|R|}{k} \leq \left( \frac{e|R|}{k} \right)^k \leq \left( \frac{12 \cdot 2^k}{\epsilon^2} \right)^k = \text{poly}(2^{k^2}, (1/\epsilon)^k)$$

subsets of size  $k$ , and  $\log |\mathcal{C}(R)| \leq \log \left( 2^{2^k} \cdot \binom{|R|}{k} \right) = \text{poly}(2^{k^2}, (1/\epsilon)^k)$ .

By Proposition 1, with probability at least  $1 - \delta/2$ ,

$$\Delta(h_{J_{\text{opt}}}, f) \leq \text{opt}_{\mathcal{C}(R)}(f) + \epsilon/2,$$

provided that  $\text{poly}(n, \log |\mathcal{C}(R)|, 1/\epsilon, \log(1/\delta)) = \text{poly}(n, 2^{k^2}, (1/\epsilon)^k, \log(1/\delta))$  examples are drawn. Since  $g' \in \mathcal{C}(R)$ , we obtain

$$\Delta(h_{J_{\text{opt}}}, f) \leq \Delta(g', f) + \epsilon/2 \leq \gamma + \epsilon.$$

The total running time of the algorithm is polynomial in  $n$ ,  $2^{k^2}$ ,  $(1/\epsilon)^k$ , and  $\log(1/\delta)$ . □

## References

- [1] David Aldous and Umesh V. Vazirani. A markovian extension of valiant's learning model. *Inf. Comput.*, 117(2):181–186, 1995.
- [2] Dana Angluin and Philip D. Laird. Learning From Noisy Examples. *Machine Learning*, 2(4):343–370, April 1988.

- [3] Peter L. Bartlett, Paul Fischer, and Klaus-Uwe Höffgen. Exploiting Random Walks for Learning. *Inform. and Comput.*, 176(2):121–135, 2002.
- [4] Avrim Blum and Pat Langley. Selection of Relevant Features and Examples in Machine Learning. *Artificial Intelligence*, 97(1-2):245–271, December 1997.
- [5] Nader H. Bshouty and Vitaly Feldman. On Using Extended Statistical Queries to Avoid Membership Queries. *J. Mach. Learn. Res.*, 2(3):359–396, August 2002.
- [6] Nader H. Bshouty, Elchanan Mossel, Ryan O’Donnell, and Rocco A. Servedio. Learning DNF from random walks. *J. Comput. System Sci.*, 71(3):250–265, October 2005.
- [7] David Gamarnik. Extension of the PAC Framework to Finite and Countable Markov Chains. *IEEE Trans. Inform. Theory*, 49(1):338–345, 2003.
- [8] David Gillman. A Chernoff Bound for Random Walks on Expander Graphs. *SIAM J. Comp.*, 27:12031220, August 1998.
- [9] Parikshit Gopalan, Adam Tauman Kalai, and Adam R. Klivans. Agnostically Learning Decision Trees. In Richard E. Ladner and Cynthia Dwork, editors, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008 (STOC ’08)*, pages 527–536. ACM Press, 2008.
- [10] Wassily Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *J. Amer. Statist. Assoc.*, 58:13–30, 1963.
- [11] Michael J. Kearns, Robert E. Schapire, and Linda Sellie. Toward efficient agnostic learning. *Machine Learning*, 17(2-3):115–141, 1994.
- [12] Eyal Kushilevitz and Yishay Mansour. Learning Decision Trees Using the Fourier Spectrum. *SIAM J. Comp.*, 22(6):1331–1348, December 1993.
- [13] Pascal Lézaud. Chernoff-type Bound for Finite Markov Chains. *Ann. Appl. Probab.*, 8(3):849–867, 1998.
- [14] Elchanan Mossel, Ryan W. O’Donnell, and Rocco A. Servedio. Learning functions of  $k$  relevant variables. *J. Comput. System Sci.*, 69(3):421–434, November 2004.
- [15] Sébastien Roch. On Learning Thresholds of Parities and Unions of Rectangles in Random Walk Models. *Random Structures Algorithms*, 31(4):406–417, 2007.
- [16] Martin Zinkevich. Online convex programming and generalized infinitesimal gradient ascent. In Tom Fawcett and Nina Mishra, editors, *Machine Learning, Proceedings of the Twentieth International Conference (ICML 2003), August 21-24, 2003, Washington, DC, USA*, pages 928–936. AAAI Press, 2003.

## A Independence of Points in Random Walks

An *updating random walk* is a sequence  $x^0, (x^1, i_1), (x^2, i_2), \dots$ , where  $x^0$  is drawn uniformly at random, each  $i_t \in [n]$  is a coordinate drawn uniformly at random, and  $x^t$  is set to  $x^{t-1}$  or to  $x^{t-1} \odot e_{i_t}$ , each with probability  $1/2$ . We say that in step  $t$ , coordinate  $i_t$  is *updated*.

Given an *updating* random walk  $x^0, (x^1, i_1), (x^2, i_2), \dots$ , all variables will with high probability be updated after  $\ell = \Omega(n \log n)$  steps, so that in this case,  $x^0$  and  $x^\ell$  can be considered as independent uniformly distributed random variables. More formally, let  $\mathcal{X}^\ell$  be the set of all updating random walks of length  $\ell$ , and let  $\mathcal{X}_{\text{good}}^\ell$  be the set of updating random walks such that all variables have been updated (at least once) after  $\ell$  steps. Then, conditional to the updating random walk belonging to  $\mathcal{X}_{\text{good}}^\ell$ ,  $x^0$  and  $x^\ell$  are independent (and uniformly distributed).

Since the updating random walk model is only a technical utility, we would like to say similar things about the “usual” random walk model, so that we do not have to take care of going back and forth between the models in our analyses (although that would constitute a reasonable alternative).

We proceed as follows. Given a (non-updating) random walk  $x^0, x^1, \dots$ , we perform an additional experiment to simulate an updating random walk (see also [6]). We then *accept* the (original) random walk if the additional experiment leads to a *good* updating random walk. It will then follow that, conditional to the random walk being accepted,  $x^0$  and  $x^\ell$  are independent. Our algorithms will of course not perform this experiment. Instead, we will reason in the analyses that *if* we performed the additional experiment, *then* we would accept the given random walk with a certain (high) probability (taken over the draw of the random walk *and* the additional experiment), implying that certain points are independent.

Perform the following random experiment: Given a random walk  $X$  of length  $\ell$ , draw a sequence  $F = (F_1, F_2, \dots)$  of Bernoulli trials with  $\Pr[F_j = 1] = \Pr[F_j = 0] = 1/2$  for each  $j$  until  $F$  contains  $\ell$  ones. (If this is not the case after, say,  $L = \text{poly}(\ell)$  steps, then reject  $X$ .) Otherwise, let  $\ell'$  denote the length of  $F$  and construct a sequence  $I = (i_1, \dots, i_{\ell'})$  of variable indices as follows. Denote by  $j_1 < \dots < j_\ell$  the  $\ell$  positions in  $F$  with  $F_i = 1$ . For each  $k \in [\ell]$ , let  $i_{j_k} = p_k$ , where  $p_k$  is the position in  $X$  that is flipped in the  $k$ th step. For each  $j \in [\ell'] \setminus \{j_1, \dots, j_\ell\}$ , independently draw an index  $i_j \in [n]$  with uniform probability. Accept  $X$  if  $\{i_1, \dots, i_{\ell'}\} = [n]$ , otherwise reject  $X$ .

**Lemma 4** (Formal restatement of Lemma 1). *Let  $X = (x^0, \dots, x^\ell)$  be a random walk of length  $\ell \geq n \ln(2n/\delta)$  and perform the experiment above. Then  $X$  is accepted with probability at least  $1 - \delta$ . Moreover, conditional to  $X$  being accepted, the random variables  $x^0$  and  $x^\ell$  are independent and uniformly distributed.*

*Proof.* First, by choosing  $L$  appropriately, we can ensure with probability at least  $1 - \delta/2$  that  $F$  contains at least  $\ell$  ones. By construction, the sequence  $x'^0, (x'^1, i_1), (x'^2, i_2), \dots, (x'^{\ell'}, i_{\ell'})$  with  $x'^0 = x^0$ ,  $x'^{j_k} = x_k$  for  $k \in [\ell]$ , and  $x'^j = x'^{j-1}$  for  $j \in [\ell'] \setminus \{j_1, \dots, j_\ell\}$  is distributed as an updating random walk of length  $\ell'$ . Note that unlike in the original updating random walk model, we determine the sequence  $F$  of updating outcomes *before* we determine the positions to be updated. Moreover, the choice of the coordinates to be updated in the positions where  $F_i = 1$  is incorporated in the draw of the original walk. The subsequence  $x'^0, x'^{j_1}, x'^{j_2}, \dots, x'^{j_\ell}$  is equal to the original walk  $x^0, x^1, x^2, \dots, x^\ell$ .

The probability that  $\{i_1, \dots, i_{\ell'}\} \subsetneq [n]$  is at most

$$n \cdot (1 - 1/n)^{\ell'} \leq n \cdot (1 - 1/n)^\ell \leq \delta/2$$

since  $\ell \geq n \ln(2n/\delta)$ . Consequently, with total probability at least  $1 - \delta$ , the random walk is accepted. In this case, every coordinate has eventually been updated after the  $\ell'$  steps of the updating random walk. Thus, for each coordinate  $j$ , of  $x_j^\ell = x_j^{\ell'}$  is independent of  $x_j^0 = x_j'^0$ , i.e.,  $x^0$  and  $x^\ell$  are independent and uniformly distributed (conditional to  $X$  being accepted).  $\square$

## B An Elementary Proof of Lemma 2

To estimate the convergence rate of empirical averages to their expectations, we need the following standard Chernoff-Hoeffding bound [10]: For a sequence of independent identically distributed random variables  $X_1, \dots, X_m$  with  $E[X_i] = \mu$  that take values in  $[-1, 1]$ ,

$$\Pr \left[ \left| \frac{1}{m} \sum_{i=1}^m X_i - \mu \right| \right] \leq 2e^{-\epsilon^2 m/2} . \quad (4)$$

*Proof of Lemma 2.* For each  $j \in \{0, \dots, N-1\}$ , the points  $x^{iN+j}$ ,  $i \in \{0, \dots, m/N-1\}$ , are with probability at least  $1 - (m/N-1)\delta$  pairwise independent by Lemma 1. In this case, the values  $f(x^{iN+j})$ ,  $0 \leq i \leq m/N-1$ , are independent and identically distributed samples of the random variable  $f(x)$  with  $x \in \{-1, 1\}^n$  uniformly distributed. By the Hoeffding bound,

$$\Pr \left[ \left| \frac{N}{m} \sum_{i=0}^{m/N-1} f(x^{iN+j}) - E_x[f(x)] \right| > \epsilon \right] \leq 2 \exp(-m\epsilon^2/(2N))$$

Thus, the probability that  $\left| (N/m) \sum_{i=0}^{m/N-1} f(x^{iN+j}) - E_x[f(x)] \right| > \epsilon$  for *some*  $j \in \{0, \dots, N-1\}$  is at most  $2N \exp(-m\epsilon^2/(2N))$ . Finally, we have

$$\begin{aligned} \left| \frac{1}{m} \sum_{i=0}^m f(x^i) - E_x[f(x)] \right| &= \frac{1}{m} \left| \sum_{j=0}^N \left( \sum_{i=0}^{m/N-1} f(x^{iN+j}) - \frac{m}{N} E_x[f(x)] \right) \right| \\ &\leq \frac{1}{m} \sum_{j=1}^N \frac{m}{N} \epsilon = \epsilon \end{aligned}$$

with probability at least  $1 - 2N \exp(-m\epsilon^2/(2N)) \geq 1 - \delta$ . □