Supplementary Information

Zachary Kokot

July 25, 2024

Contents

1 Proof any Density Matrix can be Expressed as a Linear Combination of Pauli Matrices

2 Proof of the Sample Complexity for the Random Local Pauli Measurement Primitive

2.1 Motivation

Part of what makes shadow tomography appealing is that it requires a smaller number of measurements to predict an observable within the same error when compared to full state tomography. In this section, we will prove that the random local Pauli measurement primitive requires a number of measurements that scales logarithmically with the number of target observables and exponentially in the locality of the observables. This is a significant improvement over full tomography, which requires a number of measurements that scales exponentially with the number of qubits.

2.2 Theorem

Fix a collection of M observables, maximum error ϵ, and failure probability δ. Set

$$K = 2\log\left(\frac{2M}{\delta}\right) \quad \text{and} \quad N \le \frac{34}{\epsilon^2} \max_{1 \le i \le M} 4^{L_i} ||O_i||_\infty^2,$$

Where L_i is the locality of the i-th observable, $||O||_\infty$ denotes the matrix norm. Then, a collection of NK independent classical shadows allow for the prediction of M observables via median of means prediction such that

$$|\hat{o}_i(N, K) - \text{tr}(O_i\rho)| \le \epsilon \quad \text{for all} \quad 1 \le i \le M$$

with probability at least $1 - \delta$.

2.3 Proof

To estimate the expectation value of M observables by median of means estimation with maximum error ϵ and success probability $1 - \delta$ we turn to the results of [1]. In which they state the following theorem:

> **Theorem 1**
>
> *Let X be a random variable with variance σ^2. Then, K independent sample means of size $N = 34\frac{\sigma^2}{\epsilon^2}$ suffice to construct a median of means estimator $\hat{\mu}(N, K)$ that obeys*
>
> $$\mathbb{P}[|\hat{\mu}(N, K) - \mathbb{E}[X]| \ge \epsilon] \le 2e^{-K/2}. \tag{1}$$

They also give the following lemma:

> ### Lemma 1
>
> *Fix an observable O and set $\hat{o} = tr(O\hat{\rho})$, where $\hat{\rho}$ is a classical shadow. Then*
>
> $$Var[\hat{o}] = \mathbb{E}\left[(\hat{o} - \mathbb{E}[\hat{o}^2])\right] \leq \left|\left|O - \frac{tr(O)}{2^n}\mathbb{I}\right|\right|_{shadow}^2. \tag{2}$$

From the above theorem and lemma, we can conclude that to estimate a single observable the size of each estimator is given by

$$N \leq \frac{34}{\epsilon^2}\left|\left|O - \frac{\text{tr}(O)}{2^n}\mathbb{I}\right|\right|_{shadow}^2. \tag{3}$$

To estimate M observables, we need to take the maximum of the above expression over all observables. This will ensure that for all observables the maximum error is less than ϵ. Thus, the size of each estimator to estimate M observables is given by

$$N \leq \frac{34}{\epsilon^2}\max_{1\leq i\leq M}\left|\left|O_i - \frac{\text{tr}(O_i)}{2^n}\mathbb{I}\right|\right|_{shadow}^2. \tag{4}$$

Finally, for the arbitrary Pauli basis measurement primitive we have that the shadow norm has the following property

$$\left|\left|O - \frac{\text{tr}(O)}{2^n}\mathbb{I}\right|\right|_{shadow}^2 \leq 4^{L(O)}||O||_\infty^2, \tag{5}$$

Where $L(O)$ is the locality of the observable and $||O||_\infty$ denotes the matrix norm. This implies that the size of each estimator to estimate M observables is given by

$$N \leq \frac{34}{\epsilon^2}\max_{1\leq i\leq M}4^{L_i}||O_i||_\infty^2. \tag{6}$$

From the above theorem, we have that for a single random variable the probability the error bound is violated is given by

$$\mathbb{P}[|\hat{\mu}(N,K) - \mathbb{E}[X]| \geq \epsilon] \leq 2e^{-K/2}. \tag{7}$$

We would like to ensure that the probability that the error bound is for any of the M observables is less than δ. To determine an expression for K which satisfies this requirement we can use Booles inequality. Booles inequality states that for any countable set of events $A_1, A_2, \ldots, A_n$ we have

$$\mathbb{P}\left[\bigcup_{i=1}^n A_i\right] \leq \sum_{i=1}^n \mathbb{P}[A_i]. \tag{8}$$

In English this means that the probability any event in the set occurs is no greater than the sum of the probabilities of the individual events. Assume the estimation of each observable has a probability of violating the error bound of δ_0. Then, by Booles inequality, the probability that the error bound is violated for any of the M observables is less than

$$\sum_{i=1}^{M} \mathbb{P}[A_i] = \sum_{i=1}^{M} \delta_0 = M\delta_0 = \delta.$$

Thus, we have that

$$2e^{-K/2} \leq \frac{\delta}{M}.$$

Rearranging the above expression we find that

$$K \geq 2\log\left(\frac{2M}{\delta}\right).$$

3 Proof of the Computational Complexity for the Estimation of Pauli Observables from shadows generated by the Random Local Pauli Measurement Primitive

3.1 Motivation

The computational complexity of the estimation of Pauli observables from shadows generated by the random local Pauli measurement primitive is an important consideration when determining the feasibility of the primitive. In this section, we will prove that the computational complexity of the estimation of Pauli observables from shadows generated by the random local Pauli measurement primitive scales linearly with the number of qubits, the number of target observables, the size of the shadow.

3.2 Theorem

3.3 Proof

References

[1] Hsin-Yuan Huang, Richard Kueng, and John Preskill. "Predicting many properties of a quantum system from very few measurements". en. In: *Nature Physics* 16.10 (2020), pp. 1050–1057. DOI: 10.1038/s41567-020-0932-7. URL: https://www.nature.com/articles/s41567-020-0932-7.