Resource-efficient algorithm for estimating the trace of quantum state powers $\mathrm{Tr}(\rho^k)$

Myeongjin Shin*, **Junseo Lee***, Seungwoo Lee, and Kabgyun Jeong

harris.junseo@gmail.com | arXiv:2408.00314

Summary

- Estimating the trace of quantum state powers, $\mathrm{Tr}(\rho^k)$, for k identical quantum states is a fundamental task with numerous applications in quantum information processing.
- Inspired by the Newton-Girard method, we significantly improve upon existing results by introducing an algorithm that requires only $\mathcal{O}(\widetilde{r})$ qubits and $\mathcal{O}(\widetilde{r})$ multi-qubit gates, where $\widetilde{r} = \min\{\mathrm{rank}(\rho), \lfloor \ln(2k/\epsilon) \rfloor\}$.

[Algorithm 1] Estimation of $\mathrm{Tr}(\rho^k)$

1. Estimate the values of $\mathrm{Tr}(\rho^\ell)$ for $\ell = 1, 2, \ldots, t$ using the method proposed in [Quek *et al.*, *Quantum*, 2024], and denote them as $Q_{\ell(\le t)}$. The estimation is $\epsilon(2kt\ln t)^{-1}$-additive.
2. Calculate the elementary symmetric polynomial b_k $(1 \le k \le t)$ defined as:

$$b_k = \frac{1}{k}\sum_{\ell=1}^{k}(-1)^{\ell-1} b_{k-\ell} Q_\ell, \ b_0 = 1. \qquad (1)$$

3. The value of $\mathrm{Tr}(\rho^\ell)$ can be ϵ-additively estimated for $\ell > t$ using the following recurrence relation:

$$Q_{\ell(>t)} = \sum_{k=1}^{t}(-1)^{k-1} b_k Q_{\ell-k}. \qquad (2)$$

[Algorithm 2] Estimation of $\mathrm{Tr}(M\rho^k)$

1. Following Steps 1 and 2 of **[Algorithm 1]**, with Step 1 providing an $\epsilon(2\|M\|_\infty kt\ln t)^{-1}$-additive estimate, we obtain $b_1, \ldots, b_t$.
2. $(\epsilon/4)$-additively estimate the values of $\mathrm{Tr}(M\rho^\ell)$ for $\ell = 1, 2, \ldots, t$ using the method proposed in [Liang *et al.*, *PRA*, 2023], and denote these values as $Q_{\ell(\le t),M}$.
3. The value of $\mathrm{Tr}(M\rho^\ell)$ can be ϵ-additively estimated for $\ell > t$ using the following recurrence relation:

$$Q_{\ell(>t),M} = \sum_{k=1}^{t}(-1)^{k-1} b_k Q_{\ell-k,M}. \qquad (3)$$

Theorem 3.3. Suppose that

$$\varepsilon_{i,M} = |\epsilon_{i,M}| = |P_{i,M} - Q_{i,M}| < \epsilon/4, \text{ and} \qquad (4)$$

$$\varepsilon_i = |\epsilon_i| = |P_i - Q_i| < \epsilon(2\|M\|_\infty kt\ln t)^{-1}, \qquad (5)$$

holds for $i = 1, 2, \ldots, t$, where the operator norm $\|M\|_\infty$ is defined corresponding to the ∞-norm for vectors $\|x\|$, as $\|M\|_\infty = \sup_{x\neq 0}\frac{\|Mx\|_\infty}{\|x\|_\infty}$. Setting $t = \widetilde{r}_M$ and proceeding with **[Algorithm 2]** based on the recurrence relation (3), the following relation always holds:

$$|\epsilon_{i,M}| = |P_{i,M} - Q_{i,M}| \le \epsilon \qquad (6)$$

for $i = 1, 2, \ldots, k$. Where $\widetilde{r}_M$ is the effective rank for the observable M defined as:

$$\widetilde{r}_M = \min\left\{r, \left\lfloor \ln\left(2k\|M\|_\infty/\epsilon\right)\right\rfloor\right\}. \qquad (7)$$

Notations: a_k and b_k represent the elementary symmetric polynomials corresponding to $P_i = \mathrm{Tr}(\rho^i)$ and $Q_i = \widetilde{\mathrm{Tr}(\rho^i)}$, respectively. Additionally, $P_{i,M} = \mathrm{Tr}(M\rho^i)$ and $Q_{i,M} = \widetilde{\mathrm{Tr}(M\rho^i)}$.

Resource requirements for estimating $\{\mathrm{Tr}(\rho^i)\}_{i=1}^k$

Method	# Depth	# Qubits	# CSWAP	# Copies	Original $\|\psi\rangle$
Generalized swap test	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k^2/\epsilon^2)$	**NOT** required
Hadamard test	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k^2/\epsilon^2)$	Required
Two-copy test	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k^2/\epsilon^2)$	Required
Two-copy test & Qubit-reset	$\mathcal{O}(k)$	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(k^2/\epsilon^2)$	Required
Multivarite trace estimation	$\mathcal{O}(1)$	$\mathcal{O}(k)$	$\mathcal{O}(k)$	$\mathcal{O}(k^2/\epsilon^2)$	**NOT** required
Ours (this work)	$\mathcal{O}(1)$	$\mathcal{O}(\widetilde{r})$	$\mathcal{O}(\widetilde{r})$	$\widetilde{\mathcal{O}}(k^2/\epsilon^2)$	**NOT required**

Effective rank for ϵ-additive estimations

Quantity	Quantum Resource Needed	Lower bound on t (in [Algorithm 1 & 2])
$\mathrm{Tr}(\rho^k)$	$\{\mathrm{Tr}(\rho^i)\}_{i=1}^t$	$\min\{\mathrm{rank}(\rho), \lfloor \ln(2k/\epsilon)\rfloor\}$
$\mathrm{Tr}(M\rho^k)$	$\{\mathrm{Tr}(\rho^i),\ \mathrm{Tr}(M\rho^i)\}_{i=1}^t$	$\min\{\mathrm{rank}(\rho), \lfloor \ln(2k\|M\|_\infty/\epsilon)\rfloor\}$
$\mathrm{Tr}(\rho^k\sigma^\ell)$	$\{\mathrm{Tr}(\rho^i),\ \mathrm{Tr}(\sigma^i)\}_{i=1}^t, \{\mathrm{Tr}(\rho^i\sigma^j)\}_{(i,j)=(1,1)}^{(t,t)}$	$\min\{\max\{\mathrm{rank}(\rho), \mathrm{rank}(\sigma)\}, \lfloor \ln((4k+4\ell)/\epsilon)\rfloor\}$

Rank is all you need

Lemma 3.1. Let $d_k = b_k - a_k$, then the following holds:

$$|d_k| \le \sum_{j=1}^{k}\frac{|\epsilon_j|}{j}. \qquad (8)$$

Theorem 3.1. Suppose that,

$$\varepsilon_i = |\epsilon_i| = |Q_i - P_i| < \epsilon(kt\ln t)^{-1} \qquad (9)$$

holds for $i = 1, 2, \ldots, t$. Setting $t = r$ and proceeding with **[Algorithm 1]** based on the recurrence relation (2), the following relation always holds:

$$|\epsilon_i| = |Q_i - P_i| < \epsilon \qquad (10)$$

for $i = 1, 2, \ldots, k$.

Corollary 3.1. To estimate $\mathrm{Tr}(\rho^i)$ for all $i \le k$ within an additive error of ϵ and with a success probability of at least $1-\delta$, where $\delta \in (0,1)$, it suffices to estimate each $\mathrm{Tr}(\rho^j)$ for $j \le r$ within an additive error of ε_j, as defined in Theorem 3.1. This can be achieved by using

$$\mathcal{O}\left(\frac{k^2r^2\ln^2 r\ln(1/\delta)}{\epsilon^2}\right) \qquad (11)$$

runs on a constant-depth quantum circuit consisting of $\mathcal{O}(j)$ qubits and $\mathcal{O}(j)$ CSWAP operations.

Application: Entanglement detection

- Separable quantum state ρ_{AB} always has a positive semi-definite (PSD) partial transpose (PT), denoted as $\rho_{AB}^{\Gamma_B}$.
- The k-th PT moment: $p_k^{\mathrm{PT}} = \mathrm{Tr}\left[\left(\rho^\Gamma\right)^k\right]$.

Lemma 5.1. A quantum state ρ is entangled if $e_i(\lambda_1, \ldots, \lambda_r) < 0$ for some $i = 1, 2, \ldots, r$, where p_i^{PT} are the PT moments of ρ^Γ, and $e_i(x_1, \ldots, x_m)$ denotes the elementary symmetric polynomial in m variables, which satisfies the recursive formula

$$e_k = \frac{1}{k}\sum_{i=1}^{k}(-1)^{i-1} e_{k-i} p_i^{\mathrm{PT}}. \qquad (12)$$

- Computing $\{p_i^{\mathrm{PT}}\}_{i=1}^t$, $t = \mathcal{O}(\ln(r/\epsilon))$ is sufficient to estimate higher-order PT moments.
- Using these PT moments and the recursive formula (12), we can detect entanglement.

Effective rank is all you need

Lemma 3.2. Suppose that $\widetilde{P}_i$ is defined as

$$\widetilde{P}_{i(\le t)} = \mathrm{Tr}(\rho^i) = \sum_{j=1}^{r} p_j^i, \qquad (13)$$

$$\widetilde{P}_{i(>t)} = \sum_{k=1}^{t}(-1)^{k-1} a_k \widetilde{P}_{i-k}. \qquad (14)$$

Then the following holds:

$$\left|\widetilde{P}_k - P_k\right| \le \frac{k}{t!}\left(1 - \frac{t}{r}\right). \qquad (15)$$

Theorem 3.2. Suppose that,

$$\varepsilon_i = |\epsilon_i| = |Q_i - P_i| < \epsilon(2kt\ln t)^{-1} \qquad (16)$$

holds for $i = 1, 2, \ldots, t$. Setting $t = \lfloor \ln(2k/\epsilon)\rfloor$ and proceeding with **[Algorithm 1]** based on the recurrence relation (2), the following relation always holds:

$$|\epsilon_i| = |Q_i - P_i| < \epsilon \qquad (17)$$

for $i = 1, 2, \ldots, k$.

Corollary 3.2. To estimate $\mathrm{Tr}(\rho^i)$ for all $i \le k$ within an additive error of ϵ and with a success probability of at least $1-\delta$, where $\delta \in (0,1)$, it suffices to estimate each $\mathrm{Tr}(\rho^j)$ for $j \le \lfloor \ln(2k/\epsilon)\rfloor$ within an additive error of ε_j, as defined in Theorem 3.2. This can be achieved by using

$$\widetilde{\mathcal{O}}\left(\frac{k^2\ln(1/\delta)}{\epsilon^2}\right) \qquad (18)$$

runs on a constant-depth quantum circuit consisting of $\mathcal{O}(j)$ qubits and $\mathcal{O}(j)$ CSWAP operations. Where $\widetilde{\mathcal{O}}(\cdot)$ ignores the logarithmic terms.

Open problems

- Tighter upper bound on $\left|\widetilde{P}_k - P_k\right|$ and t:
  - Conjecture: $t = \mathcal{O}\left(\frac{\ln(k/\epsilon)}{\ln\ln(k/\epsilon)}\right)$.
- Upper bounds for restricted settings:
  - Incoherent measurements
  - Bounded quantum memory
- γ-multiplicative error dependence
- Impact on virtual distillation
- Finding more rank-dependent algorithms