How many copies are needed for state discrimination?

Aram W. Harrow\textsuperscript{1} and Andreas Winter\textsuperscript{2}

\textsuperscript{1}Department of Computer Science, University of Bristol, Bristol BS8 1UB, U. K.
\textsuperscript{2}Department of Mathematics, University of Bristol, Bristol BS8 1TW, U. K.

The problem we are considering is motivated by the hidden subgroup problem, for which the “standard approach” is to use the oracle to produce the coset state

\[ \rho_H = \frac{1}{\sqrt{|H|}} \sum_{g \in H} |gH\rangle \langle gH|, \]

with \(|gH\rangle = |gh\rangle\) for all \(h \in H\). Determining \(H < G\) then amounts to distinguishing the \(\rho_H\), given a small number of samples (disregarding complexity issues).

Abstractly, one is given a set of quantum states \(\{\rho_i : i = 1, \ldots, N\}\) on a \(d\)-dimensional Hilbert space \(\mathcal{H}\), with the property that the pairwise fidelities are bounded away from 1:

\[ \forall i \neq j \quad F(\rho_i, \rho_j) \geq \left| \sqrt{\rho_i} - \sqrt{\rho_j} \right|^2 \leq F < 1. \]

The question is: how many copies of the unknown state \(\rho_i\) does one need to be able to distinguish them all with high reliability? In other words, we would like to find, for \(0 < \epsilon < 1\), the minimal \(n\) for which there exists a POVM \((M_j)_{j=1,\ldots,N}\) on \(\mathcal{H}^{\otimes n}\) such that for all \(i\),

\[ \text{Tr}(\rho_i^{\otimes n} M_j) \geq 1 - \epsilon. \]

Of course, this minimal \(n\) will depend on the precise geometric position of the states relative to each other, but useful bounds can be obtained simply in terms of the number \(N\) and the fidelity \(F\).

Upper bound. We invoke a result of Barnum and Knill\textsuperscript{[1]} which says that, assuming a probability distribution \((\rho_i)\) on the state set, the average success probability is lower bounded as

\[ P_{\text{succ}} := \sum_i p_i \text{Tr}(\rho_i^{\otimes n} M_i) \geq 1 - \sum_{i \neq j} \sqrt{p_i p_j} \sqrt{F(\rho_i^{\otimes n}, \rho_j^{\otimes n})} \geq 1 - N \sqrt{F^2}, \]

which is \(\geq 1 - \epsilon\) if

\[ n \geq \frac{2}{-\log F} (\log N - \log \epsilon). \quad (1) \]

In fact, this success probability is achieved by the “square root” or “pretty good” measurement\textsuperscript{[2]}, which, according to\textsuperscript{[1]}, has error probability not more than twice that of the optimal measurement. So, for every distribution there exists a POVM attaining success probability \(\geq 1 - \epsilon\). Conversely, for fixed POVM one can try to find the worst probability distribution – which may be the point mass on the state with minimal \(\text{Tr}(\rho_i^{\otimes n} M_i)\). But looking at the payoff function of this game, the success probability, we see that it is bilinear in the strategies of the players, the probability vector \((p_i)\) and the POVM \((M_i)\), and that furthermore the strategy spaces of both players are convex. Hence, we can use the min-max theorem\textsuperscript{[3]}:

\[ \max_{\{M_i\}} \min_{\{p_i\}} P_{\text{succ}} = \min_{\{p_i\}} \max_{\{M_i\}} P_{\text{succ}} \geq 1 - \epsilon, \]

so there exists a POVM \(M_i\) such that for all \(i\),

\[ \text{Tr}(\rho_i^{\otimes n} M_i) \geq 1 - \epsilon. \]

Lower bound. We quote from\textsuperscript{[2]}, the following lower bound (Theorem 1.4): to distinguish the states \(\rho_i\) with success probability \(\geq \eta\),

\[ n \geq \frac{1}{\log(\lambda d)} (\log N + \log \eta) \quad (2) \]

copies are necessary, where \(\lambda := \max_i \|\rho_i\|\) is the largest eigenvalue among the operators \(\rho_i\).

Applications and discussion. For constant \(\eta\) and \(\epsilon\), the upper and lower bounds of eqs.\textsuperscript{[1]} and\textsuperscript{[2]} are comparable, provided \(\lambda = O(1/d)\), which holds for many important examples of the hidden subgroup problem. Our upper bound can be viewed as a generalisation and improvement of the results in\textsuperscript{[2]} (Theorem 1.6), which themselves improve on\textsuperscript{[3]}, to the effect that \(n = O(\log N)\) copies of a coset state are sufficient to distinguish from among \(N\) subgroups (c.f.\textsuperscript{[7]} which has \(n = O(\log |G|)\) when specialising to the hidden subgroup problem).

Here, we get rid of assumptions on the group’s structure (and indeed groups at all), as well as a dimensional term in\textsuperscript{[3]}. Observe that by using the game theoretic trick (c.f.\textsuperscript{[4]}) we obtain a measurement with worst case error \(\epsilon\), unlike previous approaches including\textsuperscript{[2]}.

Acknowledgments. The authors thank Pranab Sen for providing the motivation for this work. They acknowledge the hospitality of the Institut Henri Poincare, Paris, where the present work was done. Funding: U.K. EPSRC (QIP IRC) and EU (QAP).

References

[1] H. N. Barnum and E. Knill. J. Math. Phys. 43(5), 2097 (2002).
[2] M. Hayashi, A. Kawachi and H. Kobayashi. arXiv.org:quant-ph/0604174 (2006).
[3] A. S. Holevo. Theor. Prob. Appl. 23, 411 (1978).
[4] D. Kretschmann, D. Schlingemann and R. F. Werner. arXiv.org:quant-ph/0605009 (2006).
[5] O. Morgenstern and J. von Neumann. Theory of Games and Economic Behavior, Princeton, 1944.
[6] P. Sen. Proc. 21st IEEE CCC (2006).
[7] M. Ettinger, P. Høyer and E. Knill. arXiv.org:quant-ph/9901034 (1999).