University of Waterloo

Faculty of Mathematics

Quantum Communication Complexity and Raz's Problem

Institute for Quantum Computing

University of Waterloo

Waterloo, Ontario

James Hawley

20423520

3A Mathematical Physics

August 27, 2014

Memorandum

To: Joseph Emerson

From: James Hawley

Date: August 27, 2014

Re: Work Report: Quantum Communication Complexity and Raz's Problem

---

I have prepared the enclosed report, "Quantum Communication Complexity and Raz's Problem", for my 3A work report and for your research group at the Institute for Quantum Computing. This report, the third of four work reports that the Co-operative Education Program requires that I successfully complete as part of my BMath Co-op degree requirements, has not received academic credit and was written entirely by myself.

The research group you lead explores open questions in quantum foundations and quantum information science. My position as an Undergraduate Student Research Assistant required that I research topics in classical and quantum information processing, understand and expand upon recent publications, and present my work to the rest of the group and other colleagues. This report is a study of Raz's problem and summarizes my work from this term.

The Faculty of Mathematics requests that you evaluate this report for command of topic and technical content/analysis. Following your assessment, the report, together with your evaluation, will be submitted to the Math Undergrad Office for evaluation on campus by work report markers. The combined marks determine whether the report will receive credit and whether it will be considered for an award.

I'd like to thank you, Richard Cleve, Mark Howard, and Joel Wallman for the helpful conversations throughout the term, as well as National Science and Energy Research Council for providing funding for this research.

James Hawley

Table of Contents

List of Figures

List of Tables

Executive Summary

This report analyzes a family of classical protocols that solves Raz's problem, a problem in the communication complexity framework of distributed computing. These solutions are adaptations of the algorithm developed by Pashayan et al. (2014), which is inspired by the stabilizer sub-theory of quantum computing and relies on the discrete Wigner function formalism.

The protocols' probabilistic convergence to the answer, their communication complexities, and how each protocol behaves in special cases of input variables are discussed. The family of protocols behaves in the following way: $O(\log\, d)$ communication complexity when stabilizer states and Clifford gates are guaranteed, $O(d \log d)$ when only the quantum gates are Clifford, $O(d^2\, \log\, d)$ when the input vector is a stabilizer state, and $O(d^3\, \log\, d)$ when there are no specifications on the input vector or gates. The protocols perform as well as the quantum algorithm presented by Buhrman et al. (2009) in the stabilizer sub-theory, but perform poorly in general.

Areas for improvement in performance include specifying better bounds on the mana of states and unitary matrices to give a tighter bound on required repetitions, determining bounds on the mana of unitary matrices in the extended Clifford hierarchy, and considering a protocol that uses the nearest neighbour in the stabilizer framework.

1.0 Introduction

Quantum computing has made great strides in recent years, and is emerging as a popular field for mathematicians, physicists, computer scientists, and electrical engineers. From a theoretical standpoint, developing algorithms that take advantage of quantum phenomena and characterizing the differences between quantum and classical computational algorithms is necessary to determine precisely what resources are needed for quantum computers to be more effective than current computers. The quantum bit (qubit) is a basis for much of the theoretical framework of quantum computing, and its two-state design is analogous to the 0-1 framework of classical computers. Working in dimensions higher than two (qubits are renamed qudits to emphasize the d-dimensional systems) can yield some results that are more intuitive than results found in two dimensions.

One area of study in quantum computing is communication complexity, and how entangled particles can help physically separated parties perform calculations. Given a problem, the communication complexity is the minimum amount of information exchanged between the two parties needed to solve the problem (Kushilevitz et al., 2006). Examining the information that must be exchanged between parties has ties to cryptography, secure communication channels, and distributed computation.

Another relevant topic of interest is known as the stabilizer sub-theory. It involves certain quantum operators (also called gates, which are mathematically represented by unitary matrices) and how quantum algorithms associated with these operators can be simulated efficiently on classical computers. Closely related to the formalism of stabilizers is the discrete Wigner function, which serves as both an intuitive approach to quantum states and a mathematical representation of them. As both of these areas are quite technical, the reader should refer to Appendices A and B for a better understanding of these topics.

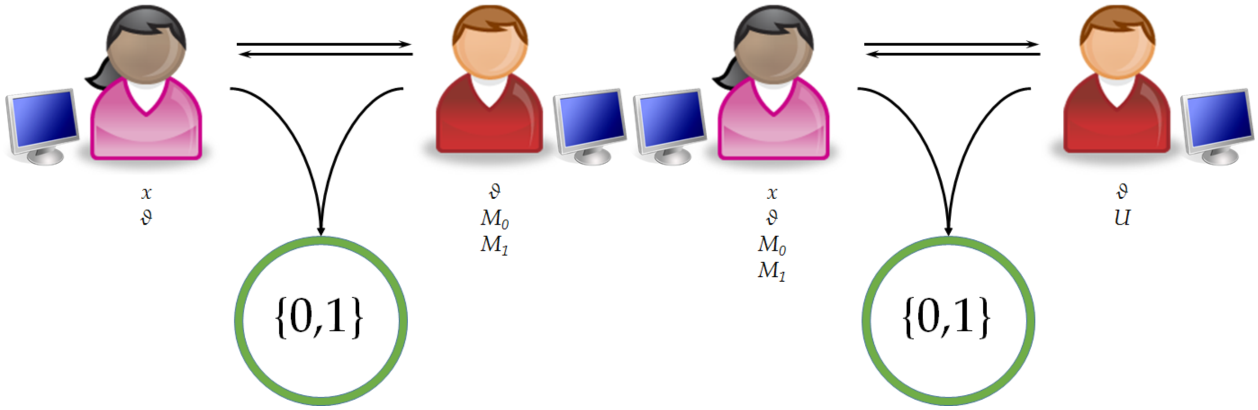
While communication complexity and the stabilizer sub-theory are not highly related topics, some problems arising from a communication complexity framework can be solved effectively by developing algorithms that are based upon the stabilizer formalism. One such problem is known as Raz's problem.

Raz's problem (Raz, 1999) comes in two variants, but both are based off of the same premise. The following definitions are consistent across both variants: the two parties of interest are named Alice and Bob; $x \in \mathbb{R}^d$ is a unit vector, where d is an odd prime number; M_0 and M_1 are orthogonal subspaces of $\mathbb{R}^d$; and $\vartheta \in \mathbb{R}$ where $0 \leq \vartheta < 1/\sqrt{2}$.

Problem 1. *Let Alice have the vector x, Bob have the subspaces M_0 and M_1, and both Alice and Bob have the value ϑ. Alice and Bob must communicate to output the value 0 if the distance $d(x, M_0) < \vartheta$, and 1 otherwise.*

Problem 2. *Let Alice have x and the subspaces M_0, M_1, Bob have an orthogonal matrix U, and both Alice and Bob have the value ϑ. Alice and Bob must communicate to output the value 0 if the distance $d(Ux, M_0) < \vartheta$, and 1 otherwise.*

The goal is to provide solutions to these problems that minimize the communication complexity between Alice and Bob. A visual representation of these problems can be seen in Figure 1. Raz showed that there exists a protocol which solves Problem 2 where the lower bound for its complexity, using probabilistic classical computation, is $\Omega(\sqrt{d})$, and the upper bound is $O(d^{3/4})$ (Raz, 1999). There is also a bound for Problem 1 of $O(\sqrt{d})$. As stated by Raz, and further discussed by Buhrman et al., efficient quantum computational protocols, however, have a communication complexity of $\Theta(log\, d)$, demonstrating an exponential separation in complexity between the two methods (Buhrman et al., 2009). The purpose of this report, then, is to develop a classical protocol that behaves like the quantum protocols in special cases, and approaches the classical lower bounds in general. In addition, the report characterizes the special cases and how the protocols behaves in general.



(a) Raz's Problem 1

(b) Raz's Problem 2

Figure 1: Visualization of Raz's problems

2.0 Analysis

To capitalize on the ideas provided by quantum mechanics, one can associate the d-dimensional vector x with the d-dimensional qudit $|\psi\rangle$, and let x be the mathematical representation of $|\psi\rangle$. In doing this, some mathematical tools used in discrete quantum systems, such as the discrete Wigner function (Appendix B), become useful in solving Raz's problems. By adapting the protocol outlined by Pashayan et al. (2014) for each problem, one can arrive at some classical computational protocols that solve Raz's problems probabilistically. These adapted protocols are more technical in nature, and are given in Appendices D and E. It is highly recommended that the reader review these appendices in order to follow the complexity analysis in the following subsections.

A key point to note is that throughout both of these protocols, no quantum computation ever occurs. These solutions are inspired by the stabilizer sub-theory, which behaves differently than general quantum computation. Additionally, calculating $\hat{x}$ between Step 5 and Step 6 in Protocol 1 (and similarly calculating $\hat{v}$ between Step 6 and Step 7 in Protocol 2) can be done since the vectors x and Ux are real (and thus $|\psi\rangle$ and $U|\psi\rangle$ are as well). If one was to perform a basis measurement on $|\psi\rangle$ and O is the random variable associated with the measurement outcome, then O is associated with the distribution $\Pr(O = k) = |\langle\psi|k\rangle|^2$. The value of the probability is the square of the kth component of $|\psi\rangle$. Computing the sample probability $\Pr(O = k)$ approximates the value of the kth element of x in Protocol 1. Doing this for each k produces the values of the vector $\hat{x}$. The same idea holds for $U|\psi\rangle$ and the kth value of Ux in Protocol 2, using $\Pr(O = k) = |\langle\psi\,|\,U\,|\,k\rangle|^2$.

2.1 Convergence and Repetition of the Protocols

The sample average, $\hat{R}$, over T repetitions, obeys the Chernoff-Hoeffding inequality (Pashayan et al., 2014):

$$\Pr(|\hat{R} - \mathbb{E}(R)|) \geq \epsilon) \leq 2e^{\frac{-T\epsilon^2}{2\mathcal{M}^2}} \tag{2.1.1}$$

where $\mathcal{M} = \mathcal{M}_\rho\mathcal{M}_U$, the total mana of the system (Appendix B). Thus, if T is large enough for each solution, then probabilistic convergence is guaranteed. In order to determine T, finding an upper bound for $\mathcal{M}$ is required. This value of $\mathcal{M}$ depends on x and the matrix U, but some upper bound for $\mathcal{M}$ can be established for all x and U. The next few subsections are dedicated to characterizing special cases of $\mathcal{M}$ given certain types of U and x.

2.1.1 Mana of General States and Matrices

Bounding $\mathcal{M}$ in a general case can be done by using the following propositions. Their proofs are listed in Appendix C for reference.

Proposition 1. *For any quantum state* $\rho, \mathcal{M}_\rho \leq \sqrt{d}$.

Proposition 2. *For any unitary (and by definition, orthogonal) matrix* $U, \mathcal{M}_U \leq d$.

This information states that for Protocol 1, $\mathcal{M} = \mathcal{M}_\rho \leq \sqrt{d}$, so Equation (2.1.1) becomes

$$\Pr(|\hat{R} - \mathbb{E}(R)|) \geq \epsilon) \leq 2e^{\frac{-T_1\epsilon^2}{2d}} \tag{2.1.2}$$

This convergence becomes independent of the dimension d if $T_1 = d$, which is a desirable quality of an algorithm. Similarly for Protocol 2, $\mathcal{M} = \mathcal{M}_U\mathcal{M}_\rho \leq d\sqrt{d}$, and thus setting $T_2 = d^{3/2}$ will remove the dependence of the size of x from the convergence of the protocol.

2.1.2 Mana of Stabilizer States and Clifford Gates

As is discussed in Appendix B, the discrete Wigner function and the stabilizer sub-theory are intimately connected, so using an algorithm based on the discrete Wigner function will likely behave differently when using stabilizer states and unitary matrices than it would behave otherwise. The following propositions are useful for characterizing the stabilizers in these solutions:

Proposition 3. *For any stabilizer state* $|\phi\rangle$, $W_{|\phi\rangle\langle\phi|}(\alpha) \geq 0$.

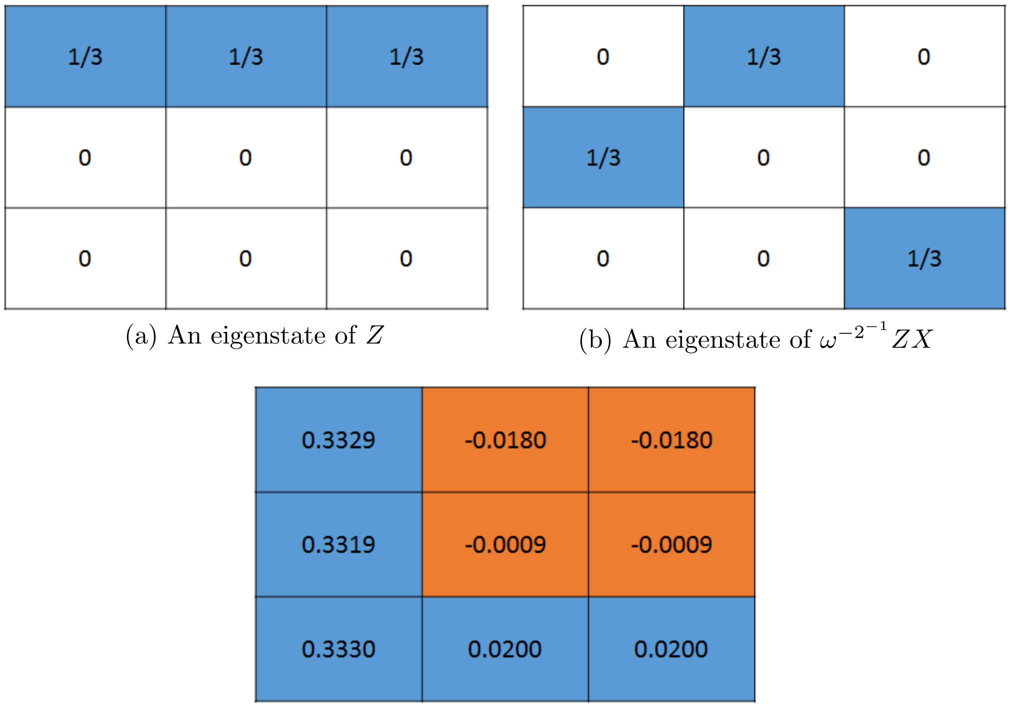
Proposition 4. *For any Clifford unitary* U, $W_U(\beta|\alpha) \geq 0$.

Proposition 3 is also known as Hudson's Theorem for finite-dimensional quantum systems, and the proof of both of these propositions is given by Gross (2006). The positivity of the Wigner function for stabilizer states and Clifford gates yields the following corollaries:

Corollary 1. *For any stabilizer state* $|\phi\rangle$, $\mathcal{M}_{|\phi\rangle\langle\phi|} = 1$.

Corollary 2. *For any Clifford unitary,* U, $\mathcal{M}_U(\alpha) = 1$ *for all* $\alpha \in \mathbb{Z}_d^2$.

These follow immediately from Propositions 3 and 4 and the properties of the discrete Wigner function (Appendix B). This means that in the case of states and matrices guaranteed to be in the stabilizer sub-theory, calculating the mana is unnecessary, and the concerns raised in Step 2 of Protocol 1 and Step 3 of Protocol 2 can be ignored. Better yet, due to the positive properties of stabilizers, Alice and Bob can use a geometric argument to produce an efficient protocol. As stated in Appendix B, stabilizer states form lines in the discrete phase space. Lines in this space are specified by $ax + bz = p \pmod{d}$, and an individual line can be uniquely determined by two points if d is prime.



1/3	1/3	1/3
0	0	0
0	0	0

(a) An eigenstate of Z

0	1/3	0
1/3	0	0
0	0	1/3

(b) An eigenstate of $\omega^{-2^{-1}}ZX$

0.3329	-0.0180	-0.0180
0.3319	-0.0009	-0.0009
0.3330	0.0200	0.0200

(c) A typical non-stabilizer state

Figure 2: The stabilizer states form a line in the discrete phase space ($d = 3$ shown), while non-stabilizer states do not.

Alice can specify what state x is by sending Bob four integers (indicating two coordinates in the discrete phase space that have non-zero values) since they uniquely determine a line. Bob then knows exactly what state Alice has. Using Figure 2a for example, Alice could send (0,0) and (0,1) to Bob (the northwest and north points in the grid), and he would know for certain which eigenstate of the Z matrix x was. In Problem 2 specifically, since Clifford matrices map stabilizer states to stabilizer states, Ux will form a line in the phase space, and Bob can send four integers back to Alice that specify two non-zero elements. Having U and x in the stabilizer sub-theory ensures a simple and effective way of solving both Problem 1 and Problem 2.

2.2 Communication Complexity of the Protocols

Without considering the precision on the mana values, Table 1 shows the maximum communication complexity of each step in Protocols 1 and 2. The communication complexity behaves like $O(T_1 \log d)$ for Protocol 1 and $O(T_2 \log d)$ for Protocol 2. Given the analysis of repetitions required for each protocol in Section 2.1, the complexities for each problem can be stated concisely. This is done in Tables 2 and 3.

Step No.	**Protocol 1**	**Protocol 2**
Step 1	0 bits	0 bits
Step 2	2 log$d$ bits	2 log$d$ bits
Step 3	0 bits	2 log$d$ bits
Step 4	0 bits	0 bits
Step 5	T_1 times	0 bits
Step 6	0 bits	T_2 times
Step 7	N/A	0 bits

Table 1: Communication complexity of each step in the two protocols.

In order to keep the complexities listed, $\hat{\mathcal{M}}_U(\alpha)$ and $\hat{\mathcal{M}}_\rho$ must be transmitted in $O(\log d)$ bits, or less, for each case. For unsigned real numbers (which can be used as the mana is always positive), this can be done using the Institute of Electrical and Electronics Engineers (IEEE) convention, since the mana is always bounded above by d. For example, if a number a can be expressed as $a = c2^q, c, q \in \mathbb{Z}$, by restricting c to be an integer 3 log d digits long and $q \in [0, 2 \log d]$, a can be any real value between 1 and d (to some finite precision), which

	Stabilizer x	**General** x
Protocol 1	• $O(\log\, d)$ • 1 round	• $O(d \log\, d)$ • d rounds
Quantum Solution 1	• $O(\log\, d)$ • 1 round	• $O(\log\, d)$ • 1 round
Raz's Solution	• $O(\sqrt{d})$	• $O(\sqrt{d})$

Table 2: Communication complexity and number of rounds for each protocol that solves Problem 1 in specified input cases.

	Stabilizer x, **Clifford** U	**General** x, **Clifford** U	**Stabilizer** x, **General** U	**General** x, **General** U
Protocol 2	• $O(\log\, d)$ • 1 round	• $O(d \log\, d)$ • d rounds	• $O(d^2 \log\, d)$ • d^2 rounds	• $O(d^3 \log\, d)$ • d^3 rounds
Quantum Solution 2	• $O(\log\, d)$ • 2 rounds	• $O(\log\, d)$ • 2 rounds	• $O(\log\, d)$ • 2 rounds	• $O(\log\, d)$ • 2 rounds
Raz's Solution	• $O(d^{3/4})$	• $O(d^{3/4})$	• $O(d^{3/4})$	• $O(d^{3/4})$

Table 3: Communication complexity and number of rounds for each protocol that solves Problem 2 in specified input cases.

is all that is required for specifying the mana. These two integers, c and q, can be expressed in $O(\log\, d)$ bits. Thus, Alice and Bob can communicate these mana values while achieving high precision and without altering the overall communication complexity of the protocols.

3.0 Conclusions

A family of classical protocols approaching $O(\sqrt{d})$ communication complexity that solve Raz's problem, and in some cases perform better than this, have now been developed and characterized. Some of these protocols will solve the problem exactly each time, and others will solve the problem probabilistically. The best case scenario arises when the two parties are working within the stabilizer sub-theory of quantum computation, where the problem can be solved exactly in one round of communication, with a complexity of $O(\log\, d)$. This mirrors the complexity of the best known quantum protocol, and is a desirable result. This complexity unfortunately does not hold when extended into general matrices and unit vectors, as Protocols 1 and 2 will require $O(d \log d)$ and $O(d^3 \log d)$ communication complexity, respectively. These solutions will converge probabilistically in multiple rounds of communication. These upper bounds for the protocols are not tight, however, so there may be room for improvement in the complexity of the solutions presented, or in developing new algorithms.

4.0 Recommendations

The guaranteed convergence of the protocols is dependent on the upper bounds on the mana values. The propositions presented give reasonable upper bounds, but they are not shown to be tight (it is not known which unitary matrices or density operators satisfy the equality in the propositions). Making use of other mathematical transformations may bring tighter bounds.

The mana has been quantified for Clifford unitary operators, but these operators do not form a set of universal quantum gates. Finding bounds on the mana for the extended Clifford hierarchy of operators may prove useful in establishing a more effective protocol for general orthogonal matrices.

Considering nearest neighbouring stabilizer states and Clifford operators may lead to better probabilistic protocols. Using states and matrices that behave efficiently under classical computation and most closely resemble the input states and matrices, one may be able to find a solution that will approximate the correct answer, and do so with little communication complexity.

References

Buhrman, Harry et al. "Non-locality and Communication Complexity" (2009), pp. 1–63. arXiv: 0907.3584v1.

Gottesman, Daniel. "The Heisenberg Representation of Quantum Computers". 1 (1998), pp. 1–20. arXiv: quant-ph/9807006v1.

Gross, D. "Hudson's theorem for finite-dimensional quantum systems". *Journal of Mathematical Physics* 47 (2006), pp. 1–25.

Kushilevitz, Eyal and Noam Nisan. *Communication Complexity.* Cambridge University Press, 2006. ISBN: 9780521029834. URL: http://books.google.ca/books?id=dHH7rdhKwzsC.

Pashayan, Hakop, Joel J Wallman, and Stephen D Bartlett. "Simulating quantum circuits with quasiprobabilities". 2014.

Raz, Ran. "Exponential separation of quantum and classical communication complexity". *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (1999), pp. 358–367. DOI: 10.1145/301250.301343.

Wootters, William K. "A Wigner-Function Formulation of Quantum Mechanics". *Annals of Physics* 176 (1987), pp. 1–21. DOI: 10.1016/0003-4916(87)90176-X.

Appendices

A The Stabilizer Sub-theory

The stabilizers states are the set of eigenstates of the Weyl-Heisenberg operators. The set of Weyl-Heisenberg operators is defined as follows:

$$\mathcal{D} = \{D_{x,z} = \omega^{-2^{-1}xz} Z^z X^x | x, z \in \mathbb{Z}_d\} \tag{A.1}$$

where $\omega = e^{\frac{i2\pi}{d}}$ and 2^{-1} is the multiplicative inverse of 2 modulo d. X and Z are d-dimensional generalizations of the two-dimensional Pauli matrices X and Z, and are defined by their action on basis vectors.

$$X\,|k\rangle = |k + 1 \pmod d\rangle \tag{A.2}$$

$$Z\,|k\rangle = \omega^k\,|k\rangle \tag{A.3}$$

Equivalently, their matrices take the forms

$$Z = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & e^{\frac{i2\pi}{d}} & & \vdots \\ \vdots & & \ddots & \\ 0 & ... & 0 & e^{\frac{i2\pi}{d}(d-1)} \end{pmatrix}, \; X = \begin{pmatrix} 0 & ... & 0 & 1 \\ 1 & 0 & ... & 0 \\ 0 & \ddots & \ddots & \vdots \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{A.4}$$

Related to the stabilizer states is the group of unitary matrices called the Clifford group. This group is defined as follows:

$$\mathcal{C}_d = \{U \in \mathcal{U}(d) |\, \forall P \in \mathcal{D}, \exists Q \in \mathcal{D} \text{ where } UPU^\dagger = Q\} \tag{A.5}$$

(Clifford operators map Weyl-Heisenberg operators to Weyl-Heisenberg operators). One reason why this particular subset of states and operators is interesting is the consequences of the Gottesman-Knill theorem. This was originally published by Gottesman and later expanded upon by Knill, and states that "A quantum circuit using only preparation of qudits in computational basis states, quantum gates from the Clifford group, and measurements in the computational basis, can be simulated efficiently on a classical computer" (Gottesman, 1998). This makes the stabilizers a very important set of gates and states when contrasting the differences between quantum and classical computing.

B The Discrete Wigner Function

The discrete Wigner function was originally introduced by Wootters as a discrete analogue to the continuous Wigner function, which is a representation of continuous quantum states in phase space (Wootters, 1987). The discrete phase space can be thought of as a d-by-d matrix (where d is the dimension of the Hilbert space), where a representation of a quantum state has a particular value in each element of the matrix. The discrete phase space also has a matrix operator associated with each point in the matrix, often called phase point operators and denoted by A. The phase point operators have the following definition:

$$A_{0,0} = \frac{1}{d} \sum_{x,z \in \mathbb{Z}_d} D_{x,z} \tag{B.1}$$

$$A_{x,z} = D_{x,z} A_{0,0} D^{\dagger}_{x,z} \tag{B.2}$$

where $D_{x,z}$ is a Weyl-Heisenberg displacement operator, as defined in Appendix A. Equivalently, the elements of the phase point operators can be expressed as

$$(A_{x,z})_{k,l} = \delta_{2x,k+l} e^{\frac{i2\pi}{d} z(k-l)} \tag{B.3}$$

where δ is the Kronecker Delta symbol, and $2x$ and $k+l$ are taken modulo d. Throughout the report, the notation $\alpha = (x, z)$, or any other Greek letter, has been used for brevity and clarity. Two useful properties of the phase point operators follow from their definition.

$$\mathrm{Tr}(A_\alpha) = 1 \tag{B.4}$$

$$\mathrm{Tr}(A_\alpha A_\beta) = d\delta_{\alpha\beta} \tag{B.5}$$

The phase point operators form a basis for the space of d-by-d matrices, so any quantum density operator ρ representing a single qudit state can be expressed as a linear combination of phase point operators. Specifically,

$$\rho = \sum_{\alpha \in \mathbb{Z}_d^2} W_\rho(\alpha) A_\alpha \tag{B.6}$$

$$U\rho U^\dagger = \sum_{\alpha,\beta \in \mathbb{Z}_d^2} W_\rho(\beta) W_U(\beta|\alpha) A_\alpha \tag{B.7}$$

for a unitary matrix U. Using the above properties of phase point operators and rearranging the previous equations yields the following definitions for the discrete Wigner function for a density operator ρ, unitary matrix U, and measurement E, respectively:

$$W_\rho(\alpha) = \frac{1}{d}\mathrm{Tr}(\rho A_\alpha) \tag{B.8}$$

$$W_U(\beta|\alpha) = \frac{1}{d}\mathrm{Tr}(A_\alpha U A_\beta U^\dagger) \tag{B.9}$$

$$W_E(\alpha) = \mathrm{Tr}(E A_\alpha) \tag{B.10}$$

The properties below follow immediately from the discrete Wigner function definition:

$$\sum_{\alpha \in \mathbb{Z}_d^2} W_\rho(\alpha) = 1 \tag{B.11}$$

$$\sum_{\alpha \in \mathbb{Z}_d^2} W_U(\beta|\alpha) = 1 \tag{B.12}$$

$$\sum_{\beta \in \mathbb{Z}_d^2} W_U(\beta|\alpha) = 1 \tag{B.13}$$

$$\sum_{\alpha \in \mathbb{Z}_d^2} W_E(\alpha) = 1 \tag{B.14}$$

$$\mathrm{Tr}(\rho\rho') = d \sum_{\alpha \in \mathbb{Z}_d^2} W_\rho(\alpha) W_{\rho'}(\alpha) \tag{B.15}$$

$$W_{U_1 U_2}(\beta|\alpha) = \sum_{\gamma \in \mathbb{Z}_d^2} W_{U_2}(\beta|\gamma) W_{U_1}(\gamma|\alpha) \tag{B.16}$$

Since the phase point operators are Hermitian, the Wigner function will always produce real values. Specific bounds for the individual values are

$$|W_\rho(\alpha)| \leq 1/d \tag{B.17}$$

$$|W_U(\beta|\alpha)| \leq 1 \tag{B.18}$$

$$|W_E(\alpha)| \leq 1 \tag{B.19}$$

(Pashayan et al., 2014). An interesting theorem arises from this formalism, named Hudson's Theorem for finite-dimension quantum systems, and its proof is given by Gross (2006). It proves that the only quantum states corresponding to an entirely non-negative discrete Wigner function are the stabilizer states. Additionally, this theorem implies that the non-zero values of W_ρ form a line if one plots the values in a matrix. This line is expressed as:

$$ax + bz = p \pmod{d} \;\; a, b, p \in \mathbb{Z}_d \tag{B.20}$$

and an example can be seen in Figure 2b. In light of the positivity of stabilizer states, the definition for the "mana" of a state and of a unitary operator are made as follows:

$$\mathcal{M}_\rho = \sum_{\alpha \in \mathbb{Z}_d^2} |W_\rho(\alpha)| \tag{B.21}$$

$$\mathcal{M}_U = \max_{\alpha \in \mathbb{Z}_d^2} \sum_{\beta \in \mathbb{Z}_d^2} |W_U(\beta|\alpha)| \tag{B.22}$$

$$\mathcal{M}_E = \max_{\alpha \in \mathbb{Z}_d^2} \sum_{j=1}^{d} |W_{E_j}(\alpha)| \tag{B.23}$$

One can intuitively think of this mana value as some measure of distance between a particular state and the stabilizer polytope, or the distance from some unitary operator to the Clifford group.

C Proofs of Propositions

Proposition 1. *For any quantum state $\rho, \mathcal{M}_\rho \leq \sqrt{d}$.*

Proof. For any density operator ρ, $1 \geq \mathrm{Tr}(\rho^2)$, and by definition of the discrete Wigner function

$$1 \geq \mathrm{Tr}(\rho^2) = d \sum_\alpha W_\rho(\alpha)^2 = d \sum_\alpha |W_\rho(\alpha)|^2 \tag{C.1}$$

Using the Cauchy-Schwarz Inequality,

$$\begin{aligned} \mathcal{M}_\rho^2 &= (\sum_\alpha |W_\rho(\alpha)|)^2 && \text{(C.2)} \\ &\leq (\sum_\alpha |W_\rho(\alpha)|^2)(\sum_\alpha |1|^2) && \text{(C.3)} \\ &= d(d \sum_\alpha |W_\rho(\alpha)|^2) && \text{(C.4)} \\ &\leq d && \text{(C.5)} \end{aligned}$$

It is not certain whether equality ever holds, so this inequality may be able to be made tighter. □

Proposition 2. *For any unitary operator $U, \mathcal{M}_U \leq d$.*

Proof.

$$UA_\alpha U^\dagger = \sum_\beta W_U(\beta|\alpha)A_\beta \tag{C.6}$$

$$d = \mathrm{Tr}(A_\alpha A_\alpha) \tag{C.7}$$

$$= \mathrm{Tr}(UA_\alpha U^\dagger UA_\alpha U^\dagger) \tag{C.8}$$

$$= \sum_\beta dW_U(\beta|\alpha)^2 \tag{C.9}$$

$$1 = \sum_\beta W_U(\beta|\alpha)^2 \tag{C.10}$$

By the Cauchy-Schwartz Inequality,

$$\mathcal{M}_U(\alpha)^2 = (\sum_\beta |W_U(\beta|\alpha)|)^2 \tag{C.11}$$

$$\leq (\sum_\beta |W_U(\beta|\alpha)|^2)(\sum_\beta |1|^2) \tag{C.12}$$

$$= d^2 \tag{C.13}$$

$$\mathcal{M}_U(\alpha) \leq d \tag{C.14}$$

Since this holds true for all α, it holds for the maximum value of $\mathcal{M}_U(\alpha)$, which is the definition of $\mathcal{M}_U$. It is not certain whether equality ever holds, so this inequality may be able to be made tighter. □

D Protocol 1: Solution to Problem 1

1. Let $\rho = |\psi\rangle \langle\psi|$, and let W_ρ and $\mathcal{M}_\rho$ be as defined in Appendix B.

2. Alice samples a value $\alpha \in \mathbb{Z}_d^2$ according to the weighted probability distribution

$$\Pr(\alpha) = \frac{|W_\rho(\alpha)|}{\mathcal{M}_\rho} \tag{D.1}$$

and sends α to Bob. She also sends $\mathrm{Sgn}(W_\rho(\alpha))$ and $\mathcal{M}_\rho$ (some positive real number). Alice will need to send back a truncated value of $\mathcal{M}_\rho$, denoted $\hat{\mathcal{M}}_\rho$, since sending the entire real number can in principle use an infinite amount of information. How precise this truncated value needs to be is discussed in Section 2.2.

3. Bob samples possible measurement outcomes from the distribution

$$\Pr(O = k|\alpha) = |W_{E_k}(\alpha)| \tag{D.2}$$

4. Bob sets the value

$$r = \hat{\mathcal{M}}_\rho W_{E_k}(\alpha)\mathrm{Sgn}(W_\rho(\alpha)) \tag{D.3}$$

He can regard this value as a realization of some random variable R, whose probability distribution is given by

$$\Pr(R = r) = \frac{|W_\rho(\alpha)|}{\mathcal{M}_\rho} \tag{D.4}$$

5. Alice and Bob repeat steps 2-4 T_1 times, and Bob calculates $\hat{R}$, the sample average of R over the T_1 repetitions. The particular value for T_1 is another topic of interest, and is discussed in Section 2.1. As shown by Pashayan et al. (2014),

$$\mathbb{E}(R) = \Pr(E_k|\rho) \tag{D.5}$$

where $\mathbb{E}(R)$ is the expected value of R. By doing this, Bob can approximate the measurement probabilities and create an estimate, $\hat{x}$, for the vector x.

6. On his computer, since Bob has the vector $\hat{x}$, he computes $\mathrm{d}(\hat{x}, M_0)$, which does not require any further communication, and outputs 1 or 0, depending on the result.

E Protocol 2: Solution to Problem 2

1. Let $\rho = |\psi\rangle \langle\psi|$, and let W_ρ and $\mathcal{M}_\rho$ be as defined in Appendix B.

2. Alice samples a value $\alpha \in \mathbb{Z}_d^2$ according to the weighted probability distribution

$$\Pr(\alpha) = \frac{|W_\rho(\alpha)|}{\mathcal{M}_\rho} \tag{E.1}$$

   and sends α to Bob.

3. Bob has the orthogonal (which is, by definition, unitary) matrix U, so by using the Wigner representation of U, W_U, he now samples $\beta \in \mathbb{Z}_d^2$ according to the distribution

$$\Pr(\beta|\alpha) = \frac{|W_U(\beta|\alpha)|}{\mathcal{M}_U(\alpha)} \tag{E.2}$$

   Bob sends β to Alice, along with $\mathrm{Sgn}(W_U(\beta|\alpha))$ and $\hat{\mathcal{M}}_U(\alpha)$. Like in the previous protocol, the precision to which Bob can send back $\hat{\mathcal{M}}_U(\alpha)$ needs to be specified. This is also discussed in Section 2.2.

4. Alice samples possible measurement outcomes from the distribution

$$\Pr(O = k|\beta) = |W_{E_k}(\beta)| \tag{E.3}$$

5. Alice sets the value

$$r = \hat{\mathcal{M}}_U(\alpha)\mathcal{M}_\rho W_{E_k}(\beta)\mathrm{Sgn}(W_\rho(\alpha)W_U(\beta|\alpha)) \tag{E.4}$$

   Alice regards this value as a realization of some random variable R, whose probability distribution is given by

$$\Pr(R = r) = \frac{|W_\rho(\alpha)|}{\mathcal{M}_\rho} \frac{|W_U(\beta|\alpha)|}{\mathcal{M}_U(\alpha)} \tag{E.5}$$

6. Alice and Bob repeat steps 2-5 T_2 times, and Alice calculates $\hat{R}$, the sample average of R over the T_2 repetitions (this value is also be discussed in Section 2.1). As shown by Pashayan et al. (2014),

   $$\mathbb{E}(R) = \Pr(E_k|\rho, U) \tag{E.6}$$

   By doing this, Alice can approximate the measurement probabilities and create an estimate, $\hat{v} \approx Ux$.

7. Alice computes $\mathrm{d}(\hat{v}, M_0)$, which does not require any communication, and outputs 1 or 0, depending on the result.