Partitioning Pauli Operators: in Theory and in Practice

by

Andrew Jena

A thesis
presented to the University Of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization (Quantum Information)

Waterloo, Ontario, Canada, 2019

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

- Chapter 1 is an introduction to the rest of the thesis with no novel material.
- Chapters 2 leans heavily on the results of Samshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan from their paper, *A new proof for the existence of mutually unbiased bases* [1].
- Chapter 3 provides a construction of a partition of Pauli operators framed in new terminology. A key fact which is used is taken from Joel V. Brawley and Timothy C. Teitloff's paper, *Similarity to symmetric matrices over finite fields* [3].
- Chapter 4 makes use of only basic concepts relating to the complexity of graph coloring. The idea to compare the partitioning problem to graph coloring was originally brought up by my advisor, Michele Mosca.
- The language in Chapter 5 is my own. It was thanks to the advice and guidance of Scott Genin that I recognized the application of these results to the variational quantum eigensolver.
- Chapter 6 is a conclusion to the rest of the paper, and the proposed future directions are a result of discussions between myself, Michele Mosca, and Scott Genin.

Abstract

Measuring the expectation value of Pauli operators on prepared quantum states is a fundamental task in the variational quantum eigensolver. Simultaneously measuring sets of operators allows for fewer measurements and an overall speedup of the measurement process. In this thesis, we look both at the task of partitioning all Pauli operators of a fixed length and of partitioning a random subset of these Pauli operators. We first show how Singer cycles can be used to optimally partition the set of all Pauli operators, giving some insight to the structure underlying many constructions of mutually unbiased bases. Thereafter, we show how graph coloring algorithms promise to provide speedups linear with respect to the lengths of the operators over currently-implemented techniques in the measurement step of the variational quantum eigensolver.

Acknowledgements

First, I would like to thank my supervisor, Michele Mosca, for helping fund, direct, and discuss my research for the entirety of this project. Second, I would like to thank Scott Genin of OTI Lumionics, who generously took the time to introduce me to the variational quantum eigensolver and helped me find a part of the problem which was both tractable to me and useful for near-term applications. Last, I would like to thank all my family and friends who allowed me to bounce ideas off of them, largely against their will, while I was writing this thesis.

Table of Contents

Chapter 1

Introduction

Our motivation for partitioning Pauli operators was, and remains, the speedup of the measurement step of the variational quantum eigensolver [10]. The variational quantum eigensolver may be a contender for a useful, near-term, quantum speedup, so the effort to optimize the measurement process is a popular topic of investigation [11, 5]. Before jumping into this practical problem and discussing how our results could apply to near-term experiments, we will first investigate the theory of Pauli partitioning,

The first problem we tackle is that of partitioning the entire set of Pauli operators of a fixed dimension and length. Upon recognizing the connection between these partitions and the mutually unbiased bases problem, we chose to generalize our results for qudit operators. We likewise investigate the more practical problem of partitioning an arbitrary set of Pauli operators in the language of qudit operators for the sake of completeness. Since we have made this effort to generalize our results, we will need to begin by establishing notation for the remainder of the thesis.

Definition 1 We shall use the following generalization of the Pauli matrices, which are often referred to as the shift and clock operators, respectively. For a prime, q, we define the following $q \times q$ unitary matrices:

$$X_q = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}; \quad Z_q = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \omega_q & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \omega_q^{q-1} \end{pmatrix},$$

where $\omega_q = e^{2\pi i/q}$. For $q = 2$, these are the 2×2 Pauli matrices. □

Definition 2 Let $\mathcal{P}_q$ denote the generalized Pauli group (ignoring phases) over $\mathbb{Z}/q\mathbb{Z}$. I.e., $\mathcal{P}_q = \left\{X_q^i Z_q^j : i, j \in \mathbb{Z}/q\mathbb{Z}\right\}$.

Similarly, let $\mathcal{P}_q^n = \{\bigotimes_{i=1}^n P_i : P_i \in \mathcal{P}_q\}$ be the set of generalized length-n Pauli operators (still ignoring phases) over $\mathbb{Z}/q\mathbb{Z}$. □

In Chapter 2, we begin to tackle the problem of partitioning $\mathcal{P}_q^n$ into sets in which all operators pairwise commute. We establish notation and basic results that lead to our construction in Chapter 3. We make use of facts about Singer cycles in $\mathrm{GL}_n(q)$ to prove the existence of a partition of $\mathcal{P}_q^n$ into the fewest possible number of parts, and give some applications of this result to already-known instances of the open problem of mutually unbiased bases.

We switch gears in Chapter 4 where we tackle the problem of partitioning a set of arbitrary-length Pauli operators and prove that this problem is NP-hard for worst-case sets. In Chapter 5, we discuss a particular application of this result and show the efficiency of using graph coloring algorithms to optimize the measurement step of the variational quantum eigensolver as imagined on a universal quantum computer. In Chapter 6, we conclude by comparing our algorithm to the algorithm in use at OTI Lumionics, showing an expected improvement by a factor which grows linearly with respect to the length of the Pauli operators.

Chapter 2

Partitioning $\mathcal{P}_q^n$: Foundations

Bandyopadhyay, Boykin, Roychowdhury and Vatan [1] give a similar summary of the following results. Much of the notation and many of the previously-known results in this section are based on this thesis. We cite this thesis explicitly when our wording is especially similar to theirs.

Definition 3 A set of Pauli operators is **commuting** if each pair of Pauli operators in the set pairwise commutes. □

Before we attempt to partition $\mathcal{P}_q^n$ into commuting sets, it is important to put bounds on the problem and to figure how many parts we might expect to be optimal.

Proposition 1 $\left|\mathcal{P}_q^n\right| = q^{2n}$. □

PROOF Since $|\mathcal{P}_q| = q^2$, we have q^2 unique choices for each P_i in our tensor product definition of $\mathcal{P}_q^n$. Thus, there are $(q^2)^n = q^{2n}$ unique operators in $\mathcal{P}_q^n$. ■

Proposition 2 *The maximum number of pairwise commuting operators in $\mathcal{P}_q^n$ is q^n.* □

PROOF Let $A_1, \ldots, A_k$ be a set of pairwise commuting operators in $\mathcal{P}_q^n$. Since these are pairwise commuting operators, there exists some unitary, U, such that $UA_jU^\dagger$ is diagonal, for all $j \in \{1, \ldots, k\}$ [9].

Moreover, since we are dealing with commuting Pauli operations, we may choose this unitary carefully such that $\left\{UA_jU^\dagger : j \in \{1, \ldots, k\}\right\} \subseteq \left\{\bigotimes_{\ell=1}^n X_q^0 Z_q^{j_\ell} : j_\ell \in \mathbb{Z}/q\mathbb{Z}\right\}$. In fact, we can efficiently construct such an operator from the generalized Clifford group, which we prove in the Diagonalization Algorithm.

Since $\left|\left\{\bigotimes_{\ell=1}^{n} X_q^0 Z_q^{j_\ell} : j_\ell \in \mathbb{Z}/q\mathbb{Z}\right\}\right| = q^n$, this gives an upper bound on the maximum number of pairwise commuting operators in $\mathcal{P}_q^n$. ■

Proposition 3 *The minimum number of parts in a partition of $\mathcal{P}_q^n$ into commuting sets is $q^n + 1$.* □

PROOF We first note that $\mathbb{1}_{q^n} = \bigotimes_{\ell=1}^{n} X_q^0 Z_q^0$ commutes with all operators. Thus, the number of non-identity operators in $\mathcal{P}_q^n$ is $q^{2n} - 1$ and the maximum number of non-identity pairwise-commuting operators in $\mathcal{P}_q^n$ is $q^n - 1$. The difference of squares formula gives us:

$$\frac{q^{2n} - 1}{q^n - 1} = q^n + 1,$$

which is a lower bound on the number of parts in a partition of $\mathcal{P}_q^n$ into commuting sets. ■

Definition 4 We shall call a partition of $\mathcal{P}_q^n$ into commuting sets a **minimal partition** if it has exactly $q^n + 1$ parts. □

We now introduce the symplectic representation of Pauli operators to simplify our statements.

Definition 5 For the Pauli operator, $X_q^{x_1} Z_q^{z_1} \otimes X_q^{x_2} Z_q^{z_2} \otimes \ldots X_q^{x_n} Z_q^{z_n} \in \mathcal{P}_q^n$, we call the vector, $\left(\begin{array}{cccc|cccc} x_1 & x_2 & \ldots & x_n & z_1 & z_2 & \ldots & z_n \end{array}\right) \in (\mathbb{Z}/q\mathbb{Z})^{2n}$, its **symplectic form**. We shall switch between the normal and symplectic representations as necessary throughout the rest of the thesis. □

Since we are attempting to partition $\mathcal{P}_q^n$ into commuting sets, it is natural to first ask what it means for two Pauli operators to be commuting in our symplectic notation. This is captured by the symplectic inner product, which we define below.

Definition 6 For two Pauli operators, $\left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right)$ and $\left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right)$, the **symplectic inner product** is defined as follows:

$$\left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right) \odot \left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right) = \boldsymbol{x_i} \cdot \boldsymbol{z_j} - \boldsymbol{z_i} \cdot \boldsymbol{x_j}.$$ □

Lemma 1 $\left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right), \left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right) \in \mathcal{P}_q^n$ *commute* $\iff \left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right) \odot \left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right) \equiv 0 \ (mod\ q)$. □

PROOF This is simple to show using the fact that $Z_q X_q = \omega_q X_q Z_q$. ■

Lemma 2 *For all $a \in \mathbb{Z}/q\mathbb{Z}$, we have:*

$$\left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right) \odot \left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right) \equiv 0 \ (mod\ q) \implies a\left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right) \odot \left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right) \equiv 0 \ (mod\ q). \qquad \square$$

PROOF Follows directly from the definition of the symplectic inner product and a bit of algebra. ■

Lemma 3

$$\left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right) \odot \left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right) \equiv 0 \ (mod\ q) \ and \ \left(\boldsymbol{x_k} \mid \boldsymbol{z_k}\right) \odot \left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right) \equiv 0 \ (mod\ q)$$
$$\implies \left(\left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right) + \left(\boldsymbol{x_i} \mid \boldsymbol{z_i}\right)\right) \odot \left(\boldsymbol{x_j} \mid \boldsymbol{z_j}\right) \equiv 0 \ (mod\ q). \qquad \square$$

PROOF Again, follows directly from the definition of the symplectic inner product and a bit of algebra. ■

Lemma 2 and Lemma 3 give us an important piece of information. We see that any operator in the span of a set of commuting operators will commute with the whole set. In other words, any set of q^n pairwise-commuting Pauli operators must be equal to its own span, or else we could extend to have a larger commuting set. With this realization, we may identify each part by a basis of its operators.

Given a minimal partition of $\mathcal{P}_q^n$ into the $q^n + 1$ parts, $\mathcal{C}_0, \ldots, \mathcal{C}_{q^n}$, we might wish to have a succinct way of writing down our partition. Since each part in a minimal partition must have $q^n - 1$ non-identity Pauli operators, we can identify each part by n linearly independent operators. Letting the symplectic representation of these operators be the rows of a matrix, we may write each part as $\mathcal{C}_i = \left(B_i \mid A_i\right)$, where B_i and A_i are in $(\mathbb{Z}/q\mathbb{Z})^{n \times n}$.

Using our Diagonalization Algorithm, we know that we may conjugate all the operators by a Clifford group element such that one of the parts is diagonal. WLOG, we shall henceforth assume that $\mathcal{C}_0 = \left(0_n \mid \mathbb{1}_n\right)$.

Under this assumption, if any other part contains two operators with equal X component, then their difference (which is in the span so must also be in the same part) will be in part 0. Thus, we observe that all possible X components must appear in every other part of our partition. This allows us to write our partition as follows:

$$\mathcal{C}_0 = \left(0_n \mid \mathbb{1}_n\right), \ \mathcal{C}_1 = \left(\mathbb{1}_n \mid A_1\right), \ \ldots, \mathcal{C}_{q^n} = \left(\mathbb{1}_n \mid A_{q^n}\right).$$

Now, we ask which conditions these matrices, A_i, must satisfy in a minimal partition.

Proposition 4 *In order to have a minimal partition, the following conditions must hold:*

1. *A_i is symmetric, for all $i \in \{1, \ldots, q^n\}$*
2. *$A_i - A_j$ is invertible, for all $i \neq j$.* □

Proof

1. The symplectic inner product of the a^{th} row and the b^{th} row of $\mathcal{C}_i$ is $A_i(a,b) - A_i(b,a)$ (where these are the (a,b) and (b,a) entries of A_i, respectively). Since this difference is zero for any commuting operators, we must have $A_i(a,b) = A_i(b,a)$, for all i, a, b. In other words, A_i is symmetric, for all i.
2. We require that the parts, $\mathcal{C}_i$, of our partition be disjoint. With this notation, this is equivalent to requiring the span of the rows of A_i to be disjoint from the span of the rows of A_j, for all $i \neq j$. This is equivalent to the requirement that $\boldsymbol{v}A_i - \boldsymbol{v}A_j \not\equiv \mathbf{0} \pmod{q}$, for all non-zero $\boldsymbol{v} \in (\mathbb{Z}/q\mathbb{Z})^n$ and for all $i \neq j$. In other words, $A_i - A_j$ must be invertible. ■

Chapter 3

Partitioning $\mathcal{P}_q^n$: Singer Cycles and Mutually Unbiased Bases

To begin our new results, we start with an assumption which, in lieu of the X-ization Algorithm, is without loss of generality. We assume that $\mathcal{C}_1 = \left(\mathbb{1}_n \mid 0_n\right)$. This forces $A_2, \ldots, A_{q^n}$ to be invertible.

Now that we are working with invertible matrices, we use the following notation.

Definition 7 Let $\mathrm{GL}_n(q)$ be the set of all invertible, $n \times n$ matrices over $\mathbb{Z}/q\mathbb{Z}$. □

We now seek a set of $q^n - 1$ symmetric matrices in $\mathrm{GL}_n(q)$ such that the difference between any of our matrices is still in $\mathrm{GL}_n(q)$. Luckily, Singer cycles provide a simple construction for a set of this size in $\mathrm{GL}_n(q)$, so we shall investigate whether we can use Singer cycles to construct a set satisfying the conditions.

Definition 8 A **Singer cycle** is an element, $M \in \mathrm{GL}_n(q)$, of multiplicative order $q^n - 1$.□

The following proof has been shown many times before, but we shall investigate it in detail to gain some insight for our problem.

Proposition 5 *For all primes, q, and for all positive integers, n, there exists a Singer cycle in $GL_n(q)$.* □

Proof Let $f(x)$ be a primitive polynomial of degree n over $\mathrm{GF}(q)[x]$. Without loss of generality, we may define $\mathrm{GF}(q^n) = \mathrm{GF}(q)[x]/f(x)$.

A key fact about primitive polynomials is that $f(x) \nmid \left(x^k - 1\right)$, for all $0 < k < q^n - 1$. In other words, the polynomial x is a generator for our choice of $\mathrm{GF}(q^n)$.

We shall represent polynomials in $\mathrm{GF}(q^n)$ as vectors in $(\mathbb{Z}/q\mathbb{Z})^n$ in the following way:

$$p(x) = a_0x^0 + a_1x^1 + \ldots + a_{n-1}x^{n-1} \to \boldsymbol{v_p} = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \end{pmatrix}^\top.$$

Let C_f be the companion matrix of $f(x)$:

$$C_f = \begin{pmatrix} 0 & 0 & \ldots & 0 & \\ 1 & 0 & \ldots & 0 & \\ 0 & 1 & \ldots & 0 & \boldsymbol{v_{x^n - f(x)}} \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \ldots & 1 & \end{pmatrix}.$$

Multiplying a polynomial by x is equivalent to multiplying its corresponding vector representation on the left by C_f. Since x is a generator of $\mathrm{GF}(q^n)$, it has multiplicative order $q^n - 1$, and thus, so does C_f.

Since the first entry of $\boldsymbol{v_{x^n - f(x)}}$ is non-zero, $C_f \in \mathrm{GL}_n(q)$, so C_f is a Singer cycle. ∎

We have now seen that a companion matrix for a primitive polynomial of degree n over $\mathrm{GF}(q)$ will always be a Singer cycle. Next, we show that any similar matrix is also a Singer cycle.

Proposition 6 *Let C be a Singer cycle in $GL_n(q)$ and let A be an arbitrary element of $GL_n(q)$. Then ACA^{-1} is also a Singer cycle in $GL_n(q)$.* □

Proof Since $A, C \in \mathrm{GL}_n(q)$, it is clear that $ACA^{-1} \in \mathrm{GL}_n(q)$. Thus, all we need to show is that this matrix has multiplicative order $q^n - 1$.

Assume that $(ACA^{-1})^i = (ACA^{-1})^j$ for some i, j. Then we have:

$$\begin{aligned} 0_n &= \left(ACA^{-1}\right)^i - \left(ACA^{-1}\right)^j \\ &= AC^iA^{-1} - AC^jA^{-1} \\ &= A\left(C^i - C^j\right)A^{-1} \end{aligned}$$

which implies that $C^i = C^j$. By our choice of C, this only occurs when $i \equiv j \pmod{q^n - 1}$. In other words, any similar matrix has multiplicative order $q^n - 1$, making it a Singer cycle. ∎

With this, we rely on a Theorem from [3] to get us closer to our goal.

Theorem 1 *If $f(x)$ is primitive, then C_f is similar (over $GL_n(q)$) to a symmetric matrix.* □

We first observe that if a matrix, A, is symmetric, then $A^k = (A^\top)^k = (A^k)^\top$, so any power of A is also symmetric. Since a Singer cycles gives rise to a set of $q^n - 1$ distinct matrices in $\mathrm{GL}_n(q)$, a symmetric Singer cycle generates a set which satisfies condition (i) of Proposition 4. However, in order to prove that we may construct a minimal partition, we still need to show that the second condition is satisfied by the powers of our symmetric Singer cycle. Luckily, this is the case, as we show below.

Proposition 7 *Let C_f be the companion matrix of a primitive polynomial of degree n over $GF(q)[x]$; let $A \in GL_n(q)$. Then AC_fA^{-1} satisfies condition 2 in Proposition 4.* □

Proof We must show that $(AC_fA^{-1})^i - (AC_fA^{-1})^j \in \mathrm{GL}_n(q)$.

Rewriting the above expression, we get: $(AC_fA^{-1})^i - (AC_fA^{-1})^j = A\left(C_f^i - C_f^j\right)A^{-1}$.

As mentioned previously, left multiplying by C_f is equivalent to multiplying the corresponding polynomial by x. Similarly, left multiplying by C_f^i is equivalent to multiplying the corresponding polynomial by x^i.

Since x is a generator of $\mathrm{GF}(q^n)$, we observe that there exists some $k \in \{0, \ldots, q^n - 1\}$ such that $x^k = x^i - x^j$ (whenever $i \not\equiv j \pmod{q^n - 1}$). Thus, $C_f^i - C_f^j = C_f^k$, and we have $(AC_fA^{-1})^i - (AC_fA^{-1})^j = AC_f^kA^{-1}$, which is invertible. ■

Putting everything together, we have shown that we may find a symmetric Singer cycle in $\mathrm{GL}_n(q)$, and that the powers of this Singer cycle will satisfy the two conditions for $A_2, \ldots, A_{q^n}$ to produce a minimal partition of $\mathcal{P}_q^n$. Thus, we have shown, by construction, that a minimal partition of $\mathcal{P}_q^n$ exists for all primes, q, and all positive integers, n. We shall now show how this result applies to the problem of mutually unbiased bases.

Definition 9 Let $B_1 = \{|\phi_1\rangle, \ldots, |\phi_d\rangle\}$ and $B_2 = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$ be two orthonormal bases of $\mathbb{C}^d$. We say that B_1 and B_2 are **mutually unbiased bases** if:

$$\text{for all } i, j \in \{1, \ldots, d\},\ |\langle\phi_i|\psi_j\rangle| = \frac{1}{\sqrt{d}}.$$ □

We note that it has been proven that, for a given dimension, d, any set of pairwise mutually unbiased bases has size at most $d + 1$. In fact, it has also been shown previously

that this maximal number of mutually unbiased bases can be attained in prime-power dimensions, $d = q^n$. Theorem 2 will give a simple proof of this result using our new proof of the existence of a minimal partition of $\mathcal{P}_q^n$.

The following proof is adapted from a proof of the inner product between stabilizer states given in [4].

Theorem 2 *If there is a minimal partition of $\mathcal{P}_q^n$, then there is a set of $q^n + 1$ mutually unbiased bases of dimension q^n.* □

PROOF Let $\mathcal{C}_0, \ldots, \mathcal{C}_{q^n}$ be a minimal partition of $\mathcal{P}_q^n$. Let $\mathcal{C}'_i = \mathcal{C}_i \cup \mathbb{1}_{q^n}$.

As proved in the Diagonalization Algorithm and X-ization Algorithm for any $i \neq j \in \{0, \ldots, q^n\}$, there exists a Clifford group operation, U, such that $\left\{UP_{i,a}U^\dagger : P_{i,a} \in \mathcal{C}_i\right\} \subseteq \left\{\bigotimes_{\ell=1}^n X_q^0 Z_q^{j_\ell} : j_\ell \in \mathbb{Z}/q\mathbb{Z}\right\}$ and $\left\{UP_{j,a}U^\dagger : P_{j,a} \in \mathcal{C}_j\right\} \subseteq \left\{\bigotimes_{\ell=1}^n X_q^{k_\ell} Z_q^0 : k_\ell \in \mathbb{Z}/q\mathbb{Z}\right\}$. Since $|\mathcal{C}'_i| = q^n = |\mathcal{C}'_j|$, we see that the subsets are actually equivalences.

Writing this another way, we may order the elements of $\mathcal{C}'_i$ such that:

$$UP_{i,a}U^\dagger = \bigotimes_{\ell=1}^n X_q^0 Z_q^{a_\ell} \implies P_{i,a} = U^\dagger \left(\bigotimes_{\ell=1}^n X_q^0 Z_q^{a_\ell}\right) U$$

where a_ℓ is the ℓ^{th} entry in the q-ary representation of a. Writing $U = \begin{pmatrix} |\psi_{i,0}\rangle & |\psi_{i,1}\rangle & \ldots & |\psi_{i,q^n-1}\rangle \end{pmatrix}$, we see that these states are eigenvectors for each Pauli operator in $\mathcal{C}'_i$. We may similarly order the elements of $\mathcal{C}'_j$ such that:

$$UP_{j,b}U^\dagger = \bigotimes_{\ell=1}^n X_q^{b_\ell} Z_q^0 \implies P_{j,b} = U^\dagger \left(\bigotimes_{\ell=1}^n X_q^{b_\ell} Z_q^0\right) U.$$

We let F_q be the quantum fourier transform over $\mathbb{Z}/q\mathbb{Z}$ and use the identity from the Diagonalization Algorithm to write: $F_q^{\otimes n}\left(X_q^{a_\ell} Z_q^0\right)(F_q^{\otimes n})^\dagger = X_q^0 Z_q^{a_\ell}$. This allows us to rewrite the above expression as:

$$F_q^{\otimes n} UP_{j,b}U^\dagger (F_q^{\otimes n})^\dagger = \bigotimes_{\ell=1}^n X_q^0 Z_q^{b_\ell} \implies P_{j,b} = U^\dagger (F_q^{\otimes n})^\dagger \left(\bigotimes_{\ell=1}^n X_q^0 Z_q^{b_\ell}\right) F_q^{\otimes n} U.$$

In other words, $F_q^{\otimes n} U = \begin{pmatrix} |\psi_{j,0}\rangle & |\psi_{j,1}\rangle & \ldots & |\psi_{j,q^n-1}\rangle \end{pmatrix}$ are the eigenvectors for each Pauli operator in $\mathcal{C}'_j$.

Another way to write these eigenvectors is to identify them by their column in the matrices, U and $F_q^{\otimes n}U$. By definition, we have: $|\psi_{i,a}\rangle = U|a\rangle$ (where $|a\rangle$ is the vector with a single 1 in the a^{th} entry). Similarly, $|\psi_{j,b}\rangle = F_q^{\otimes n}U|b\rangle$.

Since these states are eigenvectors of a unitary operator, they form an orthonormal basis. If we can show that the inner product between any two eigenvectors from separate parts of our partition satisfy the condition for being mutually unbiased, we will have given a construction for a set of mutually unbiased bases from a minimal partition. We check this below:

$$|\langle\psi_{i,a}|\psi_{j,b}\rangle| = |\langle a|U^\dagger F_q^{\otimes n}U|b\rangle|.$$

In other words, we are picking out the a, b entry of $F_q^{\otimes n}$ with a unitary change of basis. Since F_q is the quantum Fourier transform over $\mathbb{Z}/q\mathbb{Z}$, every entry of $F_q^{\otimes n}$ has modulus $1/\sqrt{q^n}$, and this modulus will be preserved by our change of basis. This satisfies the condition for mutually unbiased bases, so by taking the eigenvectors corresponding to each part of our partition, we will construct a set of $q^n + 1$ mutually unbiased bases in $\mathbb{C}^{q^n}$. ∎

The problem of partitioning Pauli operators has given us a nice theoretical result with respect to the open problem of finding mutually unbiased bases. However, there is still more that can be accomplished by solving the more-general problem of partitioning a subset of Pauli operators. We begin with those results in the next chapter.

Chapter 4

Partitioning Arbitrary Sets of Pauli Operators

From our previous results, we know that we may partition $\mathcal{P}_q^n$ into q^n+1 commuting parts. However, given an arbitrary set of Pauli operators, this bound provides an upper bound. How many parts might we expect to be optimal, and how might we go about finding such an optimal partition? Letting $\mathcal{P}_q^*$ denote the set of Pauli operators of dimension q and arbitrary length (where commutation between two operators is decided on the set of qudits restricted to the smaller-length operator), we shall formalize this problem and show its equivalence to graph coloring. We begin by defining some notation for our reductions and the relevant problems.

Definition 10 An algorithm, A, polytime reduces to another algorithm, B, ($A \leq_{\mathrm{P}} B$) if there exists a polytime algorithm which solves A given an oracle for solving B. □

Definition 11 A is polytime equivalent to B ($A \equiv_{\mathrm{P}} B$) if $A \leq_{\mathrm{P}} B$ and $B \leq_{\mathrm{P}} A$. □

Definition 12 A partition of $\mathcal{S} \subseteq \mathcal{P}_q^*$ into k commuting parts is a ***k*-partition** of $\mathcal{S}$. □

Definition 13 We define the k-partitioning problem (***k*Part**) as follows:

Given: $\mathcal{S} \subseteq \mathcal{P}_q^*$ and $k \in \mathbb{Z}_{\geq 1}$

Question: does there exists a k-partition of $\mathcal{S}$? □

Definition 14 A ***k*-coloring** of a simple, undirected graph, G, is a partition of the vertices of G into k co-cliques. □

Definition 15 We define the k-coloring (***k*Color**) problem as follows:

Given: a simple, undirected graph, G, and $k \in \mathbb{Z}_{\geq 1}$

Question: does there exists a k-partition of $\mathcal{S}$? □

Proposition 8 *kPart $\equiv_P$ kColor* □

Proof We shall prove the reduction in both directions.

- kPart $\leq_{\mathrm{P}}$ kColor: let O^C be an oracle for kColor .

  Given a set, $\mathcal{S} \subseteq \mathcal{P}_q^*$, and an integer, $k \in \mathbb{Z}_{\geq 1}$, we construct a graph, $G = (V, E)$, (we'll call this the **anticommutation graph**) by letting:

  - $V = \mathcal{S}$
  - $E = \{P_i P_j : P_i, P_j \in \mathcal{S}$ and P_i does *not* commute with $P_j\}$.

  We observe that a k-coloring of G is a partition of its vertices into co-cliques. In other words, each part is a commuting set of Pauli operators. Therefore, a k-partition of $\mathcal{S}$ exists if and only if a k-coloring of G exists.

  Therefore, the output of $O^C(G, k)$ is a solution to kPart.

- kColor $\leq_{\mathrm{P}}$ kPart: let O^P be an oracle for kPart .

  Given a graph, $G = (V, E)$, and an integer, $k \in \mathbb{Z}_{\geq 1}$, we first define the adjacency matrix of G to be the matrix, A_G, such that:

$$A_G(u, v) = \begin{cases} 1 & uv \in E \\ 0 & uv \notin E \end{cases}$$

  We then construct a set $\mathcal{S} \subseteq \mathcal{P}_q^*$ by letting:

  - $\mathcal{S} = \left(\mathbb{1}_n \mid A_G^{LT}\right)$,

  where A_G^{LT} is the lower triangular portion of the adjacency matrix of G. Indexing our set of Pauli operators by the vertices of G, we observe that P_u commutes with P_v if and only if $uv \notin G$.

  We observe that a k-partition of $\mathcal{S}$ is a partition of the Pauli operators into commuting sets. In other words, each part is a co-clique of the vertices of G. Therefore, a k-coloring of G exists if and only if a k-partition of $\mathcal{S}$ exists.

  Therefore, the output of $O^P(\mathcal{S}, k)$ is a solution to kColor . ■

It has long been known that kColor (for $k \geq 3$) is NP-complete with respect to $|V(G)|$. Since the number of vertices in G is the same as the number of Pauli operators in our set, $\mathcal{S}$, in both directions of our above equivalence, this immediately gives us the following result.

Theorem 3 *kPart (for $k \geq 3$) is NP-complete with respect to $|\mathcal{S}|$.* □

Using a similar reduction to above, we may show that the following problem is NP-hard.

Definition 16 Given $\mathcal{S} \subseteq \mathcal{P}_q^*$, the **Pauli partitioning problem** is to return a partition of $\mathcal{S}$ into the fewest number of commuting parts. □

In fact, this problem is exactly equivalent to coloring the corresponding anticommutation graph with the fewest colors. As such, we can say a few things about the expected number of parts in a partition of a randomly chosen set of Paulis from $\mathcal{P}_q^*$.

Proposition 9 *For almost all sets, $\mathcal{S} \subseteq \mathcal{P}_q^*$, such that all the operators in $\mathcal{S}$ are linearly independent, the number of parts in a minimal partition of $\mathcal{S}$ is:*

$$\left(\frac{1}{2} + o(1)\right) \left(\log_2(q) + o(1)\right) \frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}$$ □

Proof Let m be the largest length of any Pauli operator in $\mathcal{S}$.

For any two randomly-chosen Pauli operators, $P_i, P_j \in \mathcal{P}_q^m \setminus \mathbb{1}_{q^m}$, the probability that P_i commutes with P_j is $(q^{2m-1} - 2)/(q^{2m} - 1)$. If we choose a single non-identity qubit of P_i, then P_j may take any values on the remaining $m - 1$ qubits (i.e. q^{2m-2} possibilities), but must take any one of q values on the last qubit to make the symplectic inner product 0 (i.e. q^{2m-1} possibilities), and we subtract 2 for the identity operator and for P_i, itself.

Choosing an ordering on our set, $\mathcal{S} = \{P_1, \ldots, P_{|S|}\}$, we define the following matrix:

$$C(i,j) = P_i \odot P_j,$$

and observe that we may always find a Clifford group operation which acts by conjugation on our set transforming it into:

$$\left(\mathbb{1}_{|\mathcal{S}|}\ 0_{n-|\mathcal{S}|} \mid C^{LT}\ 0_{n-|\mathcal{S}|}\right).$$

This is because the symplectic inner product between any pair of operators is preserved in our new formulation. Thus, for any operator outside of $\mathcal{S}$, whether it commutes with P_i is

determined solely by the power of the X term on its i^{th} qubit. Since the powers on each qubit are chosen independently, the probabilities are independent.

This implies that the anticommutation graph is a random graph on $|\mathcal{S}|$ vertices with edge-probability $1-(q^{2m-1}-2)/(q^{2m}-1)$. Using the result from [2], the minimum number of colors necessary to color G is expected to be:

$$\begin{aligned}
&\left(\frac{1}{2}+o(1)\right)\log_2\left(\frac{1}{1-\left(1-\frac{q^{2m-1}-2}{q^{2m}-1}\right)}\right)\frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}\\
&=\left(\frac{1}{2}+o(1)\right)\log_2\left(\frac{q^{2m}-1}{q^{2m-1}-2}\right)\frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}\\
&=\left(\frac{1}{2}+o(1)\right)\left(\log_2(q)+o(1)\right)\frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}
\end{aligned}$$

■

In the last proposition, we have clearly required the assumption that the operators in our set were linearly independent. However, we conjecture that the value found above remains an upper bound for an arbitrary set, S.

Conjecture 1 *For almost all sets, $\mathcal{S}\subseteq\mathcal{P}_q^*$, the number of parts in a minimal partition of $\mathcal{S}$ is bounded above by:*

$$\left(\frac{1}{2}+o(1)\right)\left(\log_2(q)+o(1)\right)\frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}$$

PROOF First, we give evidence for why we might expect our assumption about linear independence to be satisfied for a randomly-chosen set.

The probability that there are no linearly dependent subsets of a set, $\mathcal{S}$, of length-m, q-ary Pauli operators is:

$$\prod_{i=0}^{|\mathcal{S}|-1}\left(1-q^{i-2m}\right)=(q^{-2m};q)_{|\mathcal{S}|},$$

where $(a;q)_k$ is the q-Pochhammer symbol.

For values of $|\mathcal{S}|\leq 2m$, this probability is bounded below by a fixed value which depends on q. For $q=2$, it is bounded by ≈ 0.288788 and for larger values of q, this value tends towards 1.

In other words, for any value of q, this size requirement is enough to ensure our graph is random with probability greater than $1/4$.

However, when $|\mathcal{S}| > 2m$, we must rely on a different argument which gives a heuristic for why the number of partitions should actually be lower than if there were not linear dependence.

In instances where we have linear dependence in our Pauli operators, by Lemmas 2 and 3, we see that we get larger co-cliques than would be expected in a random graph. If our set has some linear dependent subsets, then we should expect the same total number of edges, but larger cliques and cocliques, which should admit a coloring with fewer colors. ■

Having established these expectations, we shall now dive into some applications of these partitions and shall observe the improvements we have made to the measurement step of the variational quantum eigensolver.

Chapter 5

Measurement in the Variational Quantum Eigensolver

The variational quantum eigensolver is a quantum-classical hybrid algorithm used for finding the ground state energy of a molecule [10]. With applications ranging from quantum chemistry to combinatorial optimization and a low cost in quantum resources, the variational quantum eigensolver is a great candidate for near-term applications of quantum computers.

We shall first introduce the problem in more specificity, then we shall discuss the measurement scheme which has been used in past implementations of the algorithm. We shall compare this measurement scheme to one which we derive from our previous discussion of k-partitions, showing the benefits of the latter approach.

Definition 17 The **variational quantum eigensolver** solves the following problem:

Given: $H = \sum_k c_k P_k$, a Hamiltonian written as a sum over Pauli operators

Goal: approximate the smallest eigenvalue, λ, of H. □

To begin our analysis, we see that, if we were able to initialize the eigenstate, $|\psi\rangle$, such that $H|\psi\rangle = \lambda|\psi\rangle$, and if we could measure $\langle\psi|H|\psi\rangle = \langle\psi|\lambda|\psi\rangle = \lambda$, then we could complete our goal. However, there are two problems with this:

1. How do we produce $|\psi\rangle$?
2. How do we measure $\langle\psi|H|\psi\rangle$?

The first of the above problems is arguably dealt with by a classical optimization algorithm. Preparing an initial state, $|\psi_0\rangle$, and measuring $\langle\psi_0|H|\psi_0\rangle$, we plug our results into a classical optimizer which returns a new state, $|\psi_1\rangle$. Continuing this process, we improve our state until we construct some $|\tilde{\psi}\rangle$ such that $|\langle\tilde{\psi}|H|\tilde{\psi}\rangle - \lambda| \leq \varepsilon$, for some desired precision. The efficiency of this process and the ongoing search for improved algorithms is discussed by McClean, Romero, Babbush, and Aspuru-Guzik [8].

The second problem, however, seemingly requires us to simulate our Hamiltonian, H, which may be very difficult. To get around this, we observe that expectation values are linear, so we have:

$$\langle\psi|H|\psi\rangle = \left\langle\psi\middle|\sum c_k P_k\middle|\psi\right\rangle = \sum c_k \langle\psi|P_k|\psi\rangle .$$

Measuring $\langle\psi|P_k|\psi\rangle$ is as simple as transforming P_k into a diagonal Pauli operator and measuring in the computational basis. Therefore, we are able to accomplish this step efficiently.

While the algorithm we have outlined above looks feasible at first glance, it is still not practical for many near-term quantum devices. The first issue is the length of these Pauli operators (which determines the number of qubits in the system). For many interesting molecules, the number of qubits required is already out of the reach of near-term quantum devices.

The second issue, however, is the sheer number of runs required to make the algorithm work. Considering we require this many measurements (and this many initializations of $|\psi_i\rangle$), in each quantum step of our algorithm, it is important to try to cut down on the number of measurements required.

To do so, we observe that we may simultaneously measure any set of Pauli operators which are simultaneously diagonalizable. As shown in our Diagonalization Algorithm, we are able to simultaneously diagonalize any commuting set of Pauli operators. This shows that partitioning our Pauli operators into commuting parts may provide a time save for the variational quantum eigensolver.

This is a topic which has been investigated in previous literature, and we describe the "greedy algorithm" which has been used in previous implementations of the variational quantum eigensolver.

Definition 18 Given two Pauli operators, $\left(\boldsymbol{x_1} \mid \boldsymbol{z_1}\right)$ and $\left(\boldsymbol{x_2} \mid \boldsymbol{z_2}\right)$, we say that:

- $\left(\boldsymbol{x_1} \mid \boldsymbol{z_1}\right)$ is a subset of $\left(\boldsymbol{x_2} \mid \boldsymbol{z_2}\right)$ if $\boldsymbol{x_1}(i) \in \{0, \boldsymbol{x_2}(i)\}$ and $\boldsymbol{z_1}(i) \in \{0, \boldsymbol{z_2}(i)\}$

- $\left(\boldsymbol{x_1} \mid \boldsymbol{z_1}\right)$ is a superset of $\left(\boldsymbol{x_2} \mid \boldsymbol{z_2}\right)$ if $\boldsymbol{x_2}(i) \in \{0, \boldsymbol{x_1}(i)\}$ and $\boldsymbol{z_2}(i) \in \{0, \boldsymbol{z_1}(i)\}$ □

Definition 19 Given a set of Pauli operators, $\mathcal{S}$, the **greedy algorithm** partitions the operators into commuting sets as follows:

1. choose an ordering of the elements of $\mathcal{S}$
2. for each P (considered in order), we do the following:
   - if there exists a part which contains a superset of P, then add P to that part
   - if there exists a part which contains only subsets of P, then add P to that part
   - otherwise, create a new part consisting only of P. □

This notion of subsets and supersets is a little difficult to compare to our above algorithm, so we generalize it slightly. We define bitwise commutation as follows.

Definition 20 Given two Pauli operators, $\left(\boldsymbol{x_1} \mid \boldsymbol{z_1}\right)$ and $\left(\boldsymbol{x_2} \mid \boldsymbol{z_2}\right)$, we say that these operators **bitwise commute** if $\left(\boldsymbol{x_1}(i) \mid \boldsymbol{z_1}(i)\right) \odot \left(\boldsymbol{x_2}(i) \mid \boldsymbol{z_2}(i)\right) \equiv 0 \pmod{q}$, for all i. □

It is fairly easy to check that, if an operator is either a subset or a superset of another operator, then they bitwise commute. Furthermore, if two operators bitwise commute, then they commute in the usual sense. As such, it should be clear that an algorithm which uses a less-strict requirement for adding an operator to a part should result in fewer parts. To see just how much of an improvement we can expect from using the general notion of commutation, though, we shall compare it to an algorithm which uses bitwise commutation.

As we did before, we could generate a graph which represents anti-bitwise-commutation between the Pauli operators in our set. Analyzing an optimal coloring of this graph gives us an expected number of parts in a partition.

Conjecture 2 *Given $\mathcal{S} \subseteq \mathcal{P}_q^*$, we expect the number of parts in a minimal partition of $\mathcal{S}$ (with respect to bitwise commutation) to be bounded below by:*

$$\left(\frac{1}{2} + o(1)\right) m(\log_2(q) - o(1)) \frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)},$$

where m is the length of the largest Pauli operator in $\mathcal{S}$.

PROOF We shall first look at the probability that any two operators, P_i and P_j, chosen from $\mathcal{P}_q^m$ will bitwise commute. This requires that each bit should commute, which happens with probability $(q^3+q^2-q)/q^4$. Thus, the probability that these operators bitwise commute is $((q^3+q^2-q)^m - q^{2m})/(q^4)^m$.

The anti-bitwise-commutation graph will therefore have edge probability $1-(q^3+q^2-q)^m/(q^4)^m$, although the edge probabilities will likely not be independent. If they were independent, we would find the number of parts to be:

$$\begin{aligned}
&\left(\frac{1}{2}+o(1)\right)\log_2\left(\frac{1}{1-\left(1-\frac{(q^3+q^2-q)^m}{(q^4)^m}\right)}\right)\frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}\\
&=\left(\frac{1}{2}+o(1)\right)\log_2\left(\frac{(q^4)^m}{(q^3+q^2-q)^m}\right)\frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}\\
&=\left(\frac{1}{2}+o(1)\right)m\log_2\left(\frac{q^4}{q^3+q^2-q}\right)\frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}\\
&=\left(\frac{1}{2}+o(1)\right)m\left(\log_2(q)-o(1)\right)\frac{|\mathcal{S}|}{\log_2(|\mathcal{S}|)}.
\end{aligned}$$

Without the independence of these edge probabilities, however, it is difficult to give a concrete lower bound on the number of colors we should expect using bitwise commutation. ∎

Running with our conjectures, however, we compare this to Conjecture 1 and observe that the expected number of parts is roughly m times more using bitwise commutation rather than general commutation. Since the greedy algorithm considers a partition requirement which is even stronger than bitwise commutation, graph coloring algorithms would greatly improve upon existing partitioning techniques.

We have seen these conjectured results borne out on small examples, and are excited to continue testing their validity on larger Hamiltonians.

Chapter 6

Conclusion and Open Problems

In this thesis, we have covered a lot of ground with regard to partitioning Pauli operators. In particular, we have shown that minimal partitions of $\mathcal{P}_q^n$ always exist, leading to a proof of the existence of a set of $q^n + 1$ mutually unbiased bases in $\mathbb{C}^{q^n}$. Moreover, we have shown that the problem of partitioning Pauli operators is equivalent in complexity to the problem of coloring graphs, and that implementing graph coloring algorithms should significantly reduce the number of measurements required in each quantum step of the variational quantum eigensolver. We provide some launching off points for future research for interested readers.

First, we believe this to be the first construction of mutually unbiased bases from Singer cycles. While this construction has not led to the discovery of any new mutually unbiased bases, we hope it may prove useful for investigations into the still-open problem of mutually unbiased bases over composite (non-prime power) dimensions. In particular, we are interested to see whether all mutually unbiased bases over prime powers may be constructed from Singer cycles, and the lack of the existence of Singer cycles over non-prime power dimensions may provide insight into why maximal sets of mutually unbiased bases may not exist.

Second, another approach to speeding up the variational quantum eigensolver would be to find a similar matrix with a more simple expression as a sum over Pauli operators. For instance, if one could efficiently calculate the diagonalization of H (i.e. write a matrix similar to H as a sum over all diagonal Pauli matrices), then all measurements could be performed simultaneously, saving a significant amount of time. This, or similar approaches, would allow for significantly faster and more reliable computations. The variational quantum state diagonalization [7] algorithm does exactly this, but it already requires more

quantum resources than the variational quantum eigensolver. Perhaps a hybrid algorithm which mostly diagonalizes H before applying the variational quantum eigensolver could require fewer quantum resources.

Third, while we showed the equivalence between partitioning Pauli operators and coloring graphs, we did not make mention of specific graph coloring algorithms. This is because, as was mentioned many a time through Chapters 4 and 5, the graphs are not truly random. In fact, for most applications, the set of Pauli operators, itself, will not be random, since it will be the output of an algorithm for mapping a Hamiltonian onto qubits (e.g. the Bravyi-Kitaev transformation, or perhaps the Jordan-Wigner transformation). With more insight into the structure of the molecule, the outputs of these transformations, or the relations between the Pauli terms, a specific coloring algorithm could be chosen or designed for each application. In special cases, one could imagine that optimal colorings could be calculated efficiently.

References

[1] Samshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, November 2002.

[2] Béla Bollobás. The chromatic number of random graphs. *Combinatorica*, 8(1):49–55, March 1988.

[3] Joel V. Brawley and Timothy C. Teitloff. Similarity to symmetric matrices over finite fields. *Finite Fields and Their Applications*, 4(3):261–274, July 1998.

[4] Hector García, Igor Markov, and Andrew Cross. On the geometry of stabilizer states. *Quantum Information and Computation*, 14(7-8):683–720, 2014.

[5] Pranav Gokhale, Olivia Angiuli, Yongshan Ding, Kaiwen Gui, Teague Tomesh, Martin Suchara, Margaret Martonosi, and Frederic T. Chong. Miminizing state preparations in variational quantum eigensolver by partitioning into commuting families. *arXiv*, 2019.

[6] Daniel Gottesman. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos, Solitons & Fractals*, 10(10):1749–1758, 1999.

[7] Ryan LaRose, Arkin Tikku, Étude O'Neel-Judy, Lukasz Cincio, and Patrick J. Coles. Variational quantum state diagonalization. *NPJ Quantum Information*, 5(57), 2019.

[8] Jarrod R. McClean, Jonathan Romero, Ryan Babbush, and Alán Aspuru-Guzik. The theory of variational hybrid quantum-classical algorithms. *New Journal of Physics*, 18, 2015.

[9] Morris Newman. Two classical theorems on commuting matrices. *Journal of Research of the National Bureau of Standards - B. Mathematics and Mathematical Physics*, 71B(2 and 3), April 1967.

[10] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J Love, Alán Aspuru-Guzik, and Jeremy L O'Brien. A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 5(4213), 2014.

[11] Tzu-Ching Yen, Vladyslav Verteletskyi, and Artur F. Izmaylov. Measuring all compatible operators in one series of a single-qubit measurements using unitary transformations. *arXiv*, 2019.

Diagonalization Algorithm

We define the operators which act by conjugation on q-ary Pauli gates as follows:

$$\begin{aligned} F_q : X_q &\mapsto Z_q \\ Z_q &\mapsto X_q^{-1} \end{aligned}$$

$$\begin{aligned} R_q : X_q &\mapsto X_q Z_q \\ Z_q &\mapsto Z_q \end{aligned}$$

$$\begin{aligned} SUM_q : \mathbb{1}_q X_q &\mapsto \mathbb{1}_q X_q \\ X_q \mathbb{1}_q &\mapsto X_q X_q \\ \mathbb{1}_q Z_q &\mapsto Z_q^{-1} Z_q \\ Z_q \mathbb{1}_q &\mapsto Z_q \mathbb{1}_q. \end{aligned}$$ [6]

We shall use without proof the fact that these gates generate the generalized Clifford group, the set of operators which permutes the elements of $\mathcal{P}_q$. We shall give an inductive proof which can be used as an iterative algorithm to construct the specific Clifford gate which simultaneously diagonalizes a set of commuting Pauli operators.

Lemma 4 *Let $\mathcal{C}$ be a set of commuting Pauli operators. There exists a Clifford gate, G, such that $G\mathcal{C}G^\dagger = \{GPG^\dagger : P \in \mathcal{C}\} \subseteq \left\{\bigotimes_{i=1}^n X_q^0 Z_q^{j_i} : j_i \in \mathbb{Z}/q\mathbb{Z}\right\}$.* □

Proof We shall prove this by induction on the length of the Pauli operators, n.

- $n = 1$: If $\mathcal{C} \subseteq \mathcal{P}_q$ is not diagonalized, then there exists some operator, $P \in \mathcal{C}$, with a non-zero X-component. We shall write $P = X_q^a Z_q^b$ for some $a \not\equiv 0 \pmod q$. Let:

$$G_1 = R_q^{a^{-1}(q-b)}$$

where a^{-1} is the multiplicative inverse of a over $\mathbb{Z}/q\mathbb{Z}$.

By our conjugation rules above, we observe that:

$$G_1 P G_1^\dagger = X_q^a Z_q^b Z_q^{a(a^{-1}(q-b))} = X_q^a Z_q^b Z_q^{q-b} = X_q^a Z_q^q = X_q^a.$$

We have successfully removed the Z-component of this Pauli operator, but we want to remove the X-component, so we let $G = F_q G_1$. Again, following our conjugation rules, we observe that:

$$GPG^\dagger = F_q G_1 P G_1^\dagger F_q^\dagger = F_q X_q^a F_q^\dagger = Z_q^a.$$

Thus, we have successfully diagonalized a single element of $\mathcal{C}$. However, since conjugation by Clifford gates preserves commutation relations, we know that $G\mathcal{C}G^\dagger$ must still pairwise commute. Since there exists an operator with no X-component on the one and only qudit, all operators in $G\mathcal{C}G^\dagger$ must have no X-component. Thus, we have successfully diagonalized the set.

- $n > 1$: Assume we are able to successfully diagonalize any commuting set of Pauli operators on $n-1$ qudits. If $\mathcal{C} \subseteq \mathcal{P}_q^n$ is not already diagonalized, there exists some operator, $P \in \mathcal{C}$, with a nonzero X-component. Let H_1 be a SUM_q gate from a qudit with a nonzero X-component to the first qudit in our tensor product, we may now assume that $H_1 P H_1^\dagger = X_q^a Z_q^b \otimes P_1$ for some $a \not\equiv 0 \pmod q$ and some $P' \in \mathcal{P}_q^{n-1}$.

  We take advantage of our above proof and left-multiply our H_1 by the gate which acts only on the first qudit and diagonalizes it as in our base case (let's call this gate H_2). This leaves us with: $H_2 H_1 P H_1^\dagger H_2^\dagger = Z_q^a \otimes P_2$.

  Next, P_2 may have some qudits with a nonzero Z-component. Let H_3 be a series of SUM_q gates from these qudits to the first qudit, applying the gate as many times as is necessary to cancel out the Z-component. This leaves us with: $H_3 H_2 H_1 P H_1^\dagger H_2^\dagger H_3^\dagger = Z_q^a \otimes P_3$.

  P_3 has no Z-component, but my have some qudits with a nonzero X-component. We address this by letting H_4 be the $(n-1)$-fold F_q gate applied to the last $n-1$ qudits, leaving us with: $H_4 H_3 H_2 H_1 P H_1^\dagger H_2^\dagger H_3^\dagger H_4^\dagger = Z_q^a \otimes P_4$.

  P_4 has no X-component, but may have some qudits with nonzero Z-component. Using the same strategy as in constructing H_3, we use SUM_q gates to cancel out this Z-component, finally leaving us with: $H_5 H_4 H_3 H_2 H_1 P H_1^\dagger H_2^\dagger H_3^\dagger H_4^\dagger H_5^\dagger = Z_q^a \otimes \mathbb{1}_{q^{n-1}}$.

  Letting G_1 denote this product of Clifford gates we have constructed, we observe that every operator in $G_1 \mathcal{C} G_1^\dagger$ must commute with $Z_q^a \otimes \mathbb{1}_{q^{n-1}}$. This means that every operator in $G_1 \mathcal{C} G_1^\dagger$ must have no X-component in the first qudit.

Restricting ourselves to Clifford group operations on the last $n-1$ qudits, we already know by our inductive hypothesis that there exists a Clifford gate, G_2, which simultaneously diagonalizes the remaining $n-1$ qudits of $G_1 \mathcal{C} G_1^\dagger$, without affecting the first qudit.

In conclusion, every operator in $G_2 G_1 \mathcal{C} G_1^\dagger G_2$ has no X-component on every qudit. Thus, $G = G_2 G_1$ is a Clifford gate which diagonalizes $\mathcal{C}$. ∎

X-ization Algorithm

If we have used the Diagonalization Algorithm to diagonalize one of the parts of a minimal partition, every Pauli operator in the remaining non-diagonal parts will have non-zero X component. We shall provide an algorithm which uses only SUM_q and R_q gates to remove the Z component of one of these parts without disturbing the already-diagonalized part. This will allow us to assume that, WLOG, a minimal partition contains both $\left(0_n \mid \mathbb{1}_n\right)$ and $\left(\mathbb{1}_n \mid 0_n\right)$.

Lemma 5 *Let $\mathcal{C}$ be a set of commuting Pauli operators which each has non-zero X component. There exists a Clifford gate, G, composed of only SUM_q and R_q gates, such that $G\mathcal{C}G^\dagger = \{GPG^\dagger : P \in \mathcal{C}\} \subseteq \left\{\bigotimes_{i=1}^n X_q^{j_i} Z_q^0 : j_i \in \mathbb{Z}/q\mathbb{Z}\right\}$.* □

Proof We first notice that, by using only SUM_q and R_q gates, we cannot transform a matrix with non-zero X component into one which has a zero X component, and vice versa. This is because R_q does not change the X component and SUM_q cannot take $X_q^i X_q^j$ to $X_q^0 X_q^0$, for any i, j which are not both 0.

Having noticed this, we begin by a proof by induction, similar to the previous step.

- $n = 1$: Since $\mathcal{C} \subseteq \mathcal{P}_q$ has a non-zero X-component, we observe that any two Pauli operators, $P_1 = X_q^a Z_q^b, P_2 = X_q^c Z_q^d \in \mathcal{C}$ must satisfy $ad - bc \equiv 0 \pmod q$ (since they commute). Therefore, applying $R_q^{-a^{-1}b}$ results in:
  - $R_q^{-a^{-1}b} X_q^a Z_q^b = X_q^a Z_q^b Z_q^{a(-a^{-1}b)} = X_q^a Z_q^b Z_q^{-b} = X_q^a Z_q^0$
  - $R_q^{-a^{-1}b} X_q^c Z_q^d = X_q^c Z_q^d Z_q^{c(-a^{-1}b)} = X_q^c Z_q^{d-a^{-1}cb} = X_q^c Z_q^{(ad-cb)(a^{-1})} = X_q^c Z_q^0$.

  In other words, the same operator (which is well-defined since $a \neq 0$) transforms all of these matrices into matrices with no Z component, as required.

- $n > 1$: Assume we are able to successfully cancel out the Z component of any set of Paulis satisfying our conditions on $n-1$ qudits.

  Choosing an operator, $P = \left(\boldsymbol{x} \mid \boldsymbol{z}\right)$, with non-zero X component, we note that there exists a sequence of SUM_q gates, U_1, such that $U_1 P U_1^\dagger = \left(-\boldsymbol{z} \mid \boldsymbol{z}\right)$. Applying R_q to this, we see that $R_q U_1 P U_1^\dagger R_q^\dagger = \left(-\boldsymbol{z} \mid \mathbf{0}\right)$. We similarly notice that there exists a sequence of SUM_q gates, U_2, such that $U_2 R_q U_1 P U_1^\dagger R_q^\dagger U_2^\dagger = \left(1 \;\; 0 \;\; \ldots \;\; 0 \mid 0 \;\; 0 \;\; \ldots \;\; 0\right)$.

  Thus, we have mapped P to $\left(1 \;\; 0 \;\; \ldots \;\; 0 \mid 0 \;\; 0 \;\; \ldots \;\; 0\right)$. Since every operator in $\mathcal{C}$ must still commute with this vector, we observe that every operator must have Z_q^0 in the first qubit. Having done this, we may restrict our attention to the last $n-1$ qubits and the operators which have non-zero X-component on this set. By induction, we may remove the Z component of these operators. Combining these results, we end up with a set of gates which removes the Z component of all of $\mathcal{C}$, as required. ∎