MEASUREMENT BASED QUANTUM COMPUTING

MICHAEL WHITMEYER AND JAMES CHEN

1. Introduction

In the standard circuit-based model of quantum computing, we initialize a product state of all $|0\rangle$s, perform the algorithm as an encoded sequence of 1-qubit and 2-qubit gates, and then measure in a standard basis. On the other hand, in measurement-based quantum computing, we initialize an entangled state, and the algorithm is encoded as a sequence of adaptive measurements (i.e. measurements whose bases depend on the result of previous measurements). In Section 2, we will describe teleportation-based quantum computing, a canonical example of the measurement-based model [Jos05]. In Section 3, we will examine some motivations for speedups for measurement-based models, and apply these motivations to speed up Clifford operations. In Section 4, we will investigate one-way quantum computing, another canonical example of the measurement-based model [Jos05]. Finally, in Section 5 we will discuss the general computational complexity of measurement-based models and important reductions between quantum computing models [Bro10].

2. An Example: Teleportation-Based Quantum Computation

Teleportation-based quantum computing implements unitary operations by using a variation of the standard teleportation protocol. Informally, a 1-qubit unitary U is applied to a state $|\psi\rangle$ by using the protocol and measuring in a rotated basis to teleport $U|\psi\rangle$ instead of just $|\psi\rangle$. Similarly, a CNOT under the teleportation-based protocol is roughly implemented by teleporting two qubits, but with the two Bell pairs initially entangled. We describe both of these implementations in further detail below. Showing that arbitrary 1-qubit unitaries and CNOT can be implemented in the teleportation-based model is sufficient to conclude that the model is universal.

2.1. **Teleporting an Arbitrary 1-Qubit Gate.**

Recall the standard Bell Basis:

$$|B_{00}\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|B_{10}\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|B_{01}\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|B_{11}\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Now we consider the rotated (but still orthogonal and perfectly valid) basis $\mathcal{B}(U) = \{|B(U)_{cd}\rangle\}$, where $|B(U)_{cd}\rangle = (U^\dagger \otimes I)B_{cd}$. Then, instead of measuring in the Bell basis before teleportation, the idea is we measure in this new basis $\mathcal{B}(U)$. This is equivalent to applying U to our top qubit

Date: Dec 10th, 2019.

(the one being teleported) before teleporting, but it is important to note here that we are not ever actually applying a unitary, only measuring in a clever basis. After performing the teleportation scheme in this manner, our target qubit has the state $X^d Z^c U|\psi\rangle$. Then, we simply correct our Pauli errors as needed based on what we have measured, exactly as in the standard teleportation algorithm. We rigorously justify these ideas in the appendix in general with qudits.

2.2. **Teleporting a CNOT gate.** Consider Figure 1. Given two Bell pairs entangled with a CNOT ($|\chi\rangle$), we first apply the standard teleportation protocol. Informally, we can think of the CNOT entangling the Bell pairs as conjugating with the Pauli corrections out to the right hand side of Figure 1, where we can think of it as being applied on the teleported states $|\alpha\rangle$ and $|\beta\rangle$. The X and Z corrections conjugate with the CNOT as follows:

$$\begin{aligned}
\mathrm{CNOT}(X \otimes I) &= (X \otimes X)\mathrm{CNOT} \\
\mathrm{CNOT}(I \otimes X) &= (I \otimes X)\mathrm{CNOT} \\
\mathrm{CNOT}(Z \otimes I) &= (Z \otimes I)\mathrm{CNOT} \\
\mathrm{CNOT}(I \otimes Z) &= (Z \otimes Z)\mathrm{CNOT}
\end{aligned}$$

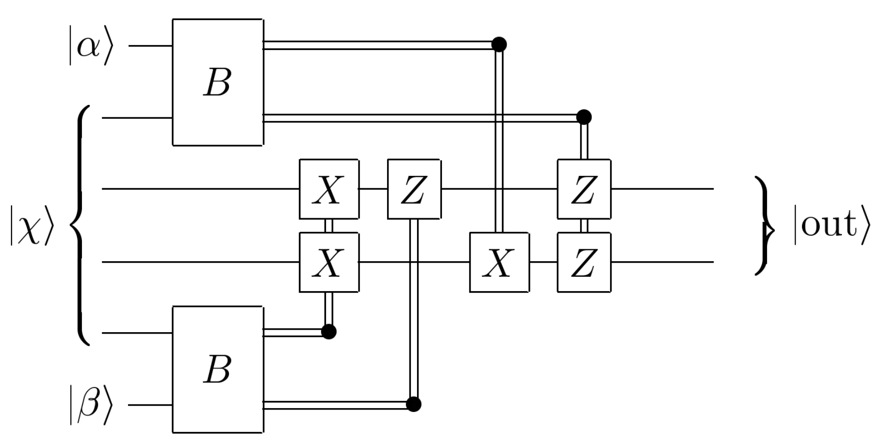

FIGURE 1. Teleporting a CNOT ($|\mathrm{out}\rangle = \mathrm{CNOT}\,|\beta\rangle\,|\alpha\rangle$).

It remains to justify the creation of $|\chi\rangle$, since we cannot apply the entangling CNOT gate. However, if we expand our initial resource state to allow 3-qubit GHZ states $|\Upsilon\rangle$, then we can create $|\chi\rangle$ using the sequence of gates shown in Figure 2.

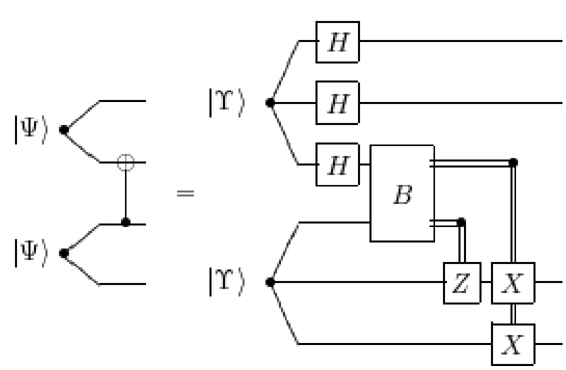

FIGURE 2. Creating $|\chi\rangle$ from GHZ resource states $|\Upsilon\rangle$ and 1-qubit gates.

3. Adaptive Measurements and the Parallelizability of Clifford Operations

3.1. **Adaptive Measurements.** One apparent advantage of measurement-based models is that since measurements are performed on separate qubits, it might be possible to perform them simultaneously. However, this is not possible in general. Suppose we wish to perform the computation $U_2U_1 |\psi\rangle$, where each U_i is a 1-qubit unitary. In the teleportation-based model described previously, we achieve this by measuring in the Bell basis $M_{\mathcal{B}(U_i)}$ and then applying Pauli corrections P_i. If tried to measure our qubits transversally and apply no intermediate Pauli corrections, our final state would be $P_2U_2P_1U_1 |\psi\rangle$, which almost always cannot be corrected to yield $U_2U_1 |\psi\rangle$.

For example, take $U_1 = R_x(\theta)$ and $U_2 = R_z(\eta)$. Then using the conjugation relations between Pauli operators and arbitrary X and Z rotations, our final state with transversal measurement is

$$X^cZ^dR_z(\eta)X^aZ^bR_x(\theta) |\psi\rangle = X^cZ^dX^aZ^bR_z((-1)^c\eta)R_x(\theta) |\psi\rangle .$$

After corrections, we have the state $R_z((-1)^c\eta)R_x(\theta) |\psi\rangle$ which cannot be transformed to the desired state $R_z(\eta)R_x(\theta) |\psi\rangle$ by simple Pauli operators. We can avoid this problem with adaptive measurements, teleporting $R_z((-1)^c\eta)$ instead of $R_z(\eta)$ after determining c:

$$X^cZ^dR_z((-1)^c\eta)X^aZ^bR_x(\theta) |\psi\rangle = X^cZ^dX^aZ^bR_z(\eta)R_x(\theta) |\psi\rangle .$$

3.2. **Parallelizing Clifford Gates.**

Definition 1. *A gate is* ***Clifford*** *if it preserves the Pauli group under conjugation. Mathematically,* $\mathcal{C} = \{C|C^\dagger PC \in \mathcal{P}\}$*. Alternatively, a unitary* C *is Clifford is* $CP = P'C$ *for Paulis* P, P'*.*

What was fundamentally forcing us to perform these adaptive measurements? Phrased a different way, what was preventing us from performing all of these measurements in parallel? It stems from the fact that most unitaries are not Clifford. But what if all our unitaries that we want to apply happen to be Clifford?

We have the follwing theorem from Josza [Jos05]:

Theorem 2. *Any Clifford circuit can be simulated by a constant depth measurement process (quantum computation), along with some log depth classical processing.*

Proof. If all our gates are Clifford, then our computation looks something like $P_kC_k \cdots P_2C_2P_1C_1|\psi\rangle$. But the fact that all the C_i's are Clifford tells us we can effectively "commute" them all over to the right (and we know exactly how each Clifford conjugates with each Pauli), to yield $X_n^{a_n}Z_n^{b_n} \cdots X_1^{a_1}Z_1^{b_1}C_n \cdots C_1|\psi\rangle$. Each of the a_i and b_i are determined by both the conjugation relationships as well as the measurement outcomes. This means we can perform all of our measurements in parallel, which tells us that the entire operation requires only *constant* quantum depth! But there is a catch: we need to classically compute each of the a_i and b_i terms. The key here is to note that each of these terms is a bitwise sum of some measurement outcomes $a_i = i_1 \oplus \cdots \oplus i_k$, which can be computed log depth by first computing $i_1 \oplus i_2$ and $i_3 \oplus i_4$ and so on in parallel, and then proceeding to the next layer. All of these calculations can be parallelized, for a total of log depth classical computation. $\square$

4. One-way Quantum Computation

In this section we will briefly introduce one-way quantum computation. Unlike the measurement-based model, the initial entangled state is not a collection of Bell pairs, but instead a cluster state formed by initializing a 2D grid of qubits to the state $|+\rangle$ and performing transversal controlled-Z operations between every neighboring pair of qubits.

4.1. Implementing an Arbitrary 1-Qubit Gate.

We can implement an arbitrary 1-qubit gate $U = R_x(\zeta)R_z(\eta)R_x(\xi)$ as in Figure 3.

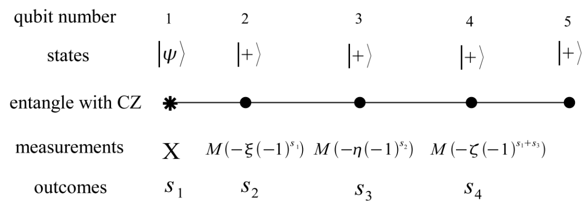

Figure 3. Creating $|\chi\rangle$ from GHZ resource states $|\Upsilon\rangle$ and 1-qubit gates.

In Figure 3, the final state on the rightmost qubit is $X^{s_2+s_4}Z^{s_1+s_3}U\,|\psi\rangle$. Applying the appropriate X and Z Pauli corrections will yield the desired state $U\,|\psi\rangle$.

4.2. Implementing a CZ gate.

We can also implement a controlled-Z gate as in Figure 4.

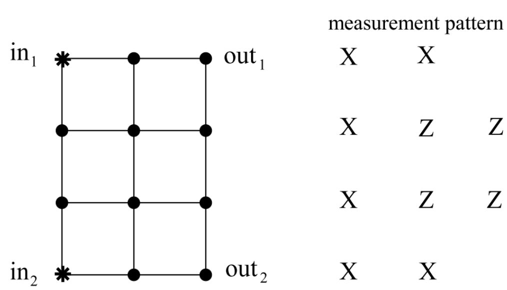

Figure 4. Creating $|\chi\rangle$ from GHZ resource states $|\Upsilon\rangle$ and 1-qubit gates.

As with the implementation of our 1-qubit unitary, Pauli corrections may need to be applied to both output qubits.

5. MBQC Computational Complexity

To investigate the computational complexity of measurement-based models, we consider a new primitive based on the one-way model, another canonical example of measurement-based quantum computing. A *measurement pattern* (MP) is a sequence of commands, where commands consist of:

- $CZ_{i,j}$: Controlled-Z gates for entangling qubits.
- $M_i(\theta)$: Measurements of qubit i in $\{|0\rangle \pm e^{i\theta}\,|1\rangle\}$ basis.
- X_i^s, Z_i^s: Dependent corrections of qubit i based on results of previous qubits (i.e. $s_1, \ldots, s_k$), where $s = s_1 + \cdots + s_k$.

Recall that for a quantum circuit C, the *size* of C is the number of gates in C and the *depth* of C is the longest path of gates. Similarly, we take the *size* of a measurement pattern t to be the number of commands in t and *depth* of t to be the longest path of dependent commands in t.

5.1. **Equivalence between MPs and Quantum Circuits.**

Lemma 3. *Any quantum circuit C can be simulated by a MP of size $O(size(C))$ and depth $O(depth(C))$.*

Proof. As shown in Section 4, each 1-qubit gate in C can be implemented as a measurement pattern with a 6-fold increase in depth and size, corresponding to the 4 measurements and the 2 corrections (X and Z) needed to yield the state $U|\psi\rangle$ on the final qubit. Moreover, each CNOT can be implemented with a 14-fold increase in size and a 3-fold increase in depth, corresponding to the 1 transversal set of 10 measurements and the 2 pairs of corrections (X and Z on each output qubit). $\square$

Lemma 4. *Any MP t can be simulated by a quantum circuit of size $O(size(t)^3)$ and depth $O(depth(t)\log(size(t)))$.*

These two lemmas hint at a depth separation between the circuit model and measurement patterns in some cases which is logarithmic in the size of the measurement pattern. For example,

$$U^{(n)}_{\text{PARITY}} : |x_1, x_2, \ldots, x_n\rangle \to \left| x_1, x_2, \ldots, \bigoplus_{i=1}^{n} x_i \right\rangle$$

requires a $\log(n)$-depth circuit simulation ([BK07]). However, it is a Clifford operation, so it is simulatable by a constant-depth MP. We pin down this separation more in the next subsection by establishing an equivalence between MPs and circuits with unbounded fan-out.

5.2. **Equivalence between MPs and Quantum Circuits with Unbounded Fan-out.**

Definition 5 (Fan-out)**.** $U^{(n)}_{FANOUT} := |y_1, ..., y_{n-1}, x\rangle \to |y_1 \oplus x, ..., y_{n-1} \oplus x, x\rangle$

Theorem 6 ([Bro10])**.** *Any circuit C with unbounded fan-out can be simulated by a measurement process (MP) of depth $O(depth(C))$. Similarly, any MP t can be simulated by a circuit with unbounded fan-out of depth $O(depth(t))$.*

Proof. We first show that there is a depth-preserving transformation from unbounded fan-out circuits to measurement patterns. The unbounded fan-out gate is Clifford and thus can be implemented by a constant depth measurement pattern. Moreover, there exists a depth-preserving transformation for all non-fan-out gates by Lemma 3.

We then show that there is a depth-preserving transformation from measurement patterns to unbounded fan-out circuits. We decompose the measurement pattern into $k = depth(t)$ layers, each of which has entangling operations, measurements, X-corrections, and Z-corrections. We show that each type of command within a layer can be done in constant depth:

- The entangling operations CZ can be done in constant depth in a quantum circuit since the CZ gates all commute.
- The measurements can also be done in constant depth since we can simultaneously apply gates to rotate each qubit into the standard basis and then use the safe storage technique (applying CNOTs between desired qubits and ancilla initialized to $|0\rangle$ effectively measures the desired qubits).

- Each dependent Z-correction can be transformed into a sequence of controlled Z gates, where the control qubits correspond to the measurement results that the Z-correction depends upon. Although this sequence of CZs is not of constant depth, the overall unitary formed by the composition of this sequence is diagonal. Moore and Nilsson showed that for pairwise commuting unitaries U_i, a sequence of controlled-U_i gates can be implemented by a constant depth measurement pattern. Hence our layer of dependent Z-corrections can be implemented in constant depth.
- Each dependent X-correction can be transformed into a Z-correction by applying a Hadamard transformation to the relevant qubit, which is at most a constant increase in depth. Then our constant-depth implementation of Z-corrections can be applied.

□

This theorem is especially powerful for two reasons:

- First, it allows us to immediately apply results of quantum circuits with unbounded fan-out to measurement patterns. For example, QFT and factoring can be done by constant depth circuits with unbounded fan-out with bounded error, and so can also be done by constant depth measurement patterns with bounded error.
- Second, it expresses the power of measurement-based quantum computing in terms of a gate in the circuit model. It was not immediately evident before this result that such a simple connection existed.

6. Conclusion

Measurement based quantum computing is a fundamentally new way to view not just quantum information processing, but computing in general. Unlike the circuit based model, there is no known classical analogue for MBQC in the classical world; it fundamentally relies on the properties of quantum mechanics. There is also a very nice connection [Got99] between the measurement based schemes we have described above and the stabilizer error correcting codes we have learned about in class. In both quantum error correction and quantum teleportation, quantum information after a partial measurement is preserved only in a subspace of the original system. In both applications, our data is transformed within this subspace, but this transformation is indexed by our measurement outcome and is therefore able to be corrected. When we generalize to teleporting a gate, rather than a state, we are simply changing what subspace is being preserved in a clever, allowing us to implement a unitary by only applying measurements.

In this review we investigated the teleportation-based model, one of the canonical examples of measurement-based quantum computing. From there, we showed how Clifford circuits can actually be computed in constant quantum depth and log classical depth using MBQC. Lastly, we introduced the one-way model and demonstrated equivalence between this model the circuit model with unbounded fan-out. We have seen how MBQC is universal and moreover can potentially offer some advantages over the circuit model for algorithms that require large fan-out.

7. References

[Bro10] Kashefi E. Perdrix S. Browne D. "Computational depth complexity of measurement-based quantum computation". In: *Theory of Quantum Computation, Communication and Cryptography* 1 (2010)), pp. 1–10.

[Got99] Chuang I. Gottesman D. "Quantum teleportation as a universal computational primitive". In: *Nature* 1 (1999), pp. 1–10.

[Jos05] R. Josza. "An Introduction to Measurement Based Quantum Computing". In: *Quantum Information Processing* 1 (2005), pp. 1–15.

8. Appendix

8.1. **Teleportation.** The following lemmas prove the standard teleportation protocol on qudits and the teleportation of a 1-qudit unitary using a rotated basis.

Lemma 7. *Let* $|\phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle$ *be the maximally entangled state in* d *dimensions, and let* $|\alpha\rangle = \sum a_j|j\rangle$*. Then projecting* $|\alpha\rangle_1|\phi\rangle_{23}$ *onto* $|\phi\rangle_{12}$ *results in the state* $\frac{1}{d}|\alpha\rangle_3$ *on qubit 3.*

Proof. We have that the projection is

$$\frac{1}{d}\left(\sum \langle i|\langle i| \sum_{j,k} a_j|j\rangle|k\rangle|k\rangle\right) = \frac{1}{d}\sum_{i,j,k} a_j\delta_{ij}\delta_{ik}|k\rangle = \frac{1}{d}\sum_{k} a_k|k\rangle$$

□

We have a very similar result for teleporting a unitary, which serves as a proof of the claim about that measuring in our rotated Bell Basis $\mathcal{B}(U)$ does in fact teleport the unitary U. We let $|\phi(U)\rangle = (U^\dagger \otimes I)|\phi\rangle$. Then we have the following lemma:

Lemma 8. *Projecting* $|\alpha\rangle_1|\phi\rangle_{23}$ *onto* $|\phi(U)\rangle_{12}$ *results in the state* $\frac{1}{d}U|\alpha\rangle_3$ *on qubit 3.*

Proof. We have our projection is

$$\frac{1}{d}\left(\sum \langle i|\langle i|U \sum_{j,k} a_j|j\rangle|k\rangle|k\rangle\right)$$
$$= \frac{1}{d}\left(\sum \langle i|\langle i| \sum_{j,k} b_j|j\rangle|k\rangle|k\rangle\right)$$

where $\sum b_j|j\rangle := U\sum a_j|j\rangle$. Then, continuing our analysis in the same manner as before, we are left with the state

$$\frac{1}{d}\sum_{i,j,k} b_j\delta_{ij}\delta_{ik}|k\rangle = \frac{1}{d}\sum_{k} b_k|k\rangle = \frac{1}{d}U\alpha$$

□