qitd463

Measurement-Based Quantum Computation

Robert B. Griffiths
Version of 22 April 2014

Contents

References:

A. M. Childs, D. W. Leung and M. A. Nielsen, "Unified deprivations of measurement-based schemes for quantum computation," Phys. Rev. A 71 (2005) 032318; arXiv:quant-ph/0404132.

D. E. Browne and H. J. Briegel, "One-way Quantum Computation," arXiv:quant-ph/0603226

M. A. Nielsen, "Cluster-state quantum computation," Reports on Mathematical Physics 57 (2006) 141; arXiv:quant-ph/0504097v2

R. Raussendorf and H. J. Briegel, "A one-way quantum computer," Phys. Rev. Lett. 86 (2001) 5188 (The original paper)

S. C. Benjamin, B. W. Lovett, J. M. Smith "Prospects for measurement-based quantum computing with solid state spins," Laser and Photonics Reviews 3 (2009) 556; arXiv:0901.3092v2 [quant-ph]

1 Introduction

★ The "circuit" scheme of quantum computation employs a number of qubits which are initially in a product state and then are subjected to various one and two-qubit gates before being measured. By contrast, the measurement-based scheme (also called "cluster state computation" and "one-way computation") assumes a collection of qubits that are initially entangled with each other in a suitable graph state. Some of these qubits are measured in particular bases, after which others are measured in other bases which, in general, are chosen in a way that depends upon the outcomes of the first series of measurements, after which still others are measured, etc. At the end the final measurement outcomes are the same, or at least can be interpreted to yield the same results, as in the circuit model. However, the perspective is quite different. In particular, after completing the initial procedures required to produce the entangled graph state no further quantum gates of any kind are required; the whole process that remains can be carried out by successive measurements in appropriately chosen bases.

• By now there is a substantial literature on measurement-based schemes. Of the references given above, probably the most accessible is the one by Nielsen.

★ The main purpose of the following notes is to clarify some points that occasionally give rise to confusion. In particular, in order to understand what is going on it is sometimes useful to think of measurements and entangling operations carried out in a different order from that in which all entangling operations are carried out first, and all measurements are carried out later.

2 Single Pair

★ The place to begin is with a single pair of qubits, 1 and 2, each of which is initially in a $|+\rangle$ state, the eigenstate of the Pauli X operator with eigenvalue $+1$. After this a controlled-phase or CP gate that carries out the unitary operator C_{12} is applied to the two qubits to produce a graph state corresponding to a graph in which the two vertices are connected by an edge.

○ See the notes "Graph States and Graph Codes".

• The resulting state $|G\rangle$ is a fully entangled state of two qubits, analogous to the singlet state often used in discussions of Einstein-Podolsky-Rosen paradox, or one of the Bell states.

★ If one measures one of two qubits in an entangled state state, what happens?

• Assume that the qubits, or to be more precise the physical objects that represent them, are far enough apart (perhaps in separate laboratories) so that the measurement apparatus used to measure one object does not interact with the other one, which remains isolated. In this case *nothing* happens to the other object: remember that the wave function "collapse" introduced in textbooks is a *calculational* device, *not* a physical process.

• Instead, what happens is that the outcome of the measurement (traditionally thought of as the position of a pointer) reveals a property possessed by the object that has just been measured, at a time just before the measurement took place. In general this property is not possessed by the object after the measurement is over, and the object itself may have disappeared. (Photons, in particular, have a habit of vanishing when they are measured.) But because the two objects, let us say the two qubits, were in an entangled stated the measured property of the one that has just disappeared is correlated with some property of the other one that remains undisturbed, and for this reason the outcome of the measurement allows the physicist to assign to the distant qubit a *conditional* quantum state, one that depends on the measurement outcome.

○ In the case of a singlet state of two spin-half particles, made famous by discussions of the Einstein-Podolsky-Rosen paradox, if Alice measures S_x and obtains the value $+1/2$ she is entitled to assign a state corresponding to $S_x = -1/2$ to Bob's particle, assuming it has not been disturbed since the singlet state was formed.

• Classical analogy. (All classical analogies are imperfect, but they can still be an aid to thinking about quantum systems.) Charlie puts one red and one green slip of paper into two envelopes, mixes them up, and sends one to Alice and the other to Bob. Alice, who knows the protocol followed by Charlie, opens her envelope and looks to see whether the slip is red or green. From this "measurement" she can infer the color of the slip in Bob's envelope. There is nothing magical about this; no long-distance influences. In the classical or in the quantum world.

★ The graph state under discussion can be written in the form

$$\sqrt{2}|G\rangle = |0\rangle \otimes |+\rangle + |1\rangle \otimes |-\rangle. \tag{1}$$

○ If it helps avoid confusion, use subscripts, as in $|0\rangle_1 \otimes |+\rangle_2$, to indicate which ket belongs to which qubit.

□ Exercise. Write out $|G\rangle$ in the standard basis and show that there are three terms with a $+$ sign, one with a $-$ sign, and that it is obvious when written out this way that $|G\rangle$ is unchanged if one interchanges the two qubits.

★ Suppose qubit 1 is measured in the z basis, i.e., the apparatus yields an output $m = 0$ in the case of $|0\rangle_1$ and $m = 1$ in the case $|1\rangle_1$. Then because the measurement reveals a property this qubit had just before the measurement took place, if $m = 0$ whoever knows the outcome of the measurement is justified in assigning to qubit 2 the state $|+\rangle$, and this assignment can be used to calculate what will happen if at some later time qubit 2 is subjected to additional interactions or measurements. Or what did happen at an earlier time, if such interactions occurred earlier (but after the time when the graph state was created). Similarly, on the basis of a measurement outcome $m = 1$ for qubit 1, qubit 2 can be assigned the state $|-\rangle$, and this is correct assuming qubit 2 has remained undisturbed since the time when the graph state was created, or correct for all times within the interval in which it remains (or remained) undisturbed.

○ To use the classical analogy, if Alice opens her envelope and sees a red slip of paper, she is justified in assigning the color green to the slip of paper in Bob's envelope, and she can use this to infer that Bob

will see a green slip if he first opens his envelope tomorrow, or saw a green slip if he opened the envelope yesterday. Assuming, of course, that he did not drop the slip into a vat of red ink before looking at it.

- To summarize: For the graph state $|G\rangle$ under discussion, the correct inference from a measurement outcome m on qubit 1 is that qubit 2, the one that has has not been measured, is in the state $Z^m|+\rangle$. In the jargon of measurement-based computation, qubit 2 is in the state $|+\rangle$ apart from a possible Pauli correction Z, and the outcome of the measurement on qubit 1 tells us whether or not this Pauli correction is present.

★ One can generalize this to any graph state $|G\rangle$ in the following way. Suppose that qubit 1 is measured in the z basis and the outcome is $m = 0$. Then the *remaining* qubits will be in the state $|G'\rangle$, where the graph G' is obtained from G by eliminating vertex 1 and all the edges that connect 1 to other vertices. However, if the outcome is $m = 1$ the other qubits should be assigned the state $(\prod Z)|G'\rangle$ obtained by applying a one qubit Z operator to each of the other qubits which were directly connected by an edge to qubit 1 in the original graph G.

□ Exercise. Derive this result. [Hint. Convince yourself using the general definition of a graph state that $\sqrt{2}|G\rangle$ is of the form $|0\rangle_1 \otimes |G'\rangle + |1\rangle_1 \otimes |G''\rangle$ for an appropriate choice of $|G'\rangle$ and $|G''\rangle$.]

★ A second type of measurement which plays a very important role in measurement-based quantum computation uses a measurement basis in the equatorial or xy plane of the Bloch sphere, so we call it an *equatorial measurement*. In particular $E(\alpha) = m$, "equatorial measurement at α yields the value m," corresponds to the measurement circuit in Fig. 1, where the final D means a measurement in the standard basis with result $m = 0$ or 1.

$$\rightarrowtail \boxed{E(\alpha)} = m \qquad \rightarrowtail \boxed{Z(\alpha)} \boxed{H} \,\rangle\!\!= m$$
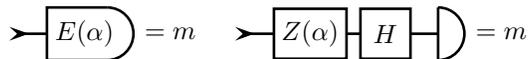
Figure 1: The equatorial measurement $E(\alpha)$ on the left corresponds to the measurement circuit on the right.

- Here $Z(\alpha)$ is the unitary operator with matrix

$$Z(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \tag{2}$$

in the standard basis.

- Suppose the $E(\alpha)$ measurement is applied to qubit 1 in the two qubit graph state (1), with measurement outcome m. What can we say about qubit 2? The result is given by setting $|\psi\rangle = |+\rangle$ in the Fundamental lemma, which it is useful to state in a form slightly more general than needed to answer this question.

★ Fundamental lemma. Let $|\psi\rangle$ be an arbitrary one qubit state, (i.e., anything of the form $a|0\rangle + b|1\rangle$). If upon applying an equatorial measurement $E(\alpha)$ to the first qubit in the state

$$|\Psi\rangle = C_{12}\Big(|\psi\rangle_1 \otimes |+\rangle_2\Big) \tag{3}$$

the outcome is m, then the second qubit can be assigned the conditional state

$$|\psi_2\rangle = HZ^m Z(\alpha)|\psi\rangle = X^m HZ(\alpha)|\psi\rangle = X^m X(\alpha)H|\psi\rangle, \tag{4}$$

where H is the Hadamard gate. Recall that the Hadamard gate interchanges the x and z axes, and as a consequence the unitary

$$X(\alpha) = HZ(\alpha)H \tag{5}$$

is a rotation by an angle α about the x axis, just as $Z(\alpha)$ represents a rotation by an angle α about the z axis.

- The lemma can be expressed using the following circuit:

□ Exercise. Prove the lemma.

★ It is worth noting that when using the Fundamental lemma one can assign an arbitrary phase to the output without changing the physics of the resulting state: one could just as well use $-X^m X(\alpha)H|\psi\rangle$ rather than $X^m X(\alpha)H|\psi\rangle$ in (4) or Fig. 2.

3

$$|\psi\rangle \qquad \boxed{E(\alpha)} = m$$

$$|+\rangle \qquad\qquad HZ^m Z(\alpha)|\psi\rangle = X^m X(\alpha)H|\psi\rangle$$
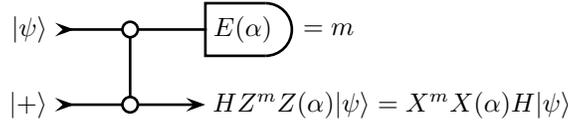
Figure 2: Fundamental lemma as a circuit.

3   Linear Graph

★ Next consider a *sequence* of measurements carried out from left to right on the *linear* graph state

$$|G\rangle = \underset{1 \quad 2 \quad 3 \quad 4}{\circ\!\!-\!\!\circ\!\!-\!\!\circ\!\!-\!\!\circ}\; - - - \tag{6}$$

obtained by starting with all qubits in the $|+\rangle$ state and then applying a CP gate $C_{j,j+1}$ between each qubit and its neighbor to the right.

○ Remember that the CP gates commute with each other, so it does not matter in which order they are applied. That is, C_{23} could be carried out either earlier or later than C_{12} and it makes no difference; the graph state in (6) is what results when one has finished applying all the CP gates.

★ What will be the result if an equatorial measurement $E(\alpha)$ is made on qubit 1 and the outcome is $m = 0$ or 1? That is, what quantum state should be assigned to the remaining qubits (remember that qubit 1 is destroyed by the measurement) in these two cases?

● The conditional state will be some sort of entangled state, and we cannot use the Fundamental lemma to answer the question, because the Fundamental lemma was derived for, and only applies to, the case of a graph of two vertices joined by a single edge, not to (6). However, we can use the Fundamental lemma to provide a useful answer to the question by means of the following trick. Suppose that instead of carrying out the measurement on the state $|G\rangle$ in (6) we instead carry it out on

$$C_{23}|G\rangle = \underset{1 \quad 2 \qquad 3 \quad 4}{\circ\!\!-\!\!\circ \qquad \circ\!\!-\!\!\circ}\; - - - \tag{7}$$

This is a product state: a state of qubits 1 and 2 tensored with a linear graph state on the remaining qubits.

● If we now apply the measurement $E(\alpha)$ to qubit 1 the Fundamental lemma tells us that qubit 2 should be assigned the state

$$|\psi_2\rangle = HZ^m Z(\alpha)|+\rangle, \tag{8}$$

and hence the collection of qubits 2, 3, 4, ... the state

$$|G'\rangle = \underset{2 \qquad 3 \quad 4}{\bullet \qquad \circ\!\!-\!\!\circ}\; - - - \tag{9}$$

where the black dot tells us that qubit 2 is not in the canonical $|+\rangle$ state, but is in a different state. For the case at hand this state is $|\psi_2\rangle$, defined in (8).

● Now C_{23} is its own inverse, $C_{23}^2 = I$. We applied it to $|G\rangle$ in order to get rid of the $2-3$ edge; now let us put the edge back again and consider

$$C_{23}|G'\rangle = \underset{2 \quad 3 \quad 4}{\bullet\!\!-\!\!\circ\!\!-\!\!\circ}\; - - - \tag{10}$$

where the black dot now tells us that $C_{23}|G'\rangle$ is a modified graph state obtained by starting with qubits 3, 4, etc. in the usual $|+\rangle$, but qubit 2 in in the state $|\psi_2\rangle$, and then carrying out CP operations corresponding to the different edges.

★ In fact $C_{23}|G'\rangle$, the state in (10), is precisely the conditional state which should be assigned to the remaining qubits if the equatorial measurement $E(\alpha)$ carried out on qubit 1 in the state $|G\rangle$ in (6) has the outcome m. To see that this is so, note that we first applied C_{23} to $|G\rangle$, carried out the measurement on qubit 1, and then applied C_{23} to the resulting state. But in fact the measurement on qubit 1 and the unitary

4

C_{23} on qubits 2 and 3 were carried out at separate locations, and cannot have had any influence on each other. Since C_{23} was carried out twice, and $C_{23}^2 = I$, a CP gate is its own inverse, the net effect was to do nothing. Applying it twice was just a calculational device which allowed us to apply the Fundamental lemma without having to plow through additional mathematics which in the end would have given us the same result.

○ Calculational tricks of this sort are very useful, and are most helpful when one remembers that they are calculational tricks and not literal descriptions of how a quantum system is actually behaving. There is a temptation to say that by the $E(\alpha)$ measurement on qubit 1 of the state $|G\rangle$ in (6) we somehow "induced" the state $|\psi_2\rangle$ on qubit 2 at a time before the entangling operations to produce the graph state took place, perhaps several hours ago. Myths of this sort can be very helpful as useful mnemonic devices, but one should remember that they are myths and not to be taken too literally. They fall in the same category, and are indeed alternative versions, of the wave function collapse myth of textbook quantum mechanics.

○ If one prefers a realistic physical description in place of the myth, it can be given in the following form. A measurement of qubit 1 reveals a property possessed by this qubit before the measurement took place, and since this property was correlated with a corresponding property of the remaining collection of qubits, the measurement outcome allowed us to assign a conditional state to the latter. A convenient way to *calculate* this conditional state is to imagine that qubit 2 was in the state $|\psi_2\rangle$ rather than in $|+\rangle$ before the other entangling operations C_{23}, C_{34}, etc. were applied.

★ The same procedure, imagining edges removed and then putting them back again, can be applied to finding the conditional state remaining after a whole sequence of measurements has been carried out. Thus if following the $E(\alpha)$ measurement of qubit 1 in the graph state $|G\rangle$ of (6) an $E(\beta)$ measurement is carried out on qubit 2 with outcome n, the state of the remaining qubits is of the form

$$\begin{array}{cc} \bullet\!\!-\!\!-\!\!-\!\!\circ\text{- - -} & \\ 3 \qquad 4 & \end{array} \tag{11}$$

where now the entangling gate C_{34} corresponding to the edge $3-4$ is thought of as applied with qubit 3 in the initial state (i.e., before applying C_{34})

$$|\psi_3\rangle = HZ^n Z(\beta)|\psi_2\rangle = X^n X(\beta)H|\psi_2\rangle = X^n X(\beta)Z^m Z(\alpha)|+\rangle. \tag{12}$$

★ To summarize. The effect of measuring one by one the qubits in a linear graph state starting at one end is to leave a state on the remaining qubits which can be thought of as obtained by applying an entangling operation corresponding to the remaining edges to a product state in which the qubit following the last one that was measured is in an *initial* state, before applying the entangling operation that connects it to the rest of the graph, of the type indicated above in (8) or (12), determined by applying (iteratively) the Fundamental lemma.

4 One Qubit Unitaries

★ One way of viewing the Fundamental lemma is that it is a prescription for carrying out a certain type of unitary operation on a qubit with the help of an ancillary qubit initially in the $|+\rangle$ state, along with a measurement of this ancillary qubit, in the manner familiar from discussions of Kraus operators. To this end it helps to redraw Fig. 2 in the form shown in Fig. 3.
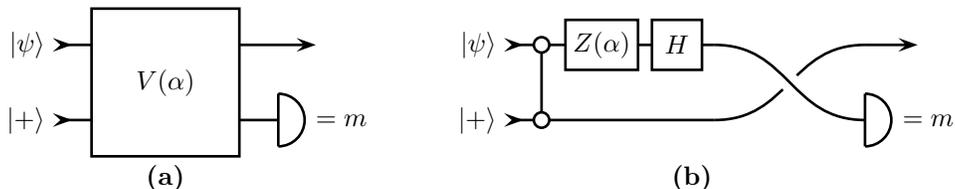
Figure 3: Alternative form of Fig. 2. The unitary $V(\alpha)$ in (a) is given by the circuit in (b).

∘ The exchange of the two qubits that occurs in part (b) can be replaced with a series of CNOT or CP gates and Hadamards which accomplishes the same thing without actually "moving" either qubit, thus justifying the idea that the measurement is carried out on the ancillary qubit, not the original qubit. But the diagram as shown in (b) is easier to understand.

• The overall effect on the input $|\psi\rangle$ can be expressed in terms of Kraus operators in the usual way:

$$V(\alpha)\Big(|\psi\rangle \otimes |+\rangle\Big) = J(\alpha)|\psi\rangle = \sum_{m=0}^{1}\Big(K_m|\psi\rangle\Big) \otimes |m\rangle;$$

$$K_0 = HZ(\alpha)/\sqrt{2}, \quad K_1 = XHZ(\alpha)/\sqrt{2} = XK_0. \tag{13}$$

Both Kraus operators are unitary operators apart from a constant, and one of them is equal to the other followed by the Pauli operator X. Thus if the measurement outcome is $m = 0$ one knows that the circuit has carried out the unitary operator $HZ(\alpha)$ on the input (upper) qubit with the result emerging at the "upper level" indicated by the final arrow in Fig. 3. If, on the other hand, the measurement outcome is $m = 1$ a different unitary, $XHZ(\alpha)$ has been carried out. The genius of the measurement-based scheme is the idea that this "extra Pauli" operator X, while it cannot be ignored, can be taken care of by adjusting what happens later.

∘ The $\sqrt{2}$ in the definition of K_0 and K_1 is there because one or the other will occur with a probability of 1/2. Once one knows which has occurred, the (re)normalized conditional state is simply the appropriate unitary times $|\psi\rangle$.

• It is helpful to keep in mind that whenever one uses Kraus operators the physical results are not changed if the different Kraus operators are multiplied by arbitrary phases. In mathematical terms, this does not change the superoperator that the Kraus operators are representing. For example, one could set K_1 equal to $-XHZ(\alpha)/\sqrt{2}$ and it would make no difference.

★ An idea of how one "takes care of" extra Paulis can be illustrated by placing two of the Fig. 3 circuits in succession:
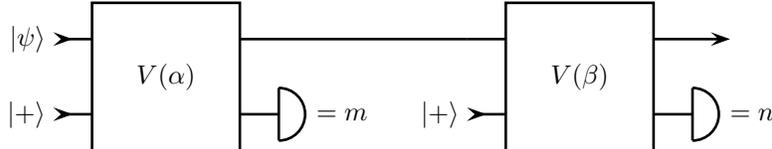
Figure 4: Two operations of the sort shown in Fig. 3 in succession.

• What emerges from the $V(\alpha)$ box is $X^m HZ(\alpha)|\psi\rangle$, and what emerges from the $V(\beta)$ box, again applying the Fundamental lemma, is

$$X^n HZ(\beta)X^m HZ(\alpha)|\psi\rangle = X^n Z^m X((-1)^m \beta)Z(\alpha)|\psi\rangle, \tag{14}$$

where $Z(\beta)X = XZ(-\beta)$ and $HZ(\beta)H = X(\beta)$ have been used to obtain the expression on the right side.

□ Exercise. Justify these steps.

• Suppose it was our intention to carry out a unitary of the form $X(\beta)Z(\alpha)$. Then the result in (14) is not entirely satisfactory, because if the first measurement outcome was $m = 0$ we get what we want up to the extra Pauli correction X^n, to be dealt with later, but if $m = 1$ the actual unitary carried out was $X(-\beta)Z(\alpha)$, definitely not what we intended, and not something that can be corrected (in general) by an extra Pauli X or Z.

• However, we can get around the $m = 1$ difficulty in the following way. As the value of m is known before the measurement associated with the second box in Fig. 4 takes place, we can change the measurement basis used for the latter, see Fig. 3(b), from β to $-\beta$, and then the sign reversal produced by $m = 1$ will give us what we wanted. Again, up to a Pauli correction, which we need to keep track of.

• A little thought shows that by paying attention to previous measurement outcomes we can always adjust the measurement basis of the next unitary so as to be able to carry out, up to Paulis, an overall

unitary which is the product of alternating $Z(\alpha)$ and $X(\beta)$ gates with different choices of angles at each step. But in fact *any* one qubit unitary, since it corresponds to some rotation of the Bloch sphere, can be written in the form $U = Z(\gamma)X(\beta)Z(\alpha)$ with an appropriate choice of Euler angles α, β, and γ. Thus the measurement-based scheme using a linear graph state can be employed to carry out any one-qubit unitary, up to Pauli corrections which are known from the measurement outcomes.

5 General Quantum Circuits

★ A quantum circuit to carry out an arbitrary unitary on N qubits can always be constructed using a set of one-qubit gates interspersed with an appropriate collection of two-qubit gates. These two qubit gates can be chosen to be CP gates.

• In addition we suppose that all the qubits at the beginning of the circuit are in $|+\rangle$ states, i.e., the overall state is a tensor product of the form $|+ + \cdots +\rangle$, and at the end they are all measured individually in the standard basis. This suffices for applications such as Deutsch-Jozsa, Shor factorization, and the like.

★ All the essential ideas can be illustrated using the example in Fig. 5 where the circuit in shown in part (a), time going from left to right, the initial graph state is in (b), while (c) and (d) illustrate some of the successive stages in the measurement process.
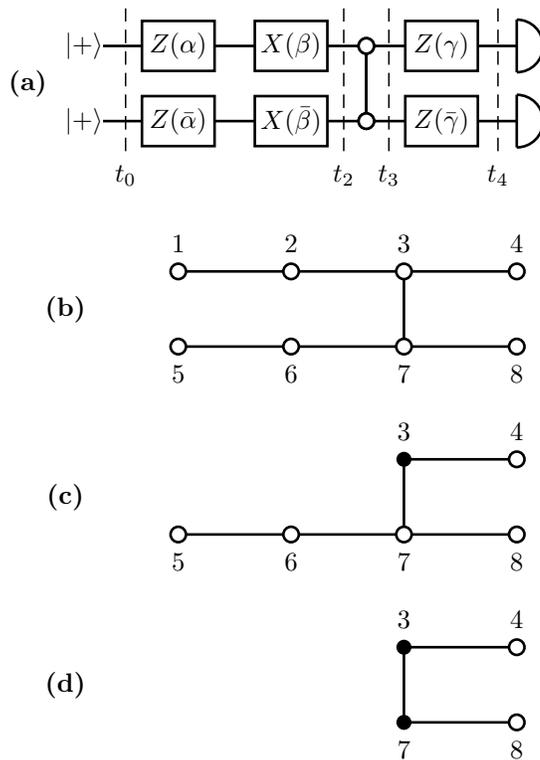
Figure 5: Quantum circuit (a) and stages (b), (c), (d) in the corresponding graph-state approach.

★ From the discussion in the previous section it follows that if qubits 1 and 2 are subjected to measurements with outcomes $E(\alpha) = m_1$ and $E(\pm\beta) = m_2$, where the $-\beta$ is to be used if $m_1 = 1$, then one can say that the resulting state of the remaining qubits, 3 through 8, will be given by (c) in the figure, interpreted as applying CP gates corresponding to the different edges in the figure to an initial product state in which all the qubits are in the $|+\rangle$ state except for 3, which is in the state

$$|\psi_3\rangle = X^{m_2} Z^{m_1} X(\beta) Z(\alpha)|+\rangle. \tag{15}$$

7

○ Note that one could write the Pauli correction as $Z^{m_1}X^{m_2}$ rather than $X^{m_2}Z^{m_1}$. The reason is that Z and X anticommute, so $ZX = -XZ$, and introducing an extra phase in (15) makes no difference.

• A similar set of measurements on qubits 5 and 6 will result in Fig. 5(d), a state of the four remaining qubits obtained by applying the three entangling operations corresponding to the three edges to a product state where qubit 3 is in the state $|\psi_3\rangle$ in (15), and qubit 7 is in the state

$$|\psi_7\rangle = X^{m_6}Z^{m_5}X(\bar\beta)Z(\bar\alpha)|+\rangle. \tag{16}$$

• Let us now work out what this state is by first ignoring the 3-4 and the 7-8 edges—we will apply them later—and asking what happens when C_{37} is applied to $|\psi_3\rangle \otimes |\psi_7\rangle$. The answer is straightforward in the case in which the measurement outcomes m_j for $j = 1$, 2, 5, and 6 are all zero: we will have exactly the same result as in the circuit in part (a) of the figure at time t_3 immediately *after* the CP gate has acted and *before* the action of the final $Z(\gamma)$ and $Z(\bar\gamma)$ gates.

★ But if some of the measurement outcomes have not been zero, then there will be extra Paulis, those indicated in (15) and (16), that precede the application of C_{37}. What shall we do with them? The Pauli Z operators commute with and can thus be pushed through the CP gate, but the X operators do not, and to handle them we apply the general rule:

$$C_{jk}X_j = X_jZ_kC_{jk}. \tag{17}$$

□ Exercise. Derive this result.

• That is, if one "pushes" the Pauli X through a CP gate to a later time, it emerges as an X acting on the same qubit, but it "induces" an additional Pauli Z on the *other* qubit. Of course, if there is already a Pauli Z correction on that qubit, the effect is to "annihilate" it when the X on the first qubit is pushed through the CP.

• To make this quite explicit, as applied to (15) and (16) one has:

$$|\Phi\rangle_{37} = C_{37}\Big(|\psi_3\rangle \otimes |\psi_7\rangle\Big) = \Big(X_3^{m_2}Z_3^{m_1+m_6} \otimes X_7^{m_6}Z_7^{m_2+m_5}\Big)C_{37}\Big(X(\beta)Z(\alpha)|+\rangle_3 \otimes X(\bar\beta)Z(\bar\alpha)|+\rangle_7\Big). \tag{18}$$

The part of this state to the right of the Pauli corrections is the same as the state in Fig. 5(a) at time t_3.

○ Since $X^2 = I = Z^2$, the exponents of the Pauli operators in (18) can be added mod 2, so they are always either 0 or 1.

• Once the Paulis have been moved through C_{37} in this way, we can imagine applying C_{34} and C_{78}; the result will be the state of the four qubits in Fig. 5(d).

★ We are now ready to complete the circuit shown in Fig. 5(a) by applying the last two gates and carrying out a measurement. Consider the $Z(\gamma)$ gate. This can be carried out using an equatorial measurement $E(\pm\gamma)$ on qubit 3, where $+\gamma$ is to be used if $m_2 = 0$ and $-\gamma$ is to be used if $m_2 = 1$. (The same rule, by the way, as if the CP gate in (a) had been absent from the circuit.) Similarly, an $E(\pm\bar\gamma)$ measurement on qubit 7 will serve to take care of $Z(\bar\gamma)$.
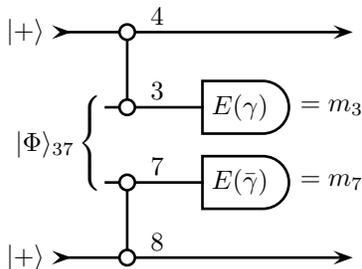
Figure 6: Circuit showing results of measurements on qubits 3 and 7.

• There is a slightly tricky point here which needs to be addressed. The Fundamental lemma of Sec. 2 has to do with the outcome of a measurement on one qubit connected by a CP gate to one other qubit. However, the situation in Fig. 5(d) looks more complicated, since there is an entangling gate connecting

qubits 3 and 7. Can we justify applying the Fundamental lemma? To see that we can, consider the circuit diagram in Fig. 6.

○ From the figure it is evident that were $|\Phi\rangle_{37}$ a product state on qubits 3 and 7, we would have no difficulty applying the fundamental lemma twice, one for the measurement of 3 and one for the measurement of 7. But an entangled $|\Phi\rangle_{37}$ is a sum of such products, and therefore we get the desired result for the final state on qubits 4 and 8.

★ After the measurements on 3 and 7, only qubits 4 and 8 remain from the original graph state, and we know that we can assign to them the same quantum state as the two qubits in Fig. 5(a) at the time t_4 just before the final measurement, apart from Pauli corrections. The next step is to measure qubits 4 and 8 in the z or standard basis, not in an equatorial basis. If there is a Pauli Z correction for either qubit, just ignore it. If, on the other hand, there is a Pauli X correction on, say, qubit 4, then the measurement outcome m_4 is to be "flipped": $m_4 = 0$ is to be interpreted as 1, and $m_4 = 1$ as 0. And the analogous rule applies for qubit 8.

• The point is: we are trying to get the same measurement results (or at least results with the same probability) as we would have gotten using the circuit in Fig. 5(a), and that circuit would have produced the final state on qubits 4 and 8 which we "produced" (or, more accurately, "discovered") by successive measurements on the other qubits, *but without the Pauli corrections.* So we can, in effect, understand our final measurement outcomes on qubits 4 and 8 by imagining that in the circuit in (a) we had inserted certain X or Z gates just before the final measurements, and figuring out how these gates would have affected the measurement outcomes.

□ Exercise. Give an argument as to why the final Pauli Z corrections just before the final measurements on qubits 4 and 8 can be ignored, and in your own words provide the rationale for "flipping" the measurement outcomes when Pauli X corrections are present.

6   Universal Graph State

★ It is possible to start with a single sufficiently large "generic" graph state and by means of suitable measurements use it to carry out a measurement-based computation which will simulate any circuit in which a collection of qubits undergoes a unitary transformation produced by single-qubit gates and CP gates on nearest neighbors, followed by measuring all the qubits in the standard basis.

○ One can, for example, carry out Shor factorization using such a circuit.

○ Two qubit gates between qubits that are not adjacent can be carried out by bringing them together using an appropriate set of exchange gates.

• The generic graph state described below is similar in spirit though it differs in detail from the original Raussendorf and Briegel proposal.

★ Consider a graph state built upon a square lattice with certain nodes missing, a small part of which is shown in Fig. 7. Let us distinguish three types of sites: A with four neighbors, B with two neighbors, one to the left and one to the right, and C with two neighbors, one above and one below. Only some of the nodes have been labeled in the figure.

Figure 7

• Suppose that all of the nodes to the left of the vertical line through A', C, and A'' correspond to qubits that have already been measured, and consequently the current graph state is represented by all the nodes on this vertical line and to the right of it, with the state on the A sites on the vertical line already known in the sense of an initial state, before the entangling operations represented by the vertical edges connecting these to the C sites, and horizontal edges connecting them to the B sites *to the right* (those to the left have already been measured, and thus have disappeared) are applied.

★ In the quantum circuit we are trying to simulate there might or might not be a two-qubit gate acting between A and A''. If there is none, imagine adding the edges (i.e., carry out the entangling operations) which connect C to the A' and A'' sites, and then measure C in the Z basis. It the measurement outcome

is 0, nothing else needs to be done; if it is 1, Pauli Z operators will be placed on the (initial) states at A' and A'', and these can be taken care of at the end of the calculation.

● If, on the other hand, the circuit we are trying to simulate has a CP gate between the sites A' and A'', then the C measurement should be carried out *in the Y basis*. There are two possible outcomes, 0 and 1. If the outcome is zero, the result is the same as if if the desired CP gate had been applied between A' and A'' and, in addition, an $S = Z(\alpha = \pi/2)$ gate had been applied both to the A' and to the A'' qubits. If the outcome is 1, the result corresponds to a CP gate accompanied by a one-qubit gate $S' = ZS = Z(\alpha = 3\pi/2)$ applied to the A' and also to the A'' qubit. Note that the order in which CP and S (or S') does not matter, as they commute.

□ Exercise. Check these assertions by working out what happens if the C gate is measured in the Y basis.

● The presence of this S gate needs to be taken into account in the protocol for the graph state measurement, and this is not difficult to do because the next step of the computation involves simulating some $Z(\alpha')$ and $Z(\alpha'')$ on these two qubits, and the presence of the S single qubit unitaries can be incorporated by a change in the corresponding angles α' or α'', assuming the Y measurement outcome on C is 0. If, on the other hand, it is 1, this adds Z Pauli corrections at A and A', which are taken care of in the same way as other Pauli corrections: keep track of them until the final measurements, as in the example in Sec. 5 above.

★ After the measurements on A' and A'' appropriate measurements are carried out on B' and B'', so as to realized (from the analogous circuit point of view) one qubit unitaries, and when the results are known one is back to a situation analogous to the one in which measurements had been carried out on all qubits to the left of those in the vertical line through A', C, and A''.

★ As pointed out earlier, the actual time at which the entangling operations corresponding to edges of the graph are carried out does not matter, as long as the edges which connect a qubit to the others are present (the entangling operations have been carried out) before this qubit is measured. Thus if there is a convenient way to set up the entire generic graph state before any measurements begin, this can be used for the measurement-based scheme. On the other hand it may be more convenient, in terms of reducing errors or reusing physical qubits, to do some of the entangling operations at the beginning, and then others later on. This will also work and, assuming no errors, lead to the same result.