Outcome Independence of Entanglement in One-Way Computation

Toshihiko Sasaki[1], Tsubasa Ichikawa[2] and Izumi Tsutsui[1]
[1] *Theory Center, Institute of Particle and Nuclear Studies, High Energy Accelerator Research Organization (KEK), 1-1 Oho, Tsukuba, Ibaraki 305-0801, Japan*
[2] *Research Center for Quantum Computing, Interdisciplinary Graduate School of Science and Engineering, Kinki University, 3-4-1 Kowakae, Higashi-Osaka, Osaka 577-8502, Japan*

We show that the various intermediate states appearing in the process of one-way computation at a given step of measurement are all equivalent modulo local unitary transformations. This implies, in particular, that all those intermediate states share the same entanglement irrespective of the measurement outcomes, indicating that the process of one-way computation is essentially unique with respect to local quantum operations.

PACS numbers: 03.65.Ud, 03.67.-a, 03.67.Lx.

I. INTRODUCTION

Entanglement is a key ingredient to make the 'quantum' distinctive against the 'classical'. The superiority of quantum computation (*e.g.* speed-up) over the classical counterpart, for instance, rests on the exploitation of entanglement, and it is a fundamental problem to figure out how it can be achieved effectively. For implementation of quantum computation [1, 2], two schemes have been primarily investigated; one is computation by synthesis of quantum logic gates [3, 4], and the other is one-way computation by local measurements of quantum states [5–10]. The significance of entanglement in the former has been studied [11–13], and it is confirmed that entanglement is essential to realize the superiority. Meanwhile, the significance of entanglement in the latter scheme has also been examined recently [9, 10], where it is found that while not all entangled states are useful, cluster states provide a preferable basis for the activation.

One-way computation has a notable affinity with entanglement in that it consumes entanglement in local measurements. This prompts us to ask precisely how entanglement is created and consumed in the actual process of computation. However, this question has been deemed difficult to answer, because the process involves various intermediate states generated by local measurements. In fact, the number of different intermediate states will grow exponentially as the increase in the number of measurements, making the analysis of entanglement virtually impossible.

In this article, we show that this is not the case – specifically, we prove that for one-way computation realized by a standard quantum circuit consisting of controlled-NOT (CNOT) gates and rotation (ROT) gates, all intermediate states appearing in the process are related by *local* unitary transformations. Since entanglement is invariant under such transformations, this implies that the consumption process of entanglement in one-way computation is actually *unique*, irrespective of the outcomes of the measurements.

II. PRELIMINARIES

To recall the prerequisite of one-way computation, consider an n-qubit system whose constituent qubits are labeled by $V = \{1, 2, \cdots, n\}$. Elements of the set V may be regarded as vertices on a plane, where edges are formed by connecting two pairs $i, j \in V$ we choose. A *graph* $G(V, E)$ is then defined as the union of V and the set E of edges chosen. Each vertex i in the graph G has the neighbor $N_i = \{j \in V \mid \{i, j\} \in E\}$ connected by the edges. We may divide V into three mutually exclusive subsets $V = C_I \cup C_M \cup C_O$, where C_I, C_M and C_O are called 'input', 'middle' and 'output' section, respectively, such that the number of the vertices in C_I is equal to that of C_O. Each qubit represented by the vertex i carries the Hilbert space $\mathcal{H}_i = \mathbb{C}^2$, and accordingly any set of vertices has the corresponding space given by the tensor product of the constituent $\mathcal{H}_i$. For example, the input section C_I has $\mathcal{H}(C_I) = \bigotimes_{i \in C_I} \mathcal{H}_i$, and as a space it is identical to the logical qubit space $\mathcal{H}(C_I) = \mathcal{H}_{\log}$ in which a desired unitary gate $U_{\rm desired}$ is realized. The basic idea of one-way computation is to acquire the output state $U_{\rm desired}|\psi_{\rm in}\rangle$ in C_O to a given input state $|\psi_{\rm in}\rangle$ in C_I, thereby achieving $|\psi_{\rm in}\rangle \to U_{\rm desired}|\psi_{\rm in}\rangle$ in $\mathcal{H}_{\log}$.

For the actual implementation, we first prepare each of the qubits i not belonging to C_I (*i.e.*, $i \in V \backslash C_I$) in the $+1$ eigenstate $|+\rangle_i$ of the spin operator σ_x^i in $\mathcal{H}_i$. Thus our initial n-qubit state is

$$|\Psi_0\rangle = |\psi_{\rm in}\rangle \otimes \bigotimes_{i \in V \backslash C_I} |+\rangle_i. \qquad (1)$$

Let $\mathbb{1}^i$ be the identity operator on $\mathcal{H}_i$, and $|0\rangle_i$, $|1\rangle_i$ be the $+1$, -1 eigenstates of σ_z^i, respectively. The conditional phase gate associated with the edge $\{i, j\} \in E$ reads

$$S_{ij} = |0\rangle_{ii}\langle 0| \otimes \mathbb{1}^j + |1\rangle_{ii}\langle 1| \otimes \sigma_z^j. \qquad (2)$$

The graph state $|G\rangle$ corresponding to $G(V, E)$ is defined from the initial state by applying the conditional phase gate for all edges in the graph:

$$|G\rangle = S|\Psi_0\rangle, \qquad S = \prod_{\{i,j\} \in E} S_{ij}. \qquad (3)$$

For brevity we hereafter omit the symbols $\otimes$ and $\mathbb{1}^i$ when no confusion arises. Note that S satisfies

$$K_i S = S\sigma_x^i, \qquad K_i = \sigma_x^i \bigotimes_{j\in N_i} \sigma_z^j. \tag{4}$$

It then follows from (1), (3) and (4) that

$$K_i|G\rangle = |G\rangle, \tag{5}$$

for all $i \in V\backslash C_I$ [5–8].

Suppose that we measure the spin of the i-th qubit in the x-y plane with angle θ using the operator $\sigma_x^i \cos\theta + \sigma_y^i \sin\theta$. According to the measurement outcomes $s = \pm 1$, the state undergoes the change $|G\rangle \to P_s^i(\theta)|G\rangle$, where the acquired post-measurement state (PMS) is characterized by the projector,

$$P_s^i(\theta) = \frac{\mathbb{1}^i + s\left(\sigma_x^i \cos\theta + \sigma_y^i \sin\theta\right)}{2}, \tag{6}$$

which fulfills

$$P_s^i(\theta)\sigma_x^i = \sigma_x^i P_s^i(-\theta), \qquad P_s^i(\theta)\sigma_z^i = \sigma_z^i P_{-s}^i(\theta). \tag{7}$$

From these we have

$$P_s^i(\theta)K_j = \begin{cases} K_i P_s^i(-\theta) & \text{if } i = j, \\ K_j P_{-s}^i(\theta) & \text{if } i \neq j,\ i \in N_j, \\ K_j P_s^i(\theta) & \text{if } i \neq j,\ i \notin N_j. \end{cases} \tag{8}$$

III. LOCAL UNITARY EQUIVALENCE

Since our one-way computation consists of a set of ROT gates and CNOT gates, we first argue that these two admit independently the local unitary equivalence for intermediate states, before combining the results to show that the same is true for a generic one-way computation.

A. Rotation Gate

Let us start with the one-qubit ROT gate, which can be parameterized by the Euler angles $\boldsymbol{\xi} = (\xi, \eta, \zeta)$ as

$$U_{\rm ROT}(\boldsymbol{\xi}) = \exp\left[-i\zeta\frac{\sigma_x}{2}\right]\exp\left[-i\eta\frac{\sigma_z}{2}\right]\exp\left[-i\xi\frac{\sigma_x}{2}\right]. \tag{9}$$

This gate can be implemented by the $n = 5$ cluster state with the graph $G_{\rm ROT}$ shown in Fig.1. Let $s_i = \pm 1$ be the outcomes of measurement for the i-th qubit with angle θ_i, which is performed successively by the ascending order of i. The actual measurement axis $\theta_i = \theta_i(\boldsymbol{\xi}, \boldsymbol{s})$ is determined from the Euler angles $\boldsymbol{\xi}$ in the ROT gate and the measurement outcomes $\boldsymbol{s} = \{s_1, s_2, s_3\}$ as

$$\theta_1 = 0, \quad \theta_2 = -s_1\xi, \quad \theta_3 = -s_2\eta, \quad \theta_4 = -s_1 s_3\zeta. \tag{10}$$

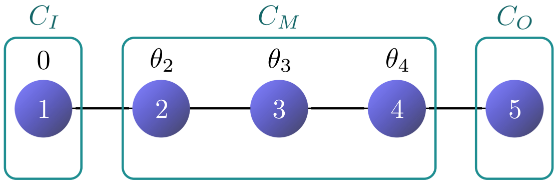

FIG. 1: The graph $G_{\rm ROT}$ for the ROT gate. The lines between the numbered vertices represent the edges, and we have, *e.g.*, the neighbor $N_2 = \{1, 3\}$. Measurement angles θ_i above the vertices i are specified by Eq. (10).

The measurement of the 1st qubit on the graph state (3) yields the PMS $P_{s_1}^1(0)|G_{\rm ROT}\rangle$, which fulfills

$$P_{s_1}^1(0)|G_{\rm ROT}\rangle = P_{s_1}^1(0)K_2|G_{\rm ROT}\rangle = K_2 P_{-s_1}^1(0)|G_{\rm ROT}\rangle, \tag{11}$$

on account of Eqs. (5) and (8) with $1 \in N_2$. This shows that the local unitary operator K_2 transforms a PMS to another PMS having the opposite measurement outcome. We also observe, from Eqs. (5) and (8) with $1 \notin N_3$ and $2 \in N_3$, that the PMS obtained after the 2nd measurement obeys

$$\begin{aligned} P_{s_2}^2(\theta_2)P_{s_1}^1(0)|G_{\rm ROT}\rangle &= P_{s_2}^2(\theta_2)P_{s_1}^1(0)K_3|G_{\rm ROT}\rangle \\ &= P_{s_2}^2(\theta_2)K_3 P_{s_1}^1(0)|G_{\rm ROT}\rangle \\ &= K_3 P_{-s_2}^2(\theta_2)P_{s_1}^1(0)|G_{\rm ROT}\rangle. \end{aligned} \tag{12}$$

A similar argument using K_2, instead of K_3 above, yields

$$P_{s_2}^2(\theta_2)P_{s_1}^1(0)|G_{\rm ROT}\rangle = K_2 P_{s_2}^2(-\theta_2)P_{-s_1}^1(0)|G_{\rm ROT}\rangle. \tag{13}$$

Since $-\theta_2 = -(-s_1)\xi$, we conclude from (12) and (13) that PMS in the 2nd measurement with different outcomes can be related by combining $\{K_2, K_3\}$.

Generalizing our reasoning, we see that the PMS of the 3rd measurement with the outcome (s_1, s_2, s_3) can also be transformed into any PMS with a different outcome (s_1', s_2', s_3') by an appropriate combination of local unitary transformations $\{K_2, K_3, K_4\}$. Clearly, the number of choices of K_i is 2^3 which is just the number of all possible different outcomes. An analogous result holds for the PMS in the 4th measurement with (s_1, s_2, s_3, s_4).

To summarize, we find that for the ROT gate all the PMS appearing at any stage of the measurement can be transformed into each other by local unitary transformations.

B. CNOT Gate

Next we turn to the CNOT gate. If implemented with i-th qubit as the control qubit and j-th as the target, the gate is represented by

$$U_{\rm CNOT} = |0\rangle_{ii}\langle 0| \otimes \mathbb{1}^j + |1\rangle_{ii}\langle 1| \otimes \sigma_x^j. \tag{14}$$

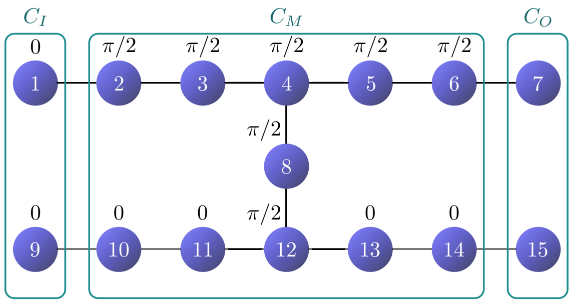

FIG. 2: The graph $G_{\rm CNOT}$ for the CNOT gate. Above the vertices i the measurement angles θ_i, which are either 0 or $\pi/2$, are indicated.

The gate, with the choice $i = 7$, $j = 15$, is realized by the $n = 15$ graph $G_{\rm CNOT}$ shown in Fig.2. Unlike the ROT case (10), all the measurement angles are predetermined independently from the outcomes.

Consider the local measurements over all qubits in $V\backslash C_O = C_I \cup C_M$. The PMS with the measurement outcomes s_i are then given by $\prod_{i\in V\backslash C_O} P^i_{s_i}(\theta_i)|G_{\rm CNOT}\rangle$ up to a normalization factor. Using the identity $P^i_s(\theta) = P^i_{-s}(\theta+\pi)$ and (8), we obtain

$$K_i \prod_{j\in\{i\}\cup N_i} P^j_{s_j}(\theta_j) = P^i_{s_i}(0) \prod_{j\in N_i} P^j_{-s_j}(\theta_j)\, K_i \qquad (15)$$

for i with $\theta_i = 0$, and

$$K_i \prod_{j\in\{i\}\cup N_i} P^j_{s_j}(\theta_j) = \prod_{j\in\{i\}\cup N_i} P^j_{-s_j}(\theta_j)\, K_i \qquad (16)$$

for i with $\theta_i = \pi/2$. These relations show that the action of K_i on the PMS flips the measurement outcomes on the qubits in N_i (including i-th qubit for $\theta_i = \pi/2$) in PMS. In the left half of Table I, we summarize the sets of s_j whose elements are flipped by K_i. By combining these K_i appropriately, we can construct unitary operators which flip the outcomes of a specific qubit without flipping the outcomes of the other qubits (see the right half of Table I). This implies that all PMS can be related to each other by local unitary transformations.

The above argument also ensures that, by an appropriate local unitary operation, we can change the measurement outcomes freely even when not all of the qubits are measured.

C. Universal Gate Set

Now we come to the point to show that one-way computation for the universal gate set enjoys the same unitary equivalence. To this end, recall first that in the logical space $\mathcal{H}_{\log}$ any unitary gate $U_{\rm desired}$ can be decomposed into a product of ROT and CNOT gates,

$$U_{\rm desired} = U_m(\boldsymbol{\xi}^m)\, U_{m-1}(\boldsymbol{\xi}^{m-1}) \cdots U_1(\boldsymbol{\xi}^1), \qquad (17)$$

operator	flipped qubits	qubit	combined operator
K_2	$1,2,3$	1	$K_2K_3K_5K_6$
K_3	$2,3,4$	2	$K_3K_4K_5K_7K_8K_{13}K_{15}$
K_4	$3,4,5,8$	3	$K_4K_6K_7K_8K_{13}K_{15}$
K_5	$4,5,6$	4	K_5K_6
K_6	$5,6$	5	K_6K_7
K_7	6	6	K_7
K_8	$4,8,12$	8	$K_5K_6K_8K_{13}K_{15}$
K_{10}	$9,11$	9	$K_5K_6K_8K_{10}K_{12}K_{14}$
K_{11}	$10,12$	10	$K_{11}K_{13}K_{15}$
K_{12}	$8,11,12,13$	11	$K_5K_6K_8K_{12}K_{14}$
K_{13}	$12,14$	12	$K_{13}K_{15}$
K_{14}	13	13	K_{14}
K_{15}	14	14	K_{15}

TABLE I: (Left) The action K_i and the flipped qubits j in the measurement outcomes s_j. (Right) The qubit i and the combined operator required to flip only the outcome s_i leaving all the rest s_j for $j \neq i$ unaltered.

where $U_\alpha(\boldsymbol{\xi}^\alpha)$, $\alpha = 1,\ldots,m$, are either $U_{\rm ROT}$ in (9) or $U_{\rm CNOT}$ in (14) acting in (generally different) subspaces in $\mathcal{H}_{\log}$, with $\boldsymbol{\xi}^\alpha = (\xi^\alpha, \eta^\alpha, \zeta^\alpha)$ being relevant only for $U_{\rm ROT}$. Each U_α is implemented at step α in the whole process of computation and, accordingly, we consider a graph G consisting of subgraphs G^α, with their own vertices $V^\alpha = C^\alpha_I \cup C^\alpha_M \cup C^\alpha_O$, which are either $G_{\rm ROT}$ or $G_{\rm CNOT}$ in correspondence with U_α in (17). The actual process of step α involves an extended graph $G^\alpha_{\rm ext} \supset G^\alpha$ rigged with vertices which are irrelevant for the implementation of U_α but necessary to provide $\mathcal{H}_{\log}$ as the operational space. We denote by X^α_I and X^α_O the input and the output section of $G^\alpha_{\rm ext}$ containing C^α_I and C^α_O, respectively, for which we have $\mathcal{H}(X^\alpha_I) = \mathcal{H}(X^\alpha_O) = \mathcal{H}_{\log}$. The input section X^α_I contains those vertices in C^β_O with $\beta \le \alpha$ which have not been used in earlier steps, and likewise X^α_O contains those vertices in C^β_I with $\beta \ge \alpha$ which will be used in later steps, such that $X^1_I = C_I$, $X^k_O = X^{k+1}_I$ for $k = 1,\ldots,m-1$ and $X^m_O = C_O$ (see Fig.3 for illustration).

To describe the process more explicitly, consider a projection associated with the measurements over an arbitrary subset $L^\alpha \subset V^\alpha\backslash C^\alpha_O$ of qubits in G^α with outcomes $\boldsymbol{s}^\alpha = \{s^\alpha_i = \pm 1 \mid i \in L^\alpha\}$,

$$P(L^\alpha, \boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha) = \prod_{i\in L^\alpha} P^i_{s^\alpha_i}(\theta^\alpha_i), \qquad (18)$$

where θ^α_i are given by $\theta^\alpha_i = \theta_i(\boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha)$ as in (10) for $G^\alpha = G_{\rm ROT}$, while $\theta^\alpha_i = 0$ or $\pi/2$ for $G^\alpha = G_{\rm CNOT}$ according to Fig. 2. With modified angles $f^\alpha\boldsymbol{\xi}^\alpha$ (to be discussed shortly) with $f^1\boldsymbol{\xi}^1 = \boldsymbol{\xi}^1$, the PMS of the entire system at an intermediate step $\alpha = k$ after the measurements over

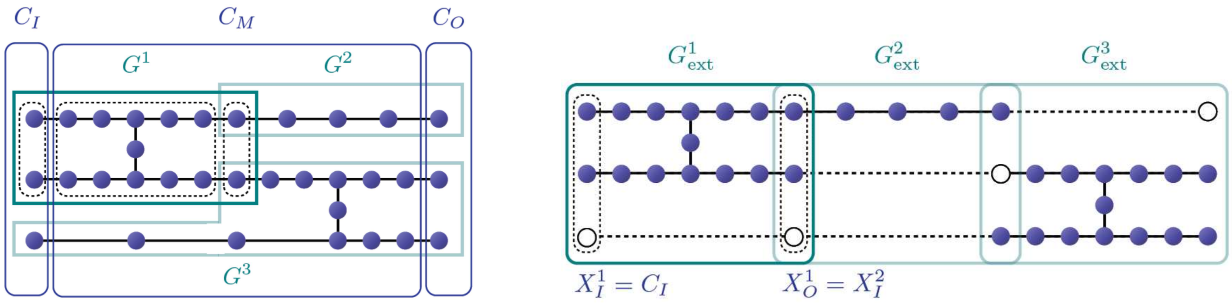

FIG. 3: (Left) The graph G for the unitary gate $U_{\text{desired}} = U_{\text{CNOT}}U_{\text{ROT}}U_{\text{CNOT}}$. (Right) The diagram of the process of computation with extended graphs G^α_{ext} obtained by adding to G^α virtual vertices (open circles) which are aliases of the nearest vertices connected by the dotted lines. All the input and output sections X^α_I and X^α_O in G^α_{ext} possess the same number of qubits to provide the space $\mathcal{H}_{\text{log}}$.

$\Lambda_k = \cup_{\alpha=1}^k L^\alpha$ can then be written as

$$|\Psi(\Sigma_k;\Lambda_k)\rangle := \left[\prod_{\alpha=1}^{k} P(L^\alpha, f^\alpha \boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha) S^\alpha\right] |\Psi_0\rangle, \qquad (19)$$

where the product is in the descending order of α from the left. In (19), $S^\alpha = \prod_{\{i,j\}\in E^\alpha} S_{ij}$ is the operator (2) associated with the edges E^α in G^α, $|\Psi_0\rangle$ is the initial state (1) for the total graph G, and we have introduced the notation $\Sigma_k = \{\boldsymbol{s}^1, \ldots, \boldsymbol{s}^k\}$ for the collection of the measurement outcomes up to step k.

We now notice that, by using the $k = 1$ PMS states in (19), the local unitary equivalence argued earlier for ROT and CNOT may be expressed concisely as

$$|\Psi(\Sigma_1;\Lambda_1)\rangle = U(\Sigma_1, \Sigma'_1)\, |\Psi(\Sigma'_1;\Lambda_1)\rangle, \qquad (20)$$

with a local unitary transformation $U(\Sigma_1, \Sigma'_1)$. Indeed, this is so because $|\Psi_0\rangle$ in (19) contains $\bigotimes_{i\in(C^1_M \cup C^1_O)} |+\rangle_i$ which is sufficient for our argument there.

An important property in one-way computation is that, after the full measurements $L^\alpha = V^\alpha \backslash C^\alpha_O$, the PMS at each step k admits the form,

$$|\Psi(\Sigma_k;\Lambda_k)\rangle = |\psi^k_{\text{out}}\rangle \otimes |\phi^k\rangle, \qquad (21)$$

where $|\psi^k_{\text{out}}\rangle \in \mathcal{H}(X^k_O)$ is the output state, and $|\phi^k\rangle \in \mathcal{H}(V\backslash X^k_O)$. The output state $|\psi^k_{\text{out}}\rangle$, which becomes the input state $|\psi^{k+1}_{\text{in}}\rangle$ in the next step, turns out to be

$$|\psi^k_{\text{out}}\rangle = R_k\, U_k(f^k \boldsymbol{\xi}^k)|\psi^k_{\text{in}}\rangle, \qquad (22)$$

with a qubit-wise local unitary (byproduct) operator $R_k = R_k(\boldsymbol{s}^k)$, where $|\psi^1_{\text{in}}\rangle$ is given by $|\psi_{\text{in}}\rangle$ in (1). The maps f^α are then determined [7] from the demand that at the final step m we obtain

$$\begin{aligned} |\psi^m_{\text{out}}\rangle &= \left[R_m U_m(f^m \boldsymbol{\xi}^m) \cdots R_1 U_1(f^1 \boldsymbol{\xi}^1)\right] |\psi^1_{\text{in}}\rangle \\ &= T\, U_{\text{desired}} |\psi^1_{\text{in}}\rangle, \qquad (23) \end{aligned}$$

with some local unitary gate T.

Having given the relationship between adjacent steps, it is straightforward to extend the result (20) to the final step $k = m$ (for detail, see the Appendix):

$$|\Psi(\Sigma_m;\Lambda_m)\rangle = U(\Sigma_m, \Sigma'_m)\, |\Psi(\Sigma'_m;\Lambda_m)\rangle. \qquad (24)$$

This shows that any two PMS with different outcomes Σ_m and Σ'_m, obtained under the measurements on the same but arbitrary set Λ_m of qubits, are equal up to a unitary local transformation $U(\Sigma_m, \Sigma'_m)$. The equivalence of entanglement possessed by those intermediate PMS follows immediately from this.

IV. SUMMARY AND DISCUSSIONS

In this article, we have shown that, for the universal gate set consisting of ROT gates and CNOT gates, all PMS with different outcomes for an arbitrarily chosen set of measurements can be related by local unitary operations. This rather simple observation should be handy for tracking the consumption process of entanglement in the cluster state during one-way computation. For instance, this will reduce the complexity of evaluating multipartite entanglement measures such as [14, 15], allowing us to consider only a single PMS for each measurement. More generally, the essential uniqueness of PMS pointed out here may provide a basis for comparing directly the process of one-way computation with those of quantum logic gates, assisting our further understanding on quantum computation.

Acknowledgments

T.S. is supported by JSPS Research Fellowships for Young Scientists, T.I. is supported by 'Open Research Center' Project for Private Universities: matching fund subsidy, and I.T. is supported by the Grant-in-Aid for Scientific Research (C), No. 20540391-H22, all of MEXT, Japan.

Appendix

In this Appendix, we prove the local unitary equivalence (24) of PMS by mathematical induction starting with (20). Our argument will be similar to those given in the text, except for some technical complication due to the maps f^α which become nontrivial for $k \geq 2$. Prior to the proof, we describe f^α and also present two formulas to be used.

We assume, for simplicity, that unmeasured outcomes are all $+1$, which is admissible since they do not influence the measurement outcomes over Λ_k. With $g_i = \frac{1-s_i}{2}$, the byproduct operators $R_\alpha(\boldsymbol{s}^\alpha)$ appearing in (22) under the given outcomes can be written as (see Ref.[7])

$$R_{\mathrm{ROT}} = (\sigma_x)^{g_2+g_4}(\sigma_z)^{g_1+g_3}, \tag{A.1}$$

if U_α is ROT, and

$$R_{\mathrm{CNOT}} = (\sigma_x^{(c)})^{\gamma_x^{(c)}}(\sigma_x^{(t)})^{\gamma_x^{(t)}}(\sigma_z^{(c)})^{\gamma_z^{(c)}}(\sigma_z^{(t)})^{\gamma_z^{(t)}}, \tag{A.2}$$

if U_α is CNOT, where the factors associated with the spin operators of the control and target qubits are given by

$$\begin{aligned}
\gamma_x^{(c)} &= g_2 + g_3 + g_5 + g_6, \\
\gamma_x^{(t)} &= g_2 + g_3 + g_8 + g_{12} + g_{14}, \\
\gamma_z^{(c)} &= g_1 + g_3 + g_4 + g_5 + g_8 + g_9 + g_{11} + 1, \\
\gamma_z^{(t)} &= g_9 + g_{11} + g_{13}.
\end{aligned} \tag{A.3}$$

We also record here some useful algebraic relations,

$$\begin{aligned}
U_{\mathrm{ROT}}[\xi,\eta,\zeta]\,\sigma_x &= \sigma_x\,U_{\mathrm{ROT}}[\xi,-\eta,\zeta], \\
U_{\mathrm{ROT}}[\xi,\eta,\zeta]\,\sigma_z &= \sigma_z\,U_{\mathrm{ROT}}[-\xi,\eta,-\zeta], \\
U_{\mathrm{CNOT}}\,\sigma_x^{(t)} &= \sigma_x^{(t)}\,U_{\mathrm{CNOT}}, \\
U_{\mathrm{CNOT}}\,\sigma_x^{(c)} &= \sigma_x^{(c)}\sigma_x^{(t)}\,U_{\mathrm{CNOT}}, \\
U_{\mathrm{CNOT}}\,\sigma_z^{(t)} &= \sigma_z^{(c)}\sigma_z^{(t)}\,U_{\mathrm{CNOT}}, \\
U_{\mathrm{CNOT}}\,\sigma_z^{(c)} &= \sigma_z^{(c)}\,U_{\mathrm{CNOT}}.
\end{aligned} \tag{A.4}$$

Now, we set $T_1 = \mathbb{1}$ and define the gate W_α by

$$W_\alpha = \begin{cases} T_\alpha & \text{if } U_\alpha \text{ is ROT}, \\ U_{\mathrm{CNOT}}\,T_\alpha\,U_{\mathrm{CNOT}}^{-1} & \text{if } U_\alpha \text{ is CNOT}, \end{cases} \tag{A.5}$$

and then put $T_{\alpha+1} = R_\alpha W_\alpha$ to proceed to the next step. This allows us to determine all these quantities for higher steps iteratively, and the maps f^α are defined by the relation,

$$U_\alpha(f^\alpha \boldsymbol{\xi}^\alpha) = W_\alpha U_\alpha(\boldsymbol{\xi}^\alpha) T_\alpha^{-1}. \tag{A.6}$$

This in fact ensures (23) with the unitary gate $T = T_{m+1}$.

At this point, we note that T_α is regarded as a local unitary operator on $\mathcal{H}(X_I^\alpha)(= \mathcal{H}_{\log})$, but it may be extended to a tensor product $\tilde{T}_\alpha := O \otimes T_\alpha \otimes \mathbb{1}$ acting on $\mathcal{H}(V)$, where O is an element of the Pauli group on $\mathcal{H}(\bigcup_{i=1}^{\alpha-1}(C_I^i \cup C_M^i))$ and $\mathbb{1}$ is the identity on the complementary subspace in $\mathcal{H}(V)$. The choice of O is immaterial in our discussion, because it commutes with $P(X^\beta, \boldsymbol{\xi}^\beta, \boldsymbol{s}^\beta)$ and S^β for $\beta = \alpha, \cdots, m$. Analogously, one can define $\tilde{W}_\alpha$ and $\tilde{R}_\alpha$ as the unitary operators on $\mathcal{H}(X_O^\alpha)$ and on $\mathcal{H}(X_O^\alpha)$, respectively, from W_α and R_α.

We these extended operators, we first show

$$\begin{aligned}
&P(L^\alpha, f^\alpha\boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha)S^\alpha\tilde{T}_\alpha|\Psi_\alpha\rangle \\
&\qquad = \tilde{W}_\alpha P(L^\alpha, \boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha)S^\alpha|\Psi_\alpha\rangle,
\end{aligned} \tag{A.7}$$

for

$$|\Psi_\alpha\rangle = |\phi_{\mathrm{in}}\rangle \otimes \bigotimes_{i \in C_M^\alpha \cup C_O^\alpha} |+\rangle_i \tag{A.8}$$

with arbitrary $|\phi_{\mathrm{in}}\rangle \in \mathcal{H}(V\backslash(C_M^\alpha \cup C_O^\alpha))$. Indeed, if U_α is ROT, and if $T_\alpha = \sigma_z$, for example, then from (A.6) we have $W_\alpha = T_\alpha$ and $f^\alpha\boldsymbol{\xi}^\alpha = (-\xi, \eta, -\zeta)$ for $\boldsymbol{\xi}^\alpha = (\xi, \eta, \zeta)$. Setting $\tilde{T}_\alpha = O\sigma_z^1$ and using (5) and (7), we find

$$\begin{aligned}
&P(L^\alpha, f^\alpha\boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha)S^\alpha\tilde{T}_\alpha|\Psi_\alpha\rangle \\
&= OP(L^\alpha, f^\alpha\boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha)\sigma_z^1 S^\alpha|\Psi_\alpha\rangle \\
&= OP(L^\alpha, f^\alpha\boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha)\sigma_z^1 K_2^\alpha K_4^\alpha S^\alpha|\Psi_\alpha\rangle \\
&= OP(L^\alpha, (-\xi, \eta, -\zeta), \boldsymbol{s}^\alpha)\sigma_x^2\sigma_x^4\sigma_z^5 S^\alpha|\Psi_\alpha\rangle \\
&= O\sigma_x^2\sigma_x^4\sigma_z^5 P(L^\alpha, \boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha)S^\alpha|\Psi_\alpha\rangle,
\end{aligned} \tag{A.9}$$

where the numbers $\{1, 2, 3, 4, 5\}$ are the labels of qubits for ROT (see Fig. 1). Since $C_O^\alpha = \{5\}$ for this case, we can put $\tilde{W}_\alpha = O\sigma_x^2\sigma_x^4\sigma_z^5$, which demonstrates (A.7). Other choices of T_α or the case of CNOT can be discussed similarly.

We also wish to establish

$$\begin{aligned}
&P(L^\alpha, \boldsymbol{\xi}^\alpha, \boldsymbol{s}^\alpha)S^\alpha|\Psi_\alpha\rangle \\
&\quad = \tilde{R}_\alpha\tilde{R}'_\alpha P(L^\alpha, \boldsymbol{\xi}^\alpha, \boldsymbol{s}'^\alpha)S^\alpha|\Psi_\alpha\rangle,
\end{aligned} \tag{A.10}$$

as a generalization of (20). Again, we examine this with an example, this time for U_α given by CNOT. Consider two sets of the measurement outcomes $\boldsymbol{s}$ and $\boldsymbol{s}'$ with, say, $s_3 \neq s'_3, s_i = s'_i (i \neq 3)$. In this case, from (A.2) we have $R_\alpha R'_\alpha = \sigma_x^7\sigma_z^7\sigma_x^{15}$, whereas from Table I, we find

$$U(\Sigma_\alpha, \Sigma'_\alpha) = K_4K_6K_7K_8K_{13}K_{15} = O\sigma_x^7\sigma_z^7\sigma_x^{15} \tag{A.11}$$

by choosing an appropriate operator O in the Pauli group. We thus find $U(\Sigma_\alpha, \Sigma'_\alpha) = \tilde{R}_\alpha\tilde{R}'_\alpha$, which shows (A.10). Other cases can also be argued analogously.

With these formulas (A.7) and (A.10), we now prove (24) for

$$U(\Sigma_m, \Sigma'_m) = \tilde{T}_{m+1}\tilde{T}'_{m+1}, \tag{A.12}$$

based on the assumption,

$$|\Psi(\Sigma_\alpha; \Lambda_\alpha)\rangle = \tilde{T}_{\alpha+1}\tilde{T}'_{\alpha+1}|\Psi(\Sigma'_\alpha; \Lambda_\alpha)\rangle \tag{A.13}$$

for $\alpha = k-1$ with some k. For $\alpha = 1$ we have already this, because $T_2 = R_1$ implies $\tilde{T}_2 = \tilde{R}_1$ and hence (A.13) with $\alpha = 1$ follows from (20). For $\alpha = k$, we utilize (A.7), (A.10) and (A.13) with $\alpha = k - 1$ to observe

$$\begin{aligned}
&|\Psi(\Sigma_k; \Lambda_k)\rangle \\
&= \left[P(X^k, f^k \boldsymbol{\xi}^k, \boldsymbol{s}^k) S^k\right] |\Psi(\Sigma_{k-1}; \Lambda_{k-1})\rangle \\
&= \left[P(X^k, f^k \boldsymbol{\xi}^k, \boldsymbol{s}^k) S^k\right] \tilde{T}_k \tilde{T}'_k |\Psi(\Sigma'_{k-1}; \Lambda_{k-1})\rangle \\
&= \tilde{W}_k \left[P(X^k, \boldsymbol{\xi}^k, \boldsymbol{s}^k) S^k\right] \tilde{T}'_k |\Psi(\Sigma'_{k-1}; \Lambda_{k-1})\rangle \\
&= \tilde{W}_k \tilde{W}'_k \left[P(X^k, f'^k \boldsymbol{\xi}^k, \boldsymbol{s}^k) S^k\right] |\Psi(\Sigma'_{k-1}; \Lambda_{k-1})\rangle \\
&= \tilde{W}_k \tilde{W}'_k \tilde{R}_k \tilde{R}'_k \left[P(X^k, f'^k \boldsymbol{\xi}^k, \boldsymbol{s}^k) S^k\right] |\Psi(\Sigma'_{k-1}; \Lambda_{k-1})\rangle \\
&= \tilde{W}_k \tilde{R}_k \tilde{W}'_k \tilde{R}'_k |\Psi(\Sigma'_k; \Lambda_k)\rangle \\
&= \tilde{T}_{k+1} \tilde{T}'_{k+1} |\Psi(\Sigma'_k; \Lambda_k)\rangle, \qquad \text{(A.14)}
\end{aligned}$$

up to a global phase. This is exactly (A.13) for $\alpha = k$, and therefore we reach (24) by mathematical induction.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge university press, Cambridge, 2000.

[2] M. Nakahara and T. Ohmi, *Quantum Computing: From Linear Algebra to Physical Realizations*, Taylor and Francis, Boca Raton, 2008.

[3] D. Deutsch, *Proc. R. Soc. Lond. A* **425** (1989) 73.

[4] A. Barenco *et al.*, *Phys. Rev. A* **52** (1995) 3457.

[5] H. J. Briegel and R. Raussendorf, *Phys. Rev. Lett.* **86** (2001) 910.

[6] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86** (2001) 5188.

[7] R. Raussendorf, D. E. Browne and H. J. Briegel, *Phys. Rev. A* **68** (2003) 022312.

[8] M. Hein *et al.*, arXiv:quant-ph/0602096.

[9] D. Gross, S. T. Flammia and J. Eisert, *Phys. Rev. Lett.* **102** (2009) 190501.

[10] M. J. Bremner, C. Mora and A. Winter, *Phys. Rev. Lett.* **102** (2009) 190502.

[11] R. Jozsa and N. Linden, *Proc. R. Soc. Lond. A* **459** (2003) 2011.

[12] S. L. Braunstein and A. K. Pati, *Quant. Inf. Comput.* **2** (2002) 399.

[13] P. Rungta, *Phys. Lett.* **373A** (2009) 2652.

[14] T. Ichikawa, T. Sasaki and I. Tsutsui, *Phys. Rev. A* **79** (2009) 052307.

[15] T. Ichikawa *et al.*, arXiv:0911.4245.