Which Graph States are Useful for Quantum Information Processing?

Mehdi Mhalla[1](✉), Mio Murao[2,3], Simon Perdrix[1], Masato Someya[2], and Peter S. Turner[2]

[1] CNRS, LIG, Université de Grenoble, Grenoble, France
mehdi.mhalla@gmail.com
[2] Graduate School of Science, The University of Tokyo, Tokyo, Japan
[3] NanoQuine, The University of Tokyo, Tokyo, Japan

Abstract. Graph states [5] are an elegant and powerful quantum resource for measurement based quantum computation (MBQC). They are also used for many quantum protocols (error correction, secret sharing, etc.). The main focus of this paper is to provide a structural characterisation of the graph states that can be used for quantum information processing. The existence of a gflow (generalized flow) [8] is known to be a requirement for open graphs (graph, input set and output set) to perform uniformly and strongly deterministic computations. We weaken the gflow conditions to define two new more general kinds of MBQC: uniform equiprobability and constant probability. These classes can be useful from a cryptographic and information point of view because even though we cannot do a deterministic computation in general we can preserve the information and transfer it perfectly from the inputs to the outputs. We derive simple graph characterisations for these classes and prove that the deterministic and uniform equiprobability classes collapse when the cardinalities of inputs and outputs are the same. We also prove the reversibility of gflow in that case. The new graphical characterisations allow us to go from open graphs to graphs in general and to consider this question: given a graph with no inputs or outputs fixed, which vertices can be chosen as input and output for quantum information processing? We present a characterisation of the sets of possible inputs and ouputs for the equiprobability class, which is also valid for deterministic computations with inputs and ouputs of the same cardinality.

1 Introduction

The graph state formalism [5] is an elegant and powerful formalism for quantum information processing. Graph states form a subfamily of the stabiliser states [4]. They provide a graphical description of entangled states and they have multiple applications in quantum information processing, in particular in measurement-based quantum computation (MBQC) [9], but also in quantum error correcting codes [4] and in quantum protocols like secret sharing [6,7]. They offer a combinatorial approach to the characterisation of the fundamental properties

D. Bacon et al. (Eds.): TQC 2011, LNCS 6745, pp. 174–187, 2014.
DOI: 10.1007/978-3-642-54429-3_12, © Springer-Verlag Berlin Heidelberg 2014

of entangled states in quantum information processing. The invariance of the entanglement by local complementation of a graph [10]; the use of measure of entanglement based on the rank-width of a graph [11]; and the combinatorial *flow* characterisation [1] of deterministic evolutions in measurement-based quantum computation witness the import role of the graph state formalism in quantum information processing.

In this paper, we focus on the application of graph states in MBQC and in particular on the characterisation of graphs that can be used to perform quantum information processing in this context. The existence of a graphical condition which guarantees that a deterministic MBQC evolution can be driven despite of the probabilistic behaviour of the measurements is a central point in MBQC. It has already been proven that the existence of a certain kind of flow called glfow characterises uniformly stepwise determinism [1]. In Sect. 3, we introduce a simpler but equivalent combinatorial characterisation using *focused gflow* and we provide a simple condition of existence of such a flow as the existence of a right inverse to the adjacency matrix of the graph. We also prove additional properties in the case where the number of input and output qubits of the computation are the same: the gflow is then reversible and the stepwise condition [1] on determinism is not required to guarantee the existence of a gflow.

The main contribution of this paper is the weakening of the determinism condition in order to consider the more general class of *information preserving* evolutions. Being information preserving is one of the most fundamental property that can be required for an MBQC computation. Indeed, some non-deterministic evolutions can be information preserving when one knows the classical outcomes of the measurements produced by the computation. Such evolutions are called *equi-probabilistic* – when each classical outcome occurs with probability 1/2 – or *constant-probabilistic* in the general case. In Sect. 4, we introduce simple combinatorial conditions for equi-probabilistic and constant-probabilistic MBQC by means of excluded violating sets of vertices. We show, in the particular case where the number of input and output qubits are the same, that graphs guaranteeing equi-probabilism and determinism are the same. In Sect. 6, using this graphical characterisation, we address the fundamental question of finding input and output vertices in an arbitrary graph for guaranteeing an equi-probabilistic (or deterministic) evolution. To this end, we show that the input and output vertices of a graph must form transversals of the violating sets induced by the equi-probabilistic characterisation. Finally, in the last section, we investigate several properties of the most general and less understood class of constant probabilistic evolutions.

2 Measurement-Based Quantum Computation

In this section, the main ingredients of measurement based quantum computation (MBQC) are described. More detailed introductions can be found in [2,3]. An MBQC is described by:

(i) an open graph (G, I, O) (G is a simple undirected graph, $I, O \subseteq V(G)$ are called resp. input and output vertices);
(ii) a map $\alpha : O^C \to [0, 2\pi)$, where $O^C := V(G) \setminus O$, which associates with every non ouput vertex an angle; and
(iii) two maps $\mathtt{x}, \mathtt{z} : O^C \to \{0,1\}^{V(G)}$ called *corrective maps*. A vertex $v \in supp(\mathtt{x}(u)) \cup supp(\mathtt{z}(u))$ is called a *corrector* of u, where $supp(y) = \{u \mid y_u = 1\}$.

The maps $\mathtt{x}, \mathtt{z}$ should be *extensive* in the sense that there exists a (strict) partial order $\prec$ over the vertices of the graph s.t. any corrector v of a vertex u is larger than u, i.e. $v \in supp(\mathtt{x}(u)) \cup supp(\mathtt{z}(u))$ implies $u \prec v$.

In the following the semantics of a given MBQC is described. The evolution can be decomposed into two steps: first the preparation of a large entangled state described by the open graph (G, I, O); then a sequence of one-qubit measurements (which basis are characterised by the map α) and Pauli operations (described by the maps $\mathtt{x}$ and $\mathtt{z}$).

Let $N : \mathbb{C}^{\{0,1\}^I} \to \mathbb{C}^{\{0,1\}^{V(G)}}$ be the preparation map which associates with any arbitrary input state located on the input qubits the initial entangled state of the MBQC:

$$N = \frac{1}{\sqrt{2^{|I^C|}}} \sum_{x \in \{0,1\}^I, y \in \{0,1\}^{I^C}} (-1)^{q(xy)} |xy\rangle \langle x|$$

where xy denotes the concatenation of x and y, and $q : \{0,1\}^{V(G)} \to \mathbb{N} :: x \mapsto |E(G) \cap (supp(x) \times supp(x))|$ associates with every x the number of edges of the subgraph $G_x = (V(G) \cap supp(x), E(G) \cap (supp(x) \times supp(x)))$ induced by x.

The one-qubit measurements, parametrized by an angle α_u, of every non-output qubit u are inducing the following projection $P_s(\alpha) : \mathbb{C}^{\{0,1\}^{V(G)}} \to \mathbb{C}^{\{0,1\}^O}$ of the entangled state onto the subspace of the output qubits, where $s \in \{0,1\}^{O^C}$ stands for the classical outcomes of the one-qubit measurements:

$$P_s(\alpha) = \frac{1}{\sqrt{2^{|I^C|}}} \sum_{x \in \{0,1\}^{O^C}, y \in \{0,1\}^O} e^{\alpha_{x \cdot s}} |y\rangle \langle xy|$$

with $\alpha_x = \sum_{u \in supp(x)} \alpha(u)$ and $x \cdot s$ is the bitwise conjonction of x and s.

Moreover, adaptative Pauli corrections depending on the classical outcomes of the measurements and on the corrective maps, are applied during the computation leading, for any possible classical outcomes $s \in \{0,1\}^{O^C}$, to the following overall (postselected) evolution $\chi_s : \mathbb{C}^{\{0,1\}^I} \to \mathbb{C}^{\{0,1\}^O}$:

$$\chi_s = P_s(\alpha) \left(\prod_{u \in V(G)} X_{s \cdot \mathtt{x}(u)} Z_{s \cdot \mathtt{z}(u)} \right) N$$

where X_s and Z_s are Pauli operators: $X_s = \bigotimes_{u \in supp(s)} X_u$ and $Z_s = \bigotimes_{u \in supp(s)} Z_u$.

An MBQC is implementing the quantum operation $\{\chi_s\}_{s\in\{0,1\}^{O^C}}$. The evolution is as follows: a classical outcome (also called branch) $s \in \{0,1\}^{O^C}$ is produced and the input state $|\phi\rangle \in \mathbb{C}^{\{0,1\}^I}$ is mapped to the state $\chi_s|\phi\rangle \in \mathbb{C}^{\{0,1\}^O}$ (up to a normalisation). The probability for an outcome $s \in \{0,1\}^{O^C}$ to occur is $p_s = ||\chi_s|\phi\rangle||^2$.

The overall evolution can be decomposed into several steps, corresponding to a possible implementation of the MBQC model: first the input state $|\phi\rangle$ is encoded into the open graph state $|\phi_G\rangle = N|\phi\rangle$, then the local measurements (qubit u is measured according the observable $\cos(\alpha(u))X + \sin(\alpha(u))Y$) and the local Pauli corrections are performed. This sequence of local operations is done according to the partial order induced by the correction maps $\mathtt{x}, \mathtt{z}$.

3 Determinism

Definition 1. *An MBQC $(G, I, O, \alpha, \mathtt{x}, \mathtt{z})$ is strongly deterministic if all the branches are implementing the same map, i.e. $\exists U$ s.t. $\forall s \in \{0,1\}^{O^C}$, $\chi_s = \frac{1}{\sqrt{2^{|O^C|}}}U$.*

Lemma 1. *If an MBQC is strongly deterministic then it implements an isometry.*

Proof. Since $\sum_{s\in\{0,1\}^{O^C}} \chi_s^\dagger\chi_s = I$, $U^\dagger U = I$ so U is an isometry and the MBQC implements the super operator $\rho \mapsto U\rho U^\dagger$. □

In order to point out the combinatorial properties of MBQC, the angles of measurements and the corrective maps can be abstracted away in the following way, keeping only the influence of the initial open graph.

Definition 2. *An open graph (G, I, O) guarantees uniformly strong determinism if $\exists \mathtt{x}, \mathtt{z}$ s.t. $\forall \alpha$, $(G, I, O, \alpha, \mathtt{x}, \mathtt{z})$ is strongly deterministic.*

An open graph is said to guarantee uniform *stepwise* strong determinism if any partial computation is also strongly deterministic:

Definition 3. *An open graph (G, I, O) guarantees uniformly stepwise strong determinism if $\exists \mathtt{x}, \mathtt{z}$ s.t. for any upward closed set $O' \supseteq O$ and for any α, $(G, I, O', \alpha, \mathtt{x}, \mathtt{z})$ is strongly deterministic, where O' is upward closed if $\forall u \in O'$, $u \prec v \Rightarrow v \in O'$ with $\prec$ the partial order induced by $\mathtt{x}$ and $\mathtt{z}$.*

The gflow of an open graph is defined as follows, based on the use of the odd neighborhood of a set of vertices: for a given subset S of vertices in a graph G, $Odd(S) := \{v \in V(G) \text{ s.t. } |\mathcal{N}_G(v) \cap S| = 1 \mod 2\}$.

Definition 4. *$(g, \prec)$ is a* gflow *of (G, I, O), where $g : O^C \to 2^{I^c}$, if for any u,*
— if $v \in g(u)$, then $u \prec v$;
— $u \in Odd(g(u))$;
— if $v \in Odd(g(u))$ and $u \neq v$ then $u \prec v$.

Theorem 1. *An open graph (G, I, O) guarantees uniform stepwise strong determinism iff (G, I, O) has a gflow.*

3.1 Focused Gflow

Since the gflow is not unique we introduce a stronger version called focused gflow, which is unique if the number of inputs and outputs are the same. The focused gflow gives rise to a simpler characterisation of uniform stepwise strong determinism. The focused gflow is based on the use of *extensive* maps.

Definition 5. *$g : O^C \to 2^{I^C}$ is a focused gflow of (G, I, O) if g is extensive – i.e. the transitive closure of the relation $\{(u, v)$ s.t. $v \in g(u)\}$ is a partial order over $V(G)$ – and $\forall u \in O^C$, $Odd(g(u)) \cap O^C = \{u\}$*

Theorem 2. *An open graph (G, I, O) guarantees uniform stepwise strong determinism iff (G, I, O) has a focused gflow.*

Proof. We prove that (G, I, O) has a gflow iff it has a focused gflow. First, assume g is a focused gflow, and let $\prec$ be the transitive closure of $\{(u, v)\ s.t.\ v \in g(u)\}$. $\prec$ is a partial order and by definition, if $v \in g(u)$ then $u \prec v$. Moreover $u \in Odd(g(u)) = \{u\}$. Finally, if $v \in Odd(g(u))$ and $v \neq u$ then $v \in O$, so there is no element larger than v by definition of $\prec$. Thus $(g, \prec)$ is a gflow. Now, assume $(g, \prec)$ is a gflow. We call the co-depth of a vertex u its distance to the output, i.e. the length k of longest strictly increasing sequence $u \prec u_1 \prec .. \prec u_k$ s.t. $u_k \in O$. We construct a focus gflow g_f by induction on the co-depth of the vertices. If u is of co-depth 1 then $g_f(u) := g(u)$. If u is of co-depth larger than 2, let $g_f(u) := g(u) \Delta \left(\Delta_{v \in Odd(g(u)) \cap O^C, v \neq u} g_f(v)\right)$, where Δ is the symmetric difference: $A \Delta B = (A \cup B) \setminus (A \cap B)$. Since $Odd(A \Delta B) = Odd(A) \Delta Odd(B)$, $Odd(g_f(u)) \cap O^C = \big(Odd(g(u)) \Delta \left(\Delta_{v \in Odd(g(u)) \cap O^C, v \neq u} Odd(g_f(v))\right)\big) \cap O^C = (Odd(g(u)) \cap O^C) \Delta (Odd(g(u)) \setminus \{u\}) \cap O^C) = \{u\}$. Moreover g_f is extensive since the relation R induced by g_f is s.t. $uRv \implies u \prec v$ so the transitive closure of R is a partial order. □

3.2 Induced Adjacency Matrix and Reversibility

We introduce the notion of induced adjacency matrix of an open graph and show that an open graph has a gflow if and only if its induced matrix has a DAG (Directed Acyclic Graph) as right inverse.

Definition 6. *The induced adjacency matrix of an open graph (G, I, O) is the submatrix $A_G|_{I^C}^{O^C}$ of the adjacency matrix $A_G = \{m_{u,v}, (u, v) \in V(G)\}$ of G removing the rows of O and column of I, i.e. $A_G|_{I^C}^{O^C} = \{m_{u,v}, (u, v) \in O^C \times I^C\}$.*

The induced matrix $A_G|_{I^C}^{O^C}$ is the matrix representation of the linear map $W \mapsto Odd(W) \cap O^C$ which domain is 2^{I^C} and codomain is 2^{O^C}.

Theorem 3. *(G, I, O) has a gflow iff there exists a DAG $F = (V(G), E)$ s.t.*

$$A_G|_{I^C}^{O^C} . A_F|_{O^C}^{I^C} = I$$

Proof. (*only if*) Assume (G, I, O) has a gflow. Thanks to lemma 2 w.l.o.g. (G, I, O) has a focused gflow g_f. Let $F = (V(G), E)$ be a directed graph s.t. $(u, v) \in E(F) \iff v \in g_f(u)$. Notice that $\forall u \in O^C$, $A_F|_{O^C}^{I^C} 1_{\{u\}} = 1_{g_f(u)}$ where 1_X is a binary vector s.t. $(1_X)_u = 1 \iff u \in X$. Moreover, since g_f is extensive, F is a DAG. Thus $A_G|_{I^C}^{O^C} A_F|_{O^C}^{I^C} 1_{\{u\}} = A_G|_{I^C}^{O^C} 1_{g(u)} = 1_{Odd(g_f(u)) \cap O^C} = 1_{\{u\}}$. (*if*) Assume $F = (V(G), E)$ be a DAG s.t. $A_G|_{I^C}^{O^C} . A_F|_{O^C}^{I^C} = I$, then let $g : O^C \to 2^{I^C} = u \mapsto \mathcal{N}_F^+(u)$. Since F is a DAG, g is extensive, and $1_{Odd(g(u)) \cap O^C} = A_F|_{O^C}^{I^C}(1_{g(u)}) = A_G|_{I^C}^{O^C} A_F|_{O^C}^{I^C} 1_{\{u\}} = 1_{\{u\}}$, so $Odd(g(u)) \cap O^C = \{u\}$. □

Thus, according to Theorem 3, an open graph has a gflow if and only if it has a DAG as right inverse. Notice that this DAG is nothing but the graphical description of the focused gflow function: the set of successors of a vertex u is the image of u by the focused gflow function.

As a corollary of Theorem 3, (G, I, O) has no gflow if $|I| > |O|$. Indeed, for dimension reasons, if $|I| > |O|$ the matrix $A_G|_{I^C}^{O^C}$ has no right inverse. When $|I| = |O|$ the focused gflow is *reversible* in the following sense:

Theorem 4. *When $|I| = |O|$, (G, I, O) has a gflow iff (G, O, I) has a gflow.*

Proof. Assume (G, I, O) has a gflow. So it exists a DAG F s.t. $A_F|_{O^C}^{I^C}$ is the right inverse of $A_G|_{I^C}^{O^C}$. Notice that the induced adjacency matrix of (G, O, I) is the transpose ${}^tA_G|_{I^C}^{O^C}$ of the one of (G, I, O). Moreover, since $A_G|_{I^C}^{O^C}$ is squared, $A_F|_{O^C}^{I^C}$ is both right and left inverse of $A_G|_{I^C}^{O^C}$. Thus, $A_G|_{O^C}^{I^C} . {}^tA_F|_{O^C}^{I^C} = {}^t(A_F|_{O^C}^{I^C} . A_G|_{I^C}^{O^C}) = I$. As a consequence $A_G|_{I^C}^{O^C}$ has a right inverse which is a DAG since the transpose of a DAG is a DAG. □

4 Relaxing Uniform Determinism

Focused gflow guarantees uniformly stepwise strong determinism. We consider here two more general classes of MBQC evolutions: the *equi-probabilistic* case where all the branches occur with the same probability, independent of the input state; and the *constant probability* case where all the branches occur with a probability independent of the input state. We show that both equi-probabilitic and constant probabilistic evolutions are information preserving and admit a simple graphical characterisation by means of violating sets.

Definition 7. *An MBQC $(G, I, O, \alpha, \mathtt{x}, \mathtt{z})$ is:*
— equi-probabilistic *if for any input state $|\phi\rangle \in \mathbb{C}^{2^I}$ and any branch $s \in \{0,1\}^{O^C}$, $p_s = ||\chi_s |\phi\rangle ||^2 = \frac{1}{2^{|O^C|}}$.*
— constant-probabilistic *if for any branch $s \in \{0,1\}^{O^C}$ the probability $p_s = ||\chi_s |\phi\rangle ||$ that the branch s occurs does not depend on the input state $|\phi\rangle$.*

Constant probabilistic (and hence equi-probabilistic) evolutions are *information preserving* in the sense that if one knows the branch s of the computation (i.e. the classical outcome) then he can recover the initial input state of the computation. Indeed, if an MBQC is constant probabilistic then the map $|\phi\rangle \mapsto ||\chi_s |\phi\rangle ||$ is constant, thus $\chi_s^\dagger \chi_s = p_s.I$. If $p_s = 0$ then the branch never occurs, otherwise the branch s is implementing an isometry.

Remark: Notice that the knowledge of the branch s, which is necessary the case in the MBQC model because of the corrective strategy, is essential to make an equi-probabilistic evolution information preserving. Indeed, consider the quantum one-time pad example with $\forall s \in \{0,1\}^2$, $\chi_s = \sigma_s/2$ where σ_s is a Pauli operator ($\sigma_{00} = I$, $\sigma_{01} = X$,$\sigma_{10} = Y$,$\sigma_{11} = Z$). This evolution is equi-probabilistic but if the information of the branch is not taken into account, the corresponding super operator is $\rho \mapsto \sum_{s\in\{0,1\}^2} \sigma_s \rho \sigma_s^\dagger = I/2$ which is clearly not information preserving.

We prove that uniform equi- and constant probabilities have simple graph characterisations by violating sets, where uniformity is defined similarly to the determinism case:

Definition 8. *An open graph (G, I, O) guarantees uniform constant (resp. equi-) probabilisty if $\exists \mathtt{x}, \mathtt{z}$ s.t. $\forall \alpha$, $(G, I, O, \alpha, \mathtt{x}, \mathtt{z})$ has a constant (resp. equi-) probabilistic evolution.*

Theorem 5. *An open graph (G, I, O) guarantees uniform equiprobability iff*

$$\forall W \subseteq O^C, Odd(W) \subseteq W \cup I \implies W = \emptyset$$

A nonempty set $W \subseteq O^C$ such that $Odd(W) \subseteq W \cup I$ is called an *internal set.* Theorem 5 says that an open graph (G, I, O) guarantees uniform equi-probability if and only if it has no internal set.

Proof. (*if*) First we assume that there is no internal set and we show that every branch occurs with the same probability $1/2^{|O^C|}$, independently of the input state and the set of measurement angles. For a given open graph (G, I, O), a given input state $|\phi\rangle$ and a given set of measurement angles $\{\alpha_v\}_{v\in O^C}$, we consider w.l.o.g. the 0-branch, i.e. the branch where all outcomes are 0 [1]. The probability of this branch is $p = ||\prod_{v\in O^c} \langle +_{\alpha_v} |\phi_G\rangle ||^2 = \frac{1}{2^{|O^C|}} ||\sum_{x\in\{0,1\}^{O^C}} e^{i\alpha_x} \langle x |\phi_G\rangle ||^2$ where $\alpha_x = \sum_{v\in O^C} \alpha_v.x_v$ and $|\phi_G\rangle = E_G |+\rangle_{I^C} |\phi\rangle_I$. As a consequence,

$$\begin{aligned}
p &= \tfrac{1}{2^{|O^C|}} \textstyle\sum_{x,y\in\{0,1\}^{O^C}} e^{i(\alpha_y - \alpha_x)} \langle\phi_G |x\rangle \langle y |\phi_G\rangle \\
&= \tfrac{1}{2^{|O^C|}} \textstyle\sum_{u\in\{-1,0,1\}^{O^C}} e^{i\alpha_u} \sum_{x,y\in\{0,1\}^{O^C} \ s.t.\ x-y=u} \langle\phi_G |x\rangle \langle y |\phi_G\rangle \\
&= \tfrac{1}{2^{|O^C|}} \textstyle\sum_{u\in\{-1,0,1\}^{O^C}} e^{i\alpha_u} \sum_{x\in\{0,1\}^{V_u^C}} \langle\phi_G |x\rangle_{V_u^C} \left|\tfrac{1+u}{2}\right\rangle_{V_u} \langle x|_{V_u^C} \left\langle\tfrac{1-u}{2}\right|_{V_u} |\phi_G\rangle \\
&= \tfrac{1}{2^{|O^C|}} \textstyle\sum_{u\in\{-1,0,1\}^{O^C}} e^{i\alpha_u} \langle\phi_G| \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left(\sum_{x\in\{0,1\}^{V_u^C}} |x\rangle \langle x|\right) \left\langle\tfrac{1-u}{2}\right|_{V_u} |\phi_G\rangle \\
&= \tfrac{1}{2^{|O^C|}} \textstyle\sum_{u\in\{-1,0,1\}^{O^C}} e^{i\alpha_u} \langle\phi_G| \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left\langle\tfrac{1-u}{2}\right|_{V_u} |\phi_G\rangle \\
&= \tfrac{1}{2^{|O^C|}} \textstyle\sum_{u\in\{-1,0,1\}^{O^C}} e^{i\alpha_u} p_u
\end{aligned}$$

[1] The other branches are taken into account by considering a different set of measurement angles e.g. the branch where all outcomes are 1 corresponds to the 0-branch when the set of measurements is $\{\alpha_v + \pi\}_{v\in O^C}$.

where $V_u = \{i \in O^C \mid u_i \neq 0\}$, $\left|\frac{1\pm u}{2}\right\rangle_{V_u} = \bigotimes_{i\in V_u}\left|\frac{1\pm u_i}{2}\right\rangle_i$, and $p_u = \langle\phi_G|\left|\frac{1+u}{2}\right\rangle_{V_u}\left\langle\frac{1-u}{2}\right|_{V_u}|\phi_G\rangle$. Notice that for any $v \in I^C$, $|\phi_G\rangle = \frac{1}{\sqrt{2}}\sum_{a\in\{0,1\}} Z^a_{\mathcal{N}_G(v)}\left|\phi_{G\setminus v}\right\rangle \otimes |a\rangle_v$. Thus for any $u \in \{-1,0,1\}^{O^C}$ s.t. $V_u \neq \emptyset$, there exists $v \in I^C \cap V_u^C \cap Odd(V_u)$ (which is not empty by hypothesis) such that:

$$\begin{aligned}
p_u &= \langle\phi_G|\left|\tfrac{1+u}{2}\right\rangle_{V_u}\left\langle\tfrac{1+u}{2}\right|_{V_u} X_{V_u}|\phi_G\rangle\\
&= \tfrac{1}{2}\textstyle\sum_{a,b\in\{0,1\}}\left\langle\phi_{G\setminus v}\right|\langle a|_v\, Z^a_{\mathcal{N}_G(v)}\left|\tfrac{1+u}{2}\right\rangle_{V_u}\left\langle\tfrac{1+u}{2}\right|_{V_u} X_{V_u} Z^b_{\mathcal{N}_G(v)}\left|\phi_{G\setminus v}\right\rangle|b\rangle_v\\
&= \tfrac{1}{2}\textstyle\sum_{a\in\{0,1\}}\left\langle\phi_{G\setminus v}\right| Z^a_{\mathcal{N}_G(v)}\left|\tfrac{1+u}{2}\right\rangle_{V_u}\left\langle\tfrac{1+u}{2}\right|_{V_u} X_{V_u} Z^a_{\mathcal{N}_G(v)}\left|\phi_{G\setminus v}\right\rangle\\
&= \tfrac{1}{2}\textstyle\sum_{a\in\{0,1\}}(-1)^a\left\langle\phi_{G\setminus v}\right| Z^a_{\mathcal{N}_G(v)}\left|\tfrac{1+u}{2}\right\rangle_{V_u}\left\langle\tfrac{1+u}{2}\right|_{V_u} Z^a_{\mathcal{N}_G(v)} X_{V_u}\left|\phi_{G\setminus v}\right\rangle\\
&= \tfrac{1}{2}\textstyle\sum_{a\in\{0,1\}}(-1)^a\left\langle\phi_{G\setminus v}\right|\left|\tfrac{1+u}{2}\right\rangle_{V_u}\left\langle\tfrac{1+u}{2}\right|_{V_u} X_{V_u}\left|\phi_{G\setminus v}\right\rangle = 0
\end{aligned}$$

where the factor $(-1)^a$ comes from the fact that X_{V_u} and $Z^a_{\mathcal{N}_G(v)}$ are commuting when $a = 0$ and anticommuting when $a = 1$ since $v \in Odd(V_u)$. As a consequence, it remains in p only the case where $V_u = \emptyset$, so $p = \frac{1}{2^{|O^C|}}\langle\phi_G|\phi_G\rangle = \frac{1}{2^{|O^C|}}$.

(*only if*) Now we prove that the existence of an internal set implies that there exists a particular input state and a particular set of measurement angles such that some branches occur with probability 0. Let $W_0 \subseteq O^C$ s.t. $Odd(W_0) \cap W_0^C \cap I^C = \emptyset$ and $P = \bigotimes_{v\in V(G)} P_v$ be a Pauli operator defined as follows:

$$\forall v \in V(G), P_v = \begin{cases} X & \text{if } v \in W_0 \text{ and } v \notin Odd(W_0)\\ Y & \text{if } v \in W_0 \cap Odd(W_0)\\ I & \text{otherwise}\end{cases}$$

Let $|\phi_0\rangle = |+\rangle_{W_0\cap I} \otimes |0\rangle_{W_0^C\cap I}$ be an input state. Notice that

$$\begin{aligned}
PE_G|+\rangle_{I^C}|\phi_0\rangle &= (-1)^{|E(W_0)|}E_G X_{W_0} Z_{Odd(W_0)\cap W_0^C}|+\rangle_{I^C}|\phi_0\rangle\\
&= (-1)^{|E(W_0)|}E_G X_{W_0}|+\rangle_{I^C\cup W_0} Z_{Odd(W_0)\cap W_0^C}|0\rangle_{W_0^C\cap I}\\
&= (-1)^{|E(W_0)|}E_G|+\rangle_{I^C}|\phi_0\rangle,
\end{aligned}$$

where $E(W) = E \cap (W \times W)$ is the set of the internal edges of W. Thus $E_G|+\rangle_{I^C}|\phi\rangle_0$ is an the eigenvector of P associated with the eigenvalue $(-1)^{|E(W_0)|}$, implying that if each qubit $v \in W_0$ is individually measured according to the observable P_v producing the classical outcome $s_v \in \{0,1\}$, then $\sum_{v\in W_0} s_v = |E(W_0)| \mod 2$. As a consequence, for the input $|\phi_0\rangle$ and any set of measurements $\{\alpha_v\}_{v\in O^C}$ s.t. $\alpha_v = 0$ if $v \in W_0 \cap Odd(W_0)^C$ and $\alpha_v = \pi/2$ if $v \in W_0 \cap Odd(W_0)$, all the branches $\mathbf{s}$ s.t. $\sum_{v\in W_0}\mathbf{s}_v = 1 + |E(W_0)| \mod 2$ occur with probability 0. □

Theorem 6. *An open graph (G, I, O) guarantees uniform constant probability iff*

$$\forall W \subseteq O^C, Odd(W) \subseteq W \cup I \implies L(W) \cap I = \emptyset$$

where $L(W) := Odd(W) \cup W$.

A nonempty set $W \subseteq O^C$ such that $Odd(W) \subseteq W \cup I$ and $L(W) \cap I \neq \emptyset$ is called a strongly internal set. Theorem 6 says that an open graph (G, I, O)

guarantees uniform constant probability if and only if it has no strongly internal set, or equivalently if and only if all internal sets are 'far enough' from the inputs.

Proof. (*if*) First we assume that there is no strongly internal set and we show that every branch occurs with a probability independent of the input. Using the notations of the proof of Theorem 5, it only remains to prove that p_u is independent of the input for any $u \neq 0$ such that $I^C \cap V_u^C \cap Odd(V_u) = \emptyset$ and $L(V_u) \cap I = \emptyset$. Note that $Odd(V_u) \subseteq V_u \subseteq I^C$ so

$$\begin{aligned} p_u &= \langle \phi_G| \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left\langle\tfrac{1+u}{2}\right|_{V_u} X_{V_u} |\phi_G\rangle \\ &= (-1)^{|E(V_u)|} \langle \phi_G| \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left\langle\tfrac{1+u}{2}\right|_{V_u} E_G Z_{Odd(V_u)} X_{V_u} |+\rangle_{I^C} |\phi\rangle_I \\ &= (-1)^{|E(V_u)|} \langle \phi_G| \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left\langle\tfrac{1+u}{2}\right|_{V_u} E_G Z_{Odd(V_u)} |+\rangle_{I^C} |\phi\rangle_I \\ &= (-1)^{|E(V_u)|+|V_u \cap Odd(V_u)|} \langle \phi_G| \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left\langle\tfrac{1+u}{2}\right|_{V_u} |\phi_G\rangle \end{aligned}$$

Moreover, for any $v \in V_u$, since $v \in I^C$, $\langle \phi_G| \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left\langle\tfrac{1+u}{2}\right|_{V_u} |\phi_G\rangle$

$$\begin{aligned} &= \tfrac{1}{2} \textstyle\sum_{a,b\in\{0,1\}} \left\langle \phi_{G\setminus v}\right| \langle a|_v Z^a_{\mathcal{N}_G(v)} \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left\langle\tfrac{1+u}{2}\right|_{V_u} Z^b_{\mathcal{N}_G(v)} |b\rangle_v \left|\phi_{G\setminus v}\right\rangle \\ &= \tfrac{1}{2} \left\langle \phi_{G\setminus v}\right| Z^{\frac{1+u_v}{2}}_{\mathcal{N}_G(v)} \left|\tfrac{1+u}{2}\right\rangle_{V_u\setminus v} \left\langle\tfrac{1+u}{2}\right|_{V_u\setminus v} Z^{\frac{1+u_v}{2}}_{\mathcal{N}_G(v)} \left|\phi_{G\setminus v}\right\rangle \\ &= \tfrac{1}{2} \left\langle \phi_{G\setminus v}\right| \left|\tfrac{1+u}{2}\right\rangle_{V_u\setminus v} \left\langle\tfrac{1+u}{2}\right|_{V_u\setminus v} \left|\phi_{G\setminus v}\right\rangle \end{aligned}$$

So, by induction, $\langle \phi_G| \left|\tfrac{1+u}{2}\right\rangle_{V_u} \left\langle\tfrac{1+u}{2}\right|_{V_u} |\phi_G\rangle = \frac{1}{2^{|V_u|}} \left\langle \phi_{G\setminus V_u}\right| \left|\phi_{G\setminus V_u}\right\rangle = \frac{1}{2^{|V_u|}}$. This shows that p_u does not depend on the input state.

(*only if*) Now we prove that the existence of a strongly internal set implies that there exists a particular set of measurement angles such that some branches occur with probability zero for some input state and with nonzero probability for other inputs. Let $W_0 \subseteq O^C$ s.t. $Odd(W_0) \cap W_0^C \cap I^C = \emptyset$, $u_0 \in L(W_0) \cap I$, and $P = \bigotimes_{v\in V} P_v$ be a Pauli operator defined like in the proof of Theorem 5. We consider the following input states: $|\phi_a\rangle = |+\rangle_{W_0\cap I} \otimes |0\rangle_{W_0^C\cap I\setminus u_0} \otimes |a\rangle_u$ for $a \in \{0,1\}$. Notice that $PE_G |+\rangle_{I^C} |\phi_a\rangle_I = (-1)^{a+|E(W_0)|} E_G |+\rangle_{I^C} |\phi_a\rangle_I$. Let $\alpha_v = \pi/2$ if $v \in W_0 \cap Odd(W_0)$ and $\alpha_v = 0$ otherwise. We consider a branch $\mathbf{s}$ of measurement which occurs with a nonzero probability if the input state is $|\phi_0\rangle$. Notice that this branch satisfies $\sum_{v\in W_0} \mathbf{s}_v = (-1)^{|E(W_0)|}$. As a consequence, if the input state is $|\phi_1\rangle$, this branch $\mathbf{s}$ occurs with probability 0. □

5 Uniform Equiprobability Versus Gflow Existence

Since the existence of a gflow implies uniform strong determinism it also implies uniform equiprobability. In general uniform equiprobability does not imply gflow:

Lemma 2. *When $|I| \neq |O|$, there exists an open graph that satisfies uniform equiprobability but that has no gflow.*

Proof. Consider the graph depicted in Fig. 1. It is easy to see that it has no gflow, as no subset of the outputs has a single vertex as its odd neighorhood. On the other hand, all the subsets of O^C have a nonempty external odd neighborhood in I^C. □

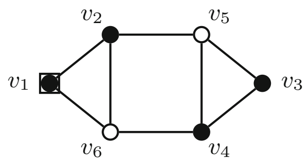

Fig. 1. Open graph (G, I, O) with $I = \{v_1\}$ and $O = \{v_5, v_6\}$ satisfying the uniform equiprobability condition but having no gflow.

However, in the particular case where $|I| = |O|$, the existence of a gflow implies uniform equiprobability.

Theorem 7. *When $|I| = |O|$, (G, I, O) guarantees uniform equiprobability iff it has a gflow.*

Proof. We only have to prove that uniform equiprobability implies the existence of gflow (the other direction is obvious). We prove the existence of a gflow for (G, O, I) which, according to Theorem 4, implies the existence of a gflow for (G, I, O). Since (G, I, O) is uniformly equiprobable, the matrix $A_G|_{O^C}^{I^C}$ is injective, so reversible. Indeed, for any $W \subseteq O^C$, $A_G|_{O^C}^{I^C}.1_W = \emptyset \iff 1_{Odd(W)\cap I^C} = 0 \implies Odd(W) \subseteq I \subseteq W \cup I$ so $W = \emptyset$. The matrix $\left(A_G|_{O^C}^{I^C}\right)^{-1}$ is the induced matrix of a directed open graph (H, O, I), where H is chosen s.t. vertices in O have no successor. In the following we show that H is a DAG. By contradiction, let $S \subseteq V(H)$ be the shortest cycle in H. Notice that $S \subseteq O^C$ since vertices in O have no successor. $A_G|_{O^C}^{I^C}.(A_G|_{O^C}^{I^C})^{-1}.1_S = 1_S \iff A_G|_{O^C}^{I^C}.1_{Odd_H(S)\cap O^C} = 1_S \iff Odd_G(Odd_H(S) \cap O^C) \cap I^C = S$. Let $W := Odd_H(S) \cap O^C$. Since S is the shortest cycle, $S \subseteq Odd_H(S)$. Moreover $S \subseteq O^C$ so $S \subseteq W$. Thus $Odd_G(W) \subseteq W \cup I^C$ which implies $W = \emptyset$, so $S = \emptyset$. Thus H is a DAG. □

Notice that thanks to Theorem 7 the stepwise condition in the characterisation of gflow can be removed, improving Theorem 1:

Corollary 1. *When $|I| = |O|$, (G, I, O) guarantees uniform strong determinism iff it has a gflow.*

Proof. Uniform strong determinism implies equiprobability which ensures the existence of gflow when $|I| = |O|$. □

6 Choosing Inputs and Outputs

The fact that the characterisation of uniform equi-probability is by excluded internal sets allows us to have a better view of the following general problem: given a graph, which vertices can be chosen as outputs and inputs for measurement based quantum information processing.

Definition 9. *Given a graph G, for any $A \subseteq V(G)$, let $\mathcal{E}_A$ be the collection of internal sets outside A: $\mathcal{E}_A := \{S \subseteq V(G), S \neq \emptyset \wedge Odd(S) \cap S^C \cap A^C = \emptyset\}$*

A transversal of a collection C of sets is a set that intersects all the elements of C. The set of all transversals of $\mathcal{E}_A$ is $T(\mathcal{E}_A) := \{S' \subseteq V(G), {}^\forall S \in \mathcal{E}_A \;\; S' \cap S \neq \emptyset\}$.

Lemma 3. *If an open graph (G, I, O) guarantees uniform equiprobability then $O \in T(\mathcal{E}_\emptyset)$.*

Proof. By contradiction if $W \in \mathcal{E}_\emptyset$ and $W \cap O = \emptyset$, then $Odd(W) \cap W^C = \emptyset$, so $Odd(W) \subseteq W \cup I^C$ which implies $W = \emptyset$. It contradicts the fact that $W \in \mathcal{E}_\emptyset$. □

Theorem 8. *An open graph (G, I, O) guarantees uniform equiprobability if and only if $O \in T(\mathcal{E}_I)$.*

Proof. $O \in T(\mathcal{E}_I) \iff \forall W \in \mathcal{E}_I, W \cap O \neq \emptyset \iff \forall W \subseteq O^C, W \notin \mathcal{E}_I \iff \forall W \subseteq O^C, \neg(Odd(W) \cap W^C \cap I^C \wedge W \neq \emptyset) \iff \forall W \subseteq O^C, (Odd(W) \subseteq W \cup I \Rightarrow W = \emptyset)$. □

Theorem 9. *Given a graph G and two subsets of vertices I and O with $|I| = |O|$, the open graph (G, I, O) guarantees equiprobability iff $I \in T(\mathcal{E}_\emptyset)$ and $O \in T(\mathcal{E}_I)$.*

Proof. When $|I| = |O|$, if (G, I, O) guarantees equiprobability then (G, I, O) has a gflow (Theorem 7) and thus (G, O, I) has a gflow (Theorem 4) as well. As a consequence (G, I, O) guarantees uniform equiprobability so $I \in T(\mathcal{E}_\emptyset)$. □

This observation allows a characterisation of the possible deterministic computations for small graphs. The main question is, given a graph G, how to find $I \subseteq V(G)$ and $O \subseteq V(G)$ with $|I| = |O|$ such that (G, I, O) has gflow.

Furthermore it is straightforward to see that :

Lemma 4. *If an open graph (G, I, O) guarantees uniform equi-probability then (G, I', O') with $I' \subseteq I$ and $O \subseteq O'$ also guarantees uniform equi-probability.*

Notice that gflow and constant probability classes are also stable by adding new outputs or removing inputs. Thus the interesting problem when choosing inputs and outputs consists of minimizing $|O|$ and maximizing $|I|$.

Thus one can take minimal elements in $T(\mathcal{E}_\emptyset)$ as inputs I and then look for minimal elements in $T(\mathcal{E}_I)$. If they have the same size then we can conclude that they are a proper input/output pair for deterministic computation. This allows one to characterise the possible deterministic computations for small graphs (as it is not polynomial to compute the big transversal sets). For instance in the case of the 2 × 3 grid, the test shows that the minimal number of outputs is 2 and that there are only 3 solutions up to symmetry (see Fig. 2).

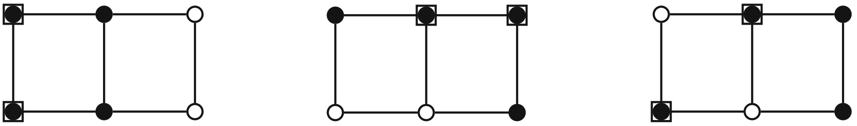

Fig. 2. Uniform deterministic choice of inputs for the 2×3 grid – input (resp. output) vertices are represented by squared (resp. white) vertices.

7 Uniform Constant Probability

The constant probability case is at the same time the most general case where information is not lost during the measurement and the less understood case. In this last section, we investigate some properties of the graph states that guarantee constant probability. We show a decomposition theorem into a gflow part and an internal set and we characterise open graphs with constant probability in the particular case of one input and one output. We also prove a reversibility property in the considered cases.

Lemma 5. *If an open graph (G, I, O) with $|I| = |O|$ guarantees uniform constant probability then there exists a subgraph G' of G such that (G', I, O) has a gflow and $V(G) \setminus V(G')$ is an internal set.*

Proof. Inductively removing the empty neighborhood subsets (W such that $Odd(W) \cap W^C = \emptyset$) leaves an open graph with gflow. □

Theorem 10. *An open graph (G, I, O) with $|I| = |O| = 1$ guarantees uniformly constant probability if and only if $\forall u \in V(G)$,*

$$d(u) = 1 \mod 2 \iff u \in I \Delta O$$

where $d(u) = |\mathcal{N}_G(u)|$ is the degree of u.

Proof. Consider a constant probability open graph $(G, \{i\}, \{o\})$, by definition there is no strongly internal set. We prove by contradiction that if $i = o$ then all the vertices have even degree and that if $i \neq o$ the input and output vertices have odd degree and all the other vertices have an even degree. Indeed:

- if $i = o$ then
  - if $d(i) = 1 \mod 2$ then $V(G) \setminus \{i\}$ is a strongly internal set.
  - if $d(i) = 0 \mod 2$ and there exists $u \neq i$, $d(u) = 1 \mod 2$. Consider the shortest path P between the output and a vertex of odd degree. $Odd(G \setminus P) \cap (G \setminus P)^C = \{i\}$ thus $V(G) \setminus P$ is a strongly internal set.
- if $i \neq o$ then
  - if $d(o) = 0 \mod 2$ then $V(G) \setminus \{o\}$ is a strongly internal set.
  - if $d(o) = 1 \mod 2$, then if there exists $u \notin \{i, o\}$ with $d(u) = 1 \mod 2$.

Consider the shortest path P between the output and a non input vertex of odd degree. If $i \notin P$ then $Odd(G\setminus P)\cap(G\setminus P)^C = \emptyset$ thus $V(G)\setminus P$ is a strongly internal set. Otherwise, if $d(i) = 1 \mod 2$ then $Odd(G \setminus P) \cap (G \setminus P)^C = \{i\}$ thus $V(G) \setminus P$ is a strongly internal set. Otherwise consider $P' \subset P$ the part of the path form o to i, $Odd(G \setminus P') \cap (G \setminus P')^C = \{i\}$ thus $V(G) \setminus P'$ is a strongly internal set. If $d(i) = 0 \mod 2$, then, as the sum of the degrees is even, there exists $u \notin \{i, o\}$ with $d(u) = 1 \mod 2$ and thus a strongly internal set.

For the other direction, suppose that $(G, \{i\}, \{o\})$ satisfies that $\forall u \in V(G)$, $d(u) = 1 \mod 2$ *iff* $u \in \{i\}\Delta\{o\}$. For any subset S of $V(G)\setminus\{i, o\}$ as $\sum_{v\in S} d(v) = 0 \mod 2$, $|Odd(S) \cap S^C| = 0 \mod 2$ and thus there is no strongly internal set if $i = o$. Furthermore, if $i \neq o$, for any set S of $V(G) \setminus \{o\}$ containing i, S contains one vertex of odd degree thus $|Odd(S) \cap S^C| = 1 \mod 2$ and therefore there is no strongly internal set. □

8 Open Questions

This work raises several open questions, from the structural point of view. For example, it is not known whether the uniform constant probability case is reversible when $|I| = |O|$. From a complexity perspective: is it possible to derive a polynomial algorithm to characterise the uniform equiprobability class and the uniform constant probability class? Is it possible to derive an efficient algorithm for finding inputs and ouputs?

Acknowledgements. The authors want to thank E. Kashefi for discussions. This work is supported by CNRS-JST Strategic French-Japanese Cooperative Program, and Special Coordination Funds for Promoting Science and Technology in Japan.

References

1. Browne, D.E., Kashefi, E., Mhalla, M., Perdrix, S.: Generalized flow and determinism in measurement-based quantum computation. New J. Phys. **9**, 250 (2007)
2. Danos, V., Kashefi, E., Panangaden, P.: The measurement calculus. J. ACM **54**, 2 (2007)
3. Danos, V., Kashefi, E., Panangaden, P., Perdrix, S.: Extended measurement calculus. In: Gay, S., Mackie, I. (eds.) Semantic Techniques in Quantum Computation. Cambridge University Press, Cambridge (2010)
4. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. thesis, California Institute of Technology, Pasadena (1997)
5. Hein, M., Eisert, J., Briegel, H.J.: Multi-party entanglement in graph states. Phys. Rev. A **69**, 062311 (2004)
6. Kashefi, E., Markham, D., Mhalla, M., Perdrix, S.: Information flow in secret sharing protocols. In: Developments in Computational Models (DCM'09), EPTCS 9, pp. 87–97 (2009)
7. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Phys. Rev. A **78**, 042309 (2008)

8. Mhalla, M., Perdrix, S.: Finding optimal flows efficiently. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part I. LNCS, vol. 5125, pp. 857–868. Springer, Heidelberg (2008)
9. Raussendorf, R., Briegel, H.: A one-way quantum computer. Phys. Rev. Lett. **86**, 5188 (2001)
10. Van den Nest, M., Dehaene, J., De Moor, B.: Graphical description of the action of local Clifford transformations on graph states. Phys. Rev. A **69**, 22316 (2004)
11. Van den Nest, M., Miyake, A., Dür, W., Briegel, H.J.: Universal resources for measurement-based quantum computation. Phys. Rev. Lett. **97**, 150504 (2006)