# Beyond Determinism in Measurement-based Quantum Computation

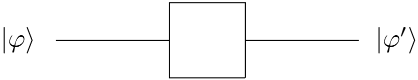
Simon Perdrix

CNRS, Laboratoire d'Informatique de Grenoble

Joint work with Mehdi Mhalla, Mio Murao, Masato Someya, Peter Turner

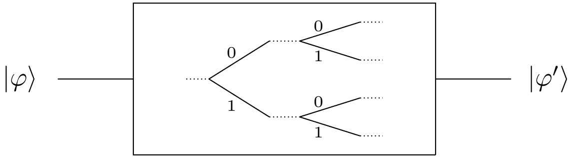
NWC, 23/05/2011
ANR CausaQ
CNRS-JST Strategic French-Japanese Cooperative Program

# Quantum Information Processing (QIP)




- Quantum computation
- Quantum protocols

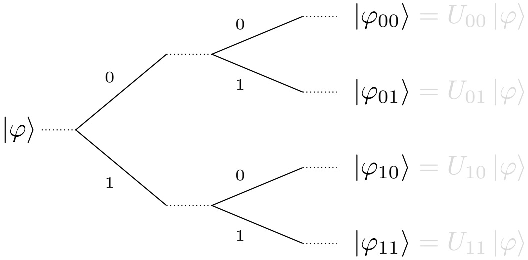
# QIP involving measurements




- Models of quantum computation:
  - Measurement-based QC with graph states (One-way QC)
  - Measurement-only QC
- Quantum protocols:
  - Teleportation
  - Blind QC
  - Secret Sharing with graph states
- To model the environment:
  - Error Correcting Codes

# Information-Preserving Evolution

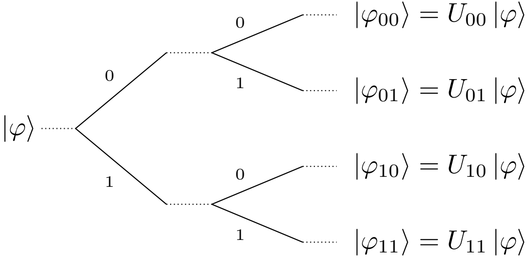
**Information preserving** $=$ **each branch is reversible**
$=$ **each branch is equivalent to an isometry**



# Information-Preserving Evolution

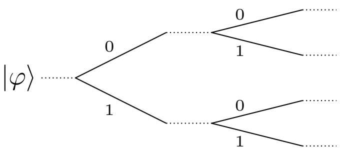
**Information preserving** $\quad = \quad$ **each branch is reversible**

$\quad = \quad$ **each branch is equivalent to an isometry**




where $\forall b, U_b$ is an isometry i.e. $\forall\,|\varphi\rangle\,, ||U_b\,|\varphi\rangle\,|| = ||\,|\varphi\rangle\,||$.

# Information-Preserving Evolution




$$|\varphi_{00}\rangle = U_{00}\,|\varphi\rangle$$
$$|\varphi_{01}\rangle = U_{01}\,|\varphi\rangle$$
$$|\varphi_{10}\rangle = U_{10}\,|\varphi\rangle$$
$$|\varphi_{11}\rangle = U_{11}\,|\varphi\rangle$$

## Theorem

*A computation is info. preserving $\iff$ the probability of each branch is independent of the initial state $|\varphi\rangle$.*

**Proof ($\Leftarrow$):** For each branch, at $i$th measurement:

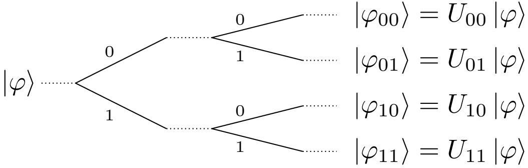
$$\left|\varphi^{(i)}\right\rangle \xmapsto[\text{prob. } p_k = ||P_k \left|\varphi^{(i)}\right\rangle||^2]{P_k} \frac{1}{\sqrt{p_k}} P_k \left|\varphi^{(i)}\right\rangle =: \left|\varphi^{(i+1)}\right\rangle$$

By induction $\left|\varphi^{(i)}\right\rangle = U^{(i)}\,|\varphi\rangle$, so $\left|\varphi^{(i+1)}\right\rangle = \frac{1}{\sqrt{p_k}} P_k U^{(i)}\,|\varphi\rangle$.

$U^{(i+1)} := \frac{1}{\sqrt{p_k}} P_k U^{(i)}$ is an isometry since for any $|\varphi\rangle$ s.t. $||\,|\varphi\rangle\,|| = 1$,

$$||\frac{1}{\sqrt{p_k}} P_k U^{(i)}\,|\varphi\rangle\,|| = \frac{1}{\sqrt{p_k}} ||P_k U^{(i)}\,|\varphi\rangle\,|| = \frac{||P_k U^{(i)}|\varphi\rangle||}{||P_k U^{(i)}|\varphi\rangle||} = 1$$

# Information-Preserving Evolution




## Theorem

*A computation is info. preserving* $\iff$ *the probability of each branch is independent of the initial state* $|\varphi\rangle$.

**Proof ($\Leftarrow$):** For each branch, at $i$th measurement:

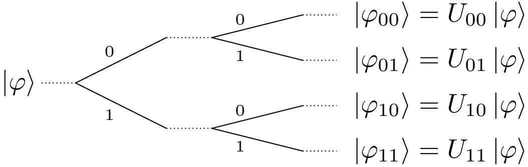
$$\left|\varphi^{(i)}\right\rangle \xmapsto[\text{prob. } p_k = ||P_k \left|\varphi^{(i)}\right\rangle||^2]{P_k} \frac{1}{\sqrt{p_k}} P_k \left|\varphi^{(i)}\right\rangle =: \left|\varphi^{(i+1)}\right\rangle$$

By induction $\left|\varphi^{(i)}\right\rangle = U^{(i)}|\varphi\rangle$, so $\left|\varphi^{(i+1)}\right\rangle = \frac{1}{\sqrt{p_k}} P_k U^{(i)} |\varphi\rangle$.

$U^{(i+1)} := \frac{1}{\sqrt{p_k}} P_k U^{(i)}$ is an isometry since for any $|\varphi\rangle$ s.t. $||\,|\varphi\rangle\,|| = 1$,

$$||\frac{1}{\sqrt{p_k}} P_k U^{(i)} |\varphi\rangle\,|| = \frac{1}{\sqrt{p_k}} ||P_k U^{(i)} |\varphi\rangle\,|| = \frac{||P_k U^{(i)}|\varphi\rangle||}{||P_k U^{(i)}|\varphi\rangle||} = 1$$

# Information-Preserving Evolution



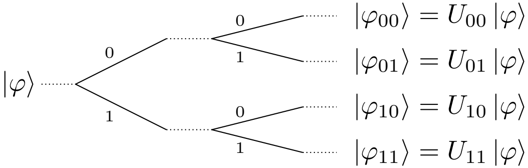

## Theorem

*A computation is info. preserving* $\iff$ *the probability of each branch is independent of the initial state* $|\varphi\rangle$*.*

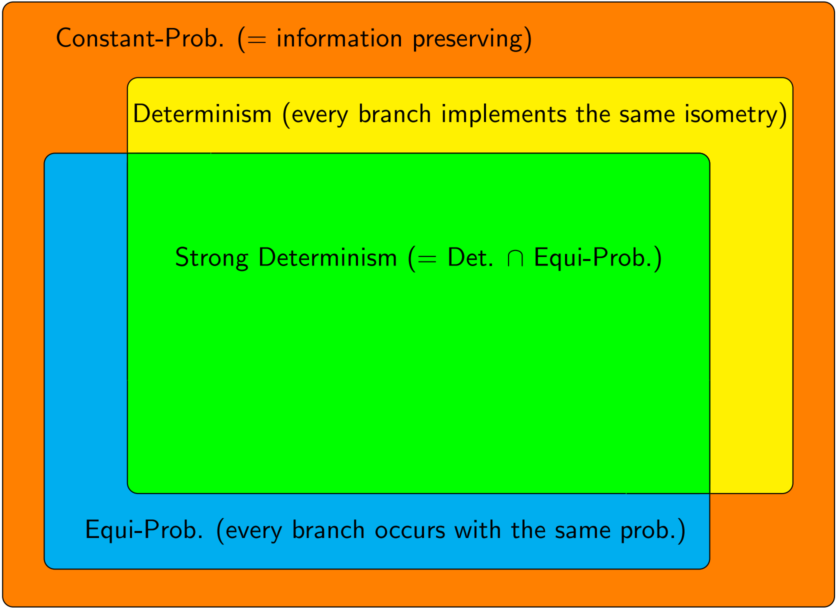
**Proof ($\Rightarrow$):** (intuition)

$$\text{Dependent probability} \implies \text{Disturbance} \implies \text{Irreversibility.}$$

# Information-Preserving Evolution



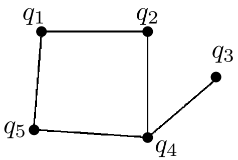

- **Constant Probability** = Information Preserving: every branch occur with a probability independent of the input state.
- **Equi-probability**: every branch occurs with the same probability.
- **Determinism**: every branch implements the same isometry $U$.
- **Strong Determinism**: determinism and equi-probability.


Constant-Prob. (= information preserving)
Determinism (every branch implements the same isometry)
Strong Determinism (= Det. ∩ Equi-Prob.)
Equi-Prob. (every branch occurs with the same prob.)

# Quantum Information Processing

# with Graph states.

# Graph States

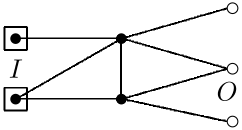



For a given graph $G = (V, E)$, let $|G\rangle \in \mathbb{C}^{2^{|V|}}$

$$|G\rangle \quad = \quad \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{q(x)} |x\rangle$$

where $q(x) = x^T.\Gamma.x$ is the number of edges in the subgraph $G_x$ induced by the subset of vertices $\{q_i \mid x_i = 1\}$.

# Open Graph States




Given an open graph $(G, I, O)$, with $I, O \subseteq V(G)$ and $|\varphi\rangle \in \mathbb{C}^{2^{|I|}}$, let

$$|G_\varphi\rangle \quad = \quad N\,|\varphi\rangle$$

where

$$N : |y\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{q(y,x)}\,|y, x\rangle$$

# Measurements / Corrections

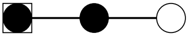
- Measurement in the $(X, Y)$-plane: for any $\alpha$,

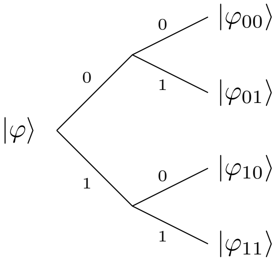
$$\cos(\alpha)X + \sin(\alpha)Y$$

$$\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle)\}$$

- Measurement of qubit $i$ produces a classical outcome $s_i \in \{0, 1\}$.
- Corrections $X^{s_i}, Z^{s_i}$

# Probabilistic Evolution



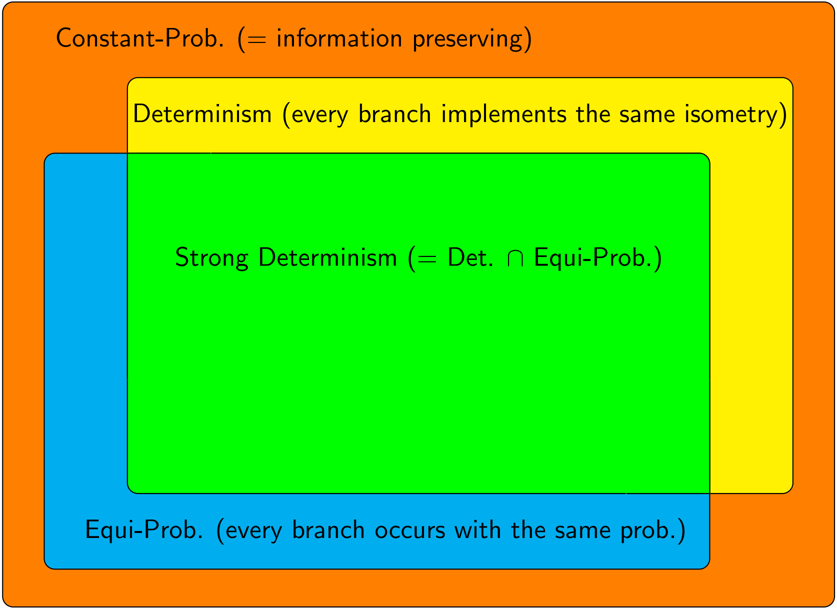


# Uniformity

The evolution depends on:

- the initial open graph $(G, I, O)$;
- the angle of measurements $(\alpha_i)$ ;
- the correction strategy ;

**Focusing on combinatorial properties:**
$(G, I, O)$ guarantees **uniform** determinism (resp. constant probability, equi-probability, ...) if there exists a correction strategy that makes the computation deterministic (resp. constant probabilistic, equi-probabilistic, ...) for **any** angle of measurements.


Constant-Prob. (= information preserving)
Determinism (every branch implements the same isometry)
Strong Determinism (= Det. ∩ Equi-Prob.)
Equi-Prob. (every branch occurs with the same prob.)

# Sufficient conditon for Strong Det.: Gflow

## Theorem (BKMP'07)

*An open graph guarantees uniform strong determinism if it has a gflow.*

## Definition (Gflow)

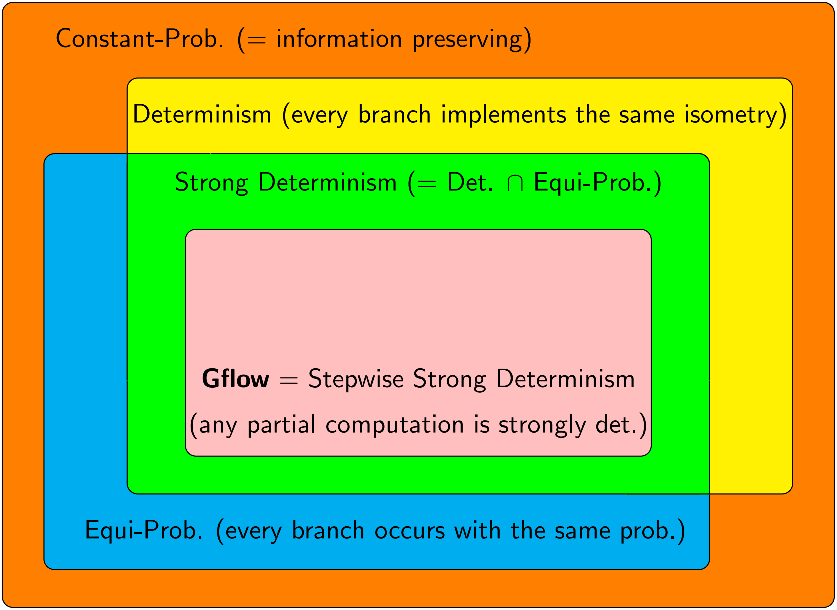
$(g, \prec)$ is a **gflow** of $(G, I, O)$, where $g : O^c \to 2^{I^c}$, if for any $u$,

— if $v \in g(u)$, then $u \prec v$
— $u \in Odd(g(u)) = \{v \in V, |N(v) \cap g(u)| = 1[2]\}$
— if $v \prec u$ then $v \notin Odd(g(u))$.

## Theorem (MMPST'11)

$(G, I, O)$ *has a gflow iff* $\exists$ *a DAG* $F$ *s.t.*

$$A_{(G,I,O)}.A_{(F,O,I)} = 1$$




Open question: Strong determinism = Gflow?

# Characterisation of Equi Prob.

## Theorem

*An open graph* $(G, I, O)$ *guarantees uniform equi. probability iff*

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

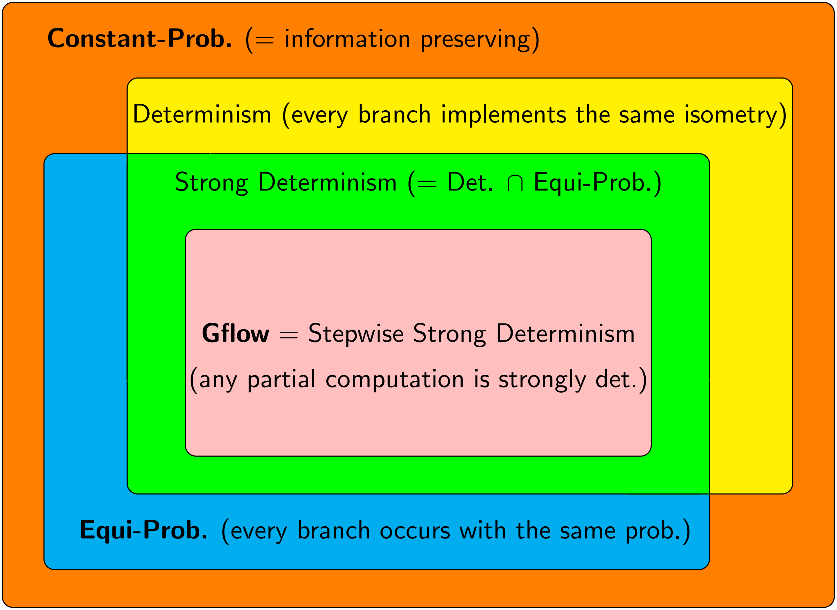
*Where Odd*$(W) = \{v \in V, |N(v) \cap W| = 1 \mathit{mod} 2\}$ *is the odd neighborhood of* $W$*.*

# Characterisation of Constant Prob.

## Theorem

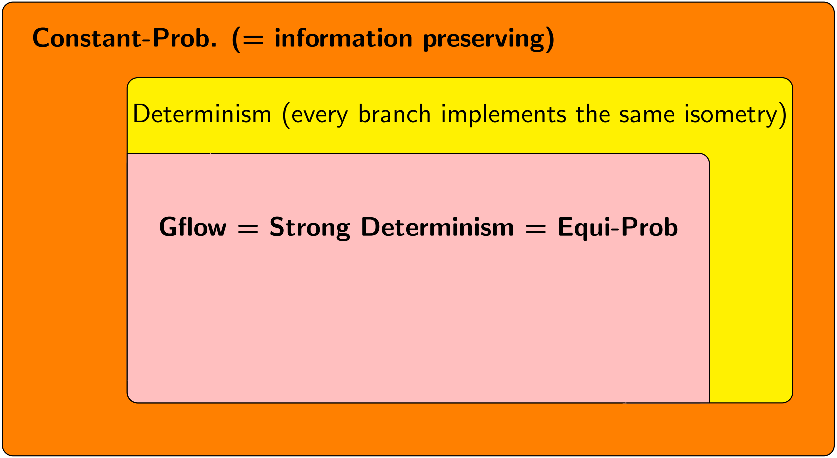
*An open graph $(G, I, O)$ guarantees uniform constant probability if and only if*

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




Open questions: Strong determinism = Gflow? Characterisation of Determinism?

# When $|I| = |O|$: Equi. Prob. $\subseteq$ Gflow



# When $|I| = |O|$

**Theorem**

*An open graph $(G, I, O)$ with $|I| = |O|$ guarantees equi-probability iff it has a gflow.*

**Corollary**

*An open graph is* **uniformly and strongly deterministic** *iff it has a gflow. (stepwise condition is not necessary in the case $|I| = |O|$)*

# Sketch of the proof

**Lemma**

*If $|I| = |O|$, $(G, I, O)$ has a gflow iff $(G, O, I)$ has a gflow.*

**Proof.**

$$\begin{array}{rcrl} & A_{(G,I,O)}.A_{(F,O,I)} & = & I \\ \iff & (A_{(G,I,O)}.A_{(F,O,I)})^T & = & I \\ \iff & A^T_{(F,O,I)}.A^T_{(G,I,O)} & = & I \\ \iff & A_{(F,I,O)}.A_{(G,O,I)} & = & I \\ \iff & A_{(G,O,I)}.A_{(F,I,O)} & = & I \end{array}$$

□

# Sketch of the proof

### Lemma

*If $|I| = |O|$, $(G, I, O)$ has a gflow iff $(G, O, I)$ has a gflow.*

### Lemma

*If $(G, I, O)$ is uniformly equi-probability then $(G, O, I)$ has a gflow.*

Idea of the proof:

- $A_{(G,O,I)}$ is the matrix of the map $L : 2^{O^c} \to 2^{I^c} = W \mapsto Odd(W) \cap I^c$. $L$ is a linear map: $L(X \Delta Y) = L(X) \Delta L(Y)$.
- If $L(W) = \emptyset$ then $Odd(W) \subseteq I$ so $Odd(W) \subseteq W \cup I$ thus $W = \emptyset$. Hence $L$ is injective so surjective since $|I| = |O|$.
- $A^{-1}_{(G,O,I)}$ is the adjacency matrix of a directed graph $H$. Let $S$ be the smallest cycle in $H$. One can show that $Odd_G(W) \subseteq W \cap I^C$ and $S \subseteq W$, where $W := Odd_H(S) \cap O^C$, thus $W = \emptyset$ and $S = \emptyset$.

# Finding $I$ and $O$

Equiprobability:

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

## Lemma

*If $(G, I, O)$ guarantees equi-probability then $(G, I', O')$ guarantees equi-probability if $I' \subseteq I$ and $O \subseteq O'$.*

Minimization of $O$ and maximization of $I$.

# Finding $I$ and $O$

Equiprobability:

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

## Definition

Given a graph $G$, let $\mathcal{E}_X = \{S \neq \emptyset \mid \mathrm{Odd}(S) \subseteq S \cup X\}$. Let $T(\mathcal{E}_X) = \{Y, \forall S \in \mathcal{E}_X, S \cap Y \neq \emptyset\}$ be the transversal of $\mathcal{E}_X$

## Lemma

*If $(G, I, O)$ guarantees equi-probability iff $O \in T(\mathcal{E}_I)$.*

# Finding $I$ and $O$ when $|I| = |O|$

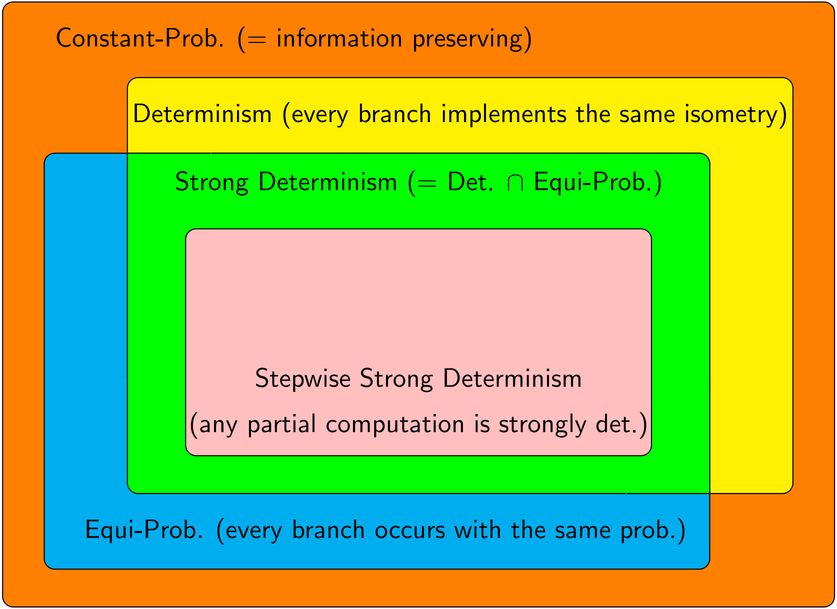
## Lemma

*For a given graph $G$, let $I = \min_{S \in T(\mathcal{E}_\emptyset)} |S|$ and $O = \min_{S \in T(\mathcal{E}_I)} |S|$. If $|I| = |O|$ then $(G, I, O)$ guarantees equiprobability.*

**Proof:** Based on the fact that $(G, I, O)$ guarantees equiprobability iff $(G, O, I)$ guarantees equiprobability when $|I| = |O|$.

# Conclusion

- Relaxing determinism condition: information preserving maps
- Information-preserving $=$ constant probability.
- Graphical characterisation of equi- and constant probability
- Equi-probability and Stong Determinism are equivalent when $|I| = |O|$.
- Stepwise condition is not necessary for GFlow when $|I| = |O|$.
- Finding $I$ and $O$ for a given graph.


Constant-Prob. (= information preserving)
Determinism (every branch implements the same isometry)
Strong Determinism (= Det. ∩ Equi-Prob.)
Stepwise Strong Determinism
(any partial computation is strongly det.)
Equi-Prob. (every branch occurs with the same prob.)