An introduction to Quantum Computing

Elham Kashefi

School of Informatics
University of Edinburgh

Overview

- Quantum Mechanics

Easy: Linear Algebra
Hard: Counter-intuitive

- Quantum Computation

Understanding Physics via Computation

- Different Models

Quantum Circuit Model
Measurement-based QC
Adiabatic QC
Quantum Cellular Automata
Topological QC

Structural relations

Quantum Computing

- A cross-disciplinary field of great importance from both a fundamental and technological perspective

- It has changed our perspective on many fundamental aspects of computing

- Common goal of computing research: The boundary between classical and quantum information processing

Logical Reversibility of Computation

C. H. Bennett (1973)

- The usual general-purpose computing automaton (e.g. a Turing machine) may be made logically reversible at every step, while retaining their simplicity and their ability to do general computations. This result is of great *physical interest* because it makes plausible the existence of thermodynamically reversible computers which could perform useful computations at useful speed while dissipating considerably less than $\kappa T \ln 2$ of energy per logical step.

– (1) Saving all intermediate results to avoid the irreversible operation of erasure
– (2) Printing outputs
– (3) Disposing undesired intermediate results, leaving only the output and input

Informally

– Start with reversible but untidy computer with its history tape
– Exploit the relationship between history tape and the machine that is produced for erasing it

$$
\begin{aligned}
(x), (\text{blank}) &\rightarrow (f(x))(\text{blank}) \\
&\rightarrow (f(x)), (f(x)) \\
&\rightarrow (f^{-1}(f(x))), (f(x)) \\
&\rightarrow (x), (f(x))
\end{aligned}
$$

Reversible Turing Machine

Theorem 1 $\forall$ *standard one-tape Turing machine* S, $\exists$ *a three-tape reversible, deterministic Turing machine* R *such that if* I *and* P *are strings on the alphabet of* S, *containing no embedded blanks, then* S *halts on* I *if and only if* R *halts on* $(I; B; B)$, *and* $S : I \rightarrow P$ *if and only if* $R : (I; B; R) \rightarrow (I; B; P)$.

Reversible Logic Gate

- A logic gate L is reversible if, for any output y, there is a unique input x such that applying $L(x) = y$.

Toffoli gate: $(a, b, c) \rightarrow (a, b, c \oplus a \wedge b)$

Theorem 2 *Toffoli gate is universal:* $\forall$ *boolean function* f, $\exists$ *a circuit consisting of Toffoli gates which*

$$(x_1, ..., x_m)(0, ..., 0) \mapsto (x_1, ..., x_m), f(x_1, ..., x_m)$$

Birth of QC

- It is possible to perform computation both *logically* and *thermodynamically* reversible.

- Quantum physics is also reversible, as the reverse-time evolution specified by the unitary operator $U^{-1} = U^{\dagger}$ always exists.

CC vs QC

- CC is a small subset of QC: the time evolution is unitary matrix with 0 and 1, rather than arbitrary complex number.

- Unitary time evolution can be *simulated* by a classical computer BUT the dimension of the unitary is bounded by the number of classical degrees of freedom.

CC vs QC

- CC is a small subset of QC: the time evolution is unitary matrix with 0 and 1, rather than arbitrary complex number.

- Unitary time evolution can be *simulated* by a classical computer BUT the dimension of the unitary is bounded by the number of classical degrees of freedom.

- QC with m physical bits can perform unitary operations in a space of 2^m dimensions, exponentially larger than its physical size.

Quantum Effects

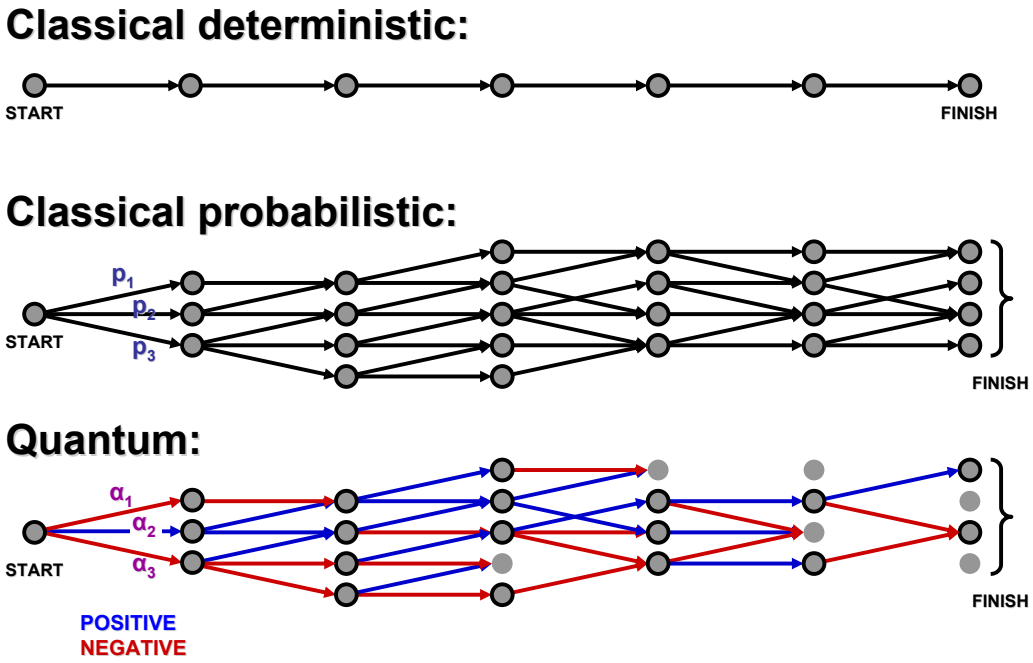
New types of behavior to make use of

- Measuring a state disturbs it
- Q systems sometimes behave as if they are in several states at once
- Different evolutions can interfere with each other

Quantum Effects

New types of behavior to make use of

- Measuring a state disturbs it
- Q systems sometimes behave as if they are in several states at once
- Different evolutions can interfere with each other



(Figure is taken from Richard Cleve Course)

QC Applications

- New algorithms that out-speed classical computing
- New unconditionally secure cryptographic protocols
- New discovery in physics (entanglement theory)
- New perspective on information theory

Research Directions

- The boundary between classical and quantum processing
- Models of quantum computing and their structural relations
- New applications, algorithms and protocols
- Physical implementations
- Comparison measures
- Fault tolerance QC
- Entanglement

QC

A quantum computation takes place in some $\mathfrak{H}_n := \otimes^n \mathbb{C}^2$.

State is represented as a non zero vector.

Evolution consists in:
— preparation maps (increasing the computation space)
— unitary transformations (reversible)
— measurements (decreasing the computation space)

The exact blend of such transformations determine different models.
— *Circuit* model has only a selection of 1- or 2-qubit unitary transformations (and measurements at the end)
— *1WQC* has preparations of $|+_\alpha\rangle$, $\wedge Z$, 1-qbit measurements, and Pauli maps
— *TQC* uses 2-qubit measurements instead of 1-qubit ones

2-state system $\mathbb{C}^2$

The canonical basis, $(1,0)$, $(0,1)$, also called the computational basis, is usually denoted $|0\rangle$, $|1\rangle$. It is orthonormal by definition of $\langle x, y\rangle_{\mathbb{C}^2}$.

Another orthonormal basis:

$$|\pm\rangle := \tfrac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

and yet another:

$$|\pm_\alpha\rangle := \tfrac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle)$$

The *preparation* map N_i^α is defined to be:

$$|+_\alpha\rangle \otimes \_ : \mathfrak{H}_n \to \mathbb{C}^2 \otimes \mathfrak{H}_n$$

Maps over $\mathbb{C}^2$

We write X and Z for the Pauli spin matrices:

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and H and $P(\alpha)$ for the Hadamard and phase operator:

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad P(\alpha) := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

All these maps are unitaries, and all self-adjoint except $P(\alpha)^\star = P(-\alpha)$.

The 2-qubit space: $\mathbb{C}^2 \otimes \mathbb{C}^2$

$\mathbb{C}^2 \otimes \mathbb{C}^2$ also has a canonical basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Bases need not be made of decomposable elements, they can use entangled elements. Here is another example (important for 1WQC), *Graph basis*, $\mathcal{G}$:

$$\begin{aligned}
\mathcal{G}_{00} &= \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \\
\mathcal{G}_{01} &= \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle) \\
\mathcal{G}_{10} &= \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle) \\
\mathcal{G}_{11} &= \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)
\end{aligned}$$

Classical vs Quantum Sates

- Classical many particle space is Cartesian product of single particle space

$$Z^{\times n} = Z \times \ldots Z$$

- Quantum many particle space is tensor product of single particle space

$$\mathcal{H}^{\otimes n} = \mathcal{H} \times \ldots \mathcal{H}$$

- The quantum sate of n particles:

$$\sum_{i=0}^{i=2^n} a_i |x_i\rangle$$

Maps on $\mathbb{C}^2 \otimes \mathbb{C}^2$

- In general if $f : A \to B$ and $g : A' \to B'$, one defines $f \otimes g : A \otimes A' \to B \otimes B' : \psi \otimes \phi \mapsto f(\psi) \otimes g(\phi)$.

- Or given $f : \mathbb{C}^2 \to \mathbb{C}^2$, one defines $\wedge f$ (read controlled-f) a new map on $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$\begin{aligned} \wedge f|0\rangle|\psi\rangle &:= |0\rangle|\psi\rangle \\ \wedge f|1\rangle|\psi\rangle &:= |1\rangle f(|\psi\rangle) \end{aligned}$$

In particular one has $\wedge Z$ which is symmetric ($\sigma \wedge Z \sigma = \wedge Z$):

$$\wedge Z(|+\rangle \otimes |+\rangle) = \mathcal{G}_{00}$$

Pauli and Clifford

Define the *Pauli group* over A as the closure of $\{X_i, Z_i \mid 1 \leq i \leq n\}$ under composition and $\otimes$. These are all local maps (corrections).

Define the *Clifford group* over A as the normalizer of the Pauli group, that is to say the set of unitaries f over A such that for all g in the Pauli group, fgf^{-1} is also in the Pauli group.

Entanglement: $\wedge Z_{ij}$ is in Clifford, since:

- $\wedge Z_{ij} X_i = X_i Z_j \wedge Z_{ij}$
- $\wedge Z_{ij} Z_i = Z_i \wedge Z_{ij}$

Quantum Parallelism

- Consider a unitary operator U such that $U|x\rangle|0\rangle = |x\rangle|f(x)\rangle$
- Evaluation of all the values in one go

$$(\frac{1}{\sqrt{2}})^n \sum_{x=0}^{x=2^n} |x\rangle|0\rangle \longrightarrow (\frac{1}{\sqrt{2}})^n \sum_{x=0}^{x=2^n} |x\rangle|f(x)\rangle$$

Quantum Parallelism

- Consider a unitary operator U such that $U|x\rangle|0\rangle = |x\rangle|f(x)\rangle$

- Evaluation of all the values in one go

$$(\frac{1}{\sqrt{2}})^n \sum_{x=0}^{x=2^n} |x\rangle|0\rangle \longrightarrow (\frac{1}{\sqrt{2}})^n \sum_{x=0}^{x=2^n} |x\rangle|f(x)\rangle$$

- BUT when you measure the output you will get only one of the value $|x\rangle|f(x)\rangle$!

Complete Projective Measurement

A complete measurement on $\mathfrak{H}_n$ is given by an orthonormal basis on $\mathfrak{H}_n$, $\mathcal{B} = \{\psi_a\}$ which defines a decomposition $\mathfrak{H}_n = \oplus_a E_a$ of $\mathfrak{H}_n$ into orthogonal (1-dimensional) subspaces E_a.

Writing $|\psi_a\rangle\langle\psi_a| : \mathfrak{H}_n \to E_a$ for the projections to E_a, one defines:

$$M^{\mathcal{B}} : \mathfrak{H}_n \to \oplus_a E_a : |\phi\rangle \mapsto \oplus_a \langle\psi_a, \phi\rangle |\psi_a\rangle$$

- Which a is chosen is observable, and is called the *outcome* of the measurement
- The probability to go from $|\phi\rangle$ to $|\psi_a\rangle\langle\psi_a|(|\phi\rangle)$ is defined as $\langle\psi_a, \phi\rangle / \langle\phi, \phi\rangle$ (by construction, they add all to 1).

Destructive measurements

Given a complete measurement over A, as $\mathcal{A} = \{\psi_a\}$, one can extend it to an incomplete measurement on $A \otimes B$, with components given by $|\psi_a\rangle\langle\psi_a| : A \otimes B \to B$.

- We write M^α for the 1-qubit destructive measurements associated to $\{|+_\alpha\rangle\}$.

Members of the M^α family are called xy-plane measurements. These are the ones we use for 1WQC.

Universality

Theorem 3 *Almost any $\wedge U$ gate is universal: by successive application of this gate to pairs of bits in an n-bit network, any unitary transformation may be approximated with arbitrary accuracy. (It suffices for U to be specified by Euler angles which are not a rational multiple of π.*

A universal set for unitaries on $\mathbb{C}^2$

$$J(\alpha) := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$

Some nice equations:

$$\begin{aligned}
J(\alpha)J(0)J(\beta) &= J(\alpha+\beta) \\
J(\alpha)J(\pi)J(\beta) &= e^{i\alpha} Z\, J(\beta-\alpha) \\
XJ(\alpha) &= J(\alpha+\pi) = J(\alpha)Z \\
H &= J(0) \\
P(\alpha) &= J(0)J(\alpha)
\end{aligned}$$

The J-Decomposition

Theorem 4 *Any unitary operator on $\mathbb{C}^2$ can be written:*

$$U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)$$

for some α, β, γ and δ in $\mathbb{R}$.

Theorem 5 *The set $\{J(\alpha), \wedge Z\}$ is universal*

Note also that $J(0)$, $J(\frac{\pi}{4})$ and $\wedge Z$ is approximately universal (in the sense, that every unitary over $\mathfrak{H}_n$ can be approximated up to an arbitrary ϵ normwise).

The J-Decomposition

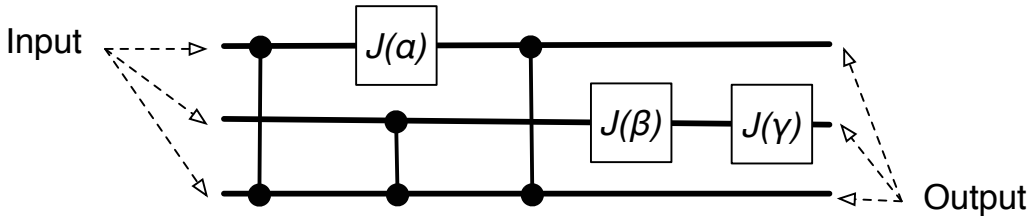
Theorem 6 *Any unitary operator on* $\mathbb{C}^2$ *can be written:*

$$U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)$$

for some α, β, γ *and* δ *in* $\mathbb{R}$.

Theorem 7 *The set* $\{J(\alpha), \wedge Z\}$ *is universal*

Note also that $J(0)$, $J(\frac{\pi}{4})$ and $\wedge Z$ is approximately universal (in the sense, that every unitary over $\mathfrak{H}_n$ can be approximated up to an arbitrary ϵ normwise).



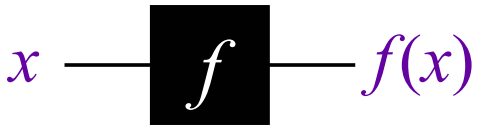
Quantum Circuit Model

- Prepare a simple initial state $|00...0\rangle$
- Perform a universal set of 1- and 2-qubit unitary gates
- Make a measurement in the computational basis at the end
- Uniform family of circuits: a procedure (e.g. Turing machine) generates efficiently the circuit diagrams for a given fixed size input

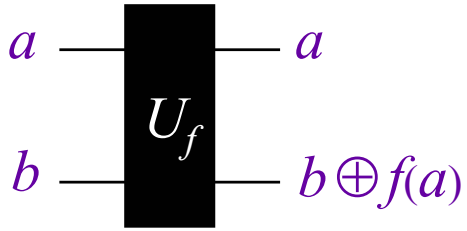
No-cloning theorem

Theorem 8 *There is no valid quantum operation that maps an arbitrary state* $|\psi\rangle$ *to* $|\psi\rangle|\psi\rangle$

Oracle Model



- Input: function f, given as a black box
- Goal: determine some information about f making as few queries to f (and other operations) as possible



Deutsch's problem

- Input: A boolean function $f : \{0,1\}^n \longrightarrow \{0,1\}$
- Output: Determine if f is constant or balanced

$$\mathcal{U}_f : |x\rangle(|0\rangle - |1\rangle) \longrightarrow \begin{cases} |x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ -|x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 1 \end{cases}$$

Thus

$$\mathcal{U}_f : \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Deutsch's problem

- Input: A boolean function $f : \{0,1\}^n \longrightarrow \{0,1\}$
- Output: Determine if f is constant or balanced

$$\mathcal{U}_f : |x\rangle(|0\rangle - |1\rangle) \longrightarrow \begin{cases} |x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ -|x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 1 \end{cases}$$

Thus

$$\mathcal{U}_f : \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Deutsch's problem

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

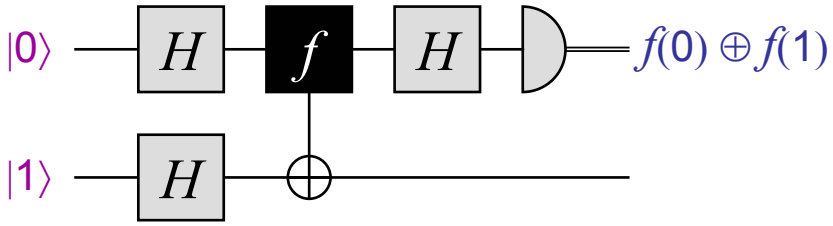
- $|f\rangle$ for any constant function is orthogonal to the corresponding state for any balanced function.

- Measurement on $|f\rangle$ which distinguishes balanced from constant

$$H_n : |x\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

$$H_n |0 \ldots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} |y\rangle$$

Deutsch's problem



Other Balance functions

For each $k \in \{0,1\}^n$ define $f_k : \{0,1\}^n \to \{0,1\}$:

$$f_k(x) = k.x = (k_1.x_1 \oplus \cdots \oplus k_n.x_n)$$

is a balanced function for $k \neq 0 \cdots 0$

Other Balance functions

For each $k \in \{0,1\}^n$ define $f_k : \{0,1\}^n \to \{0,1\}$:

$$f_k(x) = k.x = (k_1.x_1 \oplus \cdots \oplus k_n.x_n)$$

is a balanced function for $k \neq 0 \cdots 0$

$$\mathcal{U}_{f_k} : \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x.k} |x\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Other Balance functions

For each $k \in \{0,1\}^n$ define $f_k : \{0,1\}^n \to \{0,1\}$:

$$f_k(x) = k.x = (k_1.x_1 \oplus \cdots \oplus k_n.x_n)$$

is a balanced function for $k \neq 0 \cdots 0$

$$\mathcal{U}_{f_k} : \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x.k} |x\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$H_n \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x.k} |x\rangle \right) = |k\rangle$$

Other Balance functions

For each $k \in \{0,1\}^n$ define $f_k : \{0,1\}^n \longrightarrow \{0,1\}$:

$$f_k(x) = k.x = (k_1.x_1 \oplus \cdots \oplus k_n.x_n)$$

is a balanced function for $k \neq 0 \cdots 0$

$$\mathcal{U}_{f_k} : \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x.k} |x\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$H_n \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x.k} |x\rangle \right) = |k\rangle$$

2^n functions f_k are distinguished after evaluating the function only once

Quantum Algorithms

- Hidden subgroup problem

Deutsch-Jozsa, Simon Problem, QFT, Factoring, Phase estimation and Pell's Equation

- Amplitude amplification

Search, Counting and Element distinction

- Quantum random walk

Search, Graph reachability and connectivity

- Adiabatic QC SAT and NAND tree

- Topological QC

Jones' polynomial

Quantum Algorithms

The Zoo - Stephen Jordan - 175 papers

http://math.nist.gov/quantum/zoo

1. States and Ensembles

State

The Preskill course: http://www.theory.caltech.edu/preskill/ph229

- In quantum mechanics, a state is a *ray* in a Hilbert space.

–A vector space over the complex numbers $\mathbf{C}$. Vectors will be denoted $|\psi\rangle$.
–With a complex-valued inner product $\langle\psi|\phi\rangle$
(i) Positivity (ii) Linearity (iii) $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^*$
(ix) It is complete in the norm $||\psi|| = \frac{1}{2}\langle\psi|\phi\rangle$
(important in the infinite dimension)

- What is a *ray*? an equivalence class of vectors that differ by multi- plication by a nonzero complex scalar. We can choose a representative of this class to have unit norm vectors $\langle\psi|\psi\rangle = 1$.

- We will also say that $|\psi\rangle$ and $e^{i\alpha}|\psi\rangle$ describe the same physical state, where $|e^{i\alpha}| = 1$. However the relative phase in this superposition is physically significant.

Observable

- A property of a physical system that in principle can be measured. In quantum mechanics, an observable is a linear self-adjoint operator: $A = A^\dagger$

$$\langle \psi | A\psi \rangle = \langle A^\dagger \psi | \psi \rangle$$

- A self-adjoint operator in a Hilbert space has a spectral representation - its eigenstates form a complete orthonormal basis

$$A = \sum_{a_n} a_n P_n$$

- If a_n is nondegenerate, then $P_n = |n\rangle\langle n|$; it is the projection onto the corresponding eigenvector:

$$P_n P_m = \delta_{n,m} P_n \quad P_n^\dagger = P_n$$

Measurement

- In quantum mechanics, the numerical outcome of a measurement of the observable A is an eigenvalue of A

- Right after the measurement, the quantum state is an eigenstate of A with the measured eigenvalue. If the quantum state just prior to the measurement is $|\psi\rangle$, then the outcome a_n is obtained with probability

$$Prob(a_n) = ||P_n|\psi\rangle||^2 = \langle\psi|P_n|\psi\rangle$$

If the outcome is a_n, then the (normalized) quantum state becomes

$$\frac{P_n|\psi\rangle}{(\langle\psi|P_n|\psi\rangle)^{1/2}}$$

Dynamics

- Time evolution of a quantum state is unitary; it is gener- ated by a self-adjoint operator, called the *Hamiltonian* of the system. In the Schrödinger picture of dynamics, the vector describing the system moves in time as governed by the Schrödinger equation

$$\frac{d}{dt}|\psi(t)\rangle = -iH|\psi(t)\rangle$$

- We may reexpress this equation to first order in the infinitesimal quantity dt

$$|\psi(t+dt)\rangle = (1 - iHdt)|\psi(t)\rangle \qquad U(dt) = (1 - iHdt)$$

- Since a product of unitary operators is finite, time evolution over a finite interval is also unitary $|\psi(t)\rangle = U(t)|\psi(0)\rangle$.

- In the case where H is t-independent; we may write $U = e^{itH}$.

- Oddity: two different type of evolution.

non-closed system

- States are not rays.
- Measurements are not orthogonal pro jections.
- Evolution is not unitary.

Example

- A pure two-qubit state where we observe only one of the qubits.

$$|\psi\rangle_{AB} = \sum_{i,k} a_{i\mu} |i\rangle_A |\mu\rangle_B$$

- An observable acting on qubit A only can be expressed as $M_A \otimes I$

$$\langle M_A \rangle = tr(M_A \rho_A)$$

- Define partial trace as $tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|)$ we have:

$$\rho_A := tr_B(|\psi\rangle_{AB}\langle\psi|_{AB}) = \sum_{i,j,\mu} a_{i,\mu} a^*_{j,\mu} |i\rangle\langle j|$$

is a self-adjoint, positive, unit trace matrix called *density matrix*.

- A general density matrix, expressed in the basis in which it is diagonal

$$\rho := \sum_i p_i |\psi\rangle\langle\psi|$$

Decoherence

- The entanglement destroys the coherence of a superposition of states of A, so that some of the phases in the superposition become inaccessible if we look at A alone. We may describe this situation by saying that the state of system A *collapses* - it is in one of a set of alternative states, each of which can be assigned a probability.

Gleason's Theorem

Gleason's theorem starts from the premise that it is the task of quantum theory to assign consistent probabilities to all possible orthogonal projections in a Hilbert space.

- A state of a quantum system: $E \mapsto p(E) \quad 0 \leq p(E) \leq 1$ satisfying

$$p(0) = 0 \qquad p(1) = 1 \qquad E_1 E_2 = 0 \Rightarrow p(E_1 + E_2) = p(E_1) + p(E_2)$$

Gleason showed that for any such map, there is a hermitian, positive ρ with $tr(\rho) = 1$ such that

$$p(E) = tr(\rho E)$$

ensemble of pure states

- Suppose a quantum state is in one of a number of states $|\psi_i\rangle$ with respective probability p_i, $\{p_i, |\psi\rangle\}$. The density operator for the system is defined

$$\rho := \sum_i p_i |\psi\rangle\langle\psi|$$

$$\langle M_A \rangle = tr(M_A \rho_A) = \sum_i p_i \langle\psi|M|\psi\rangle$$

- There are infinite ways to write ρ as a convex combination of other states; hence infinite way of preparing an ensemble; but pure state are extremal points. This highly ambiguous nature of the preparation of a mixed quantum state is one of the characteristic features of quantum information that contrasts sharply with classical probability distributions.

General Measurement

- Described by a collection $\{M_a\}$ of measurement operators, satisfying the completeness $\sum_a M_a^\dagger M_a = I$.

- Probability of each outcome $p(a) = \langle\psi|M_a^\dagger M_a|\psi\rangle$.

- The state after measurement $\frac{M_a|\psi\rangle}{\sqrt{(\langle\psi|M_a^\dagger M_a|\psi\rangle)}}$.

Orthogonal Measurement

A complete measurement on $\mathfrak{H}_n$ is given by an orthonormal basis on $\mathfrak{H}_n$, $\mathcal{B} = \{\psi_a\}$ which defines a decomposition $\mathfrak{H}_n = \oplus_a E_a$ of $\mathfrak{H}_n$ into orthogonal (1-dimensional) subspaces E_a.

Writing $|\psi_a\rangle\langle\psi_a| : \mathfrak{H}_n \to E_a$ for the projections to E_a, one defines:

$$M^{\mathcal{B}} : \mathfrak{H}_n \to \oplus_a E_a : |\phi\rangle \mapsto \oplus_a \langle\psi_a, \phi\rangle |\psi_a\rangle$$

- Which a is chosen is observable, and is called the *outcome* of the measurement
- The probability to go from $|\phi\rangle$ to $|\psi_a\rangle\langle\psi_a|(|\phi\rangle)$ is defined as $\langle\psi_a, \phi\rangle / \langle\phi, \phi\rangle$.

- The measurement outcomes can be described by a density matrix if we knew a measurement had been performed, but we did not know the result.

$$|\psi\rangle\langle\psi| \mapsto \textstyle\sum_a E_a |\psi\rangle\langle\psi| E_a$$

Evolution of density operator

- Unitary evolution $\rho \mapsto U\rho U^\dagger$
- Consistent with the ensemble ($\sum_i p_i|\psi\rangle\langle\psi|$) interpretation

$$\rho(t) = \sum_i p_i U(t)|\psi(0)\rangle\langle\psi(0)U(t)|$$

- Measurement: $p(a) = tr(M_a^\dagger M_a \rho)$ $\quad \frac{M_a \rho M_a^\dagger}{\sqrt{tr(M_a^\dagger M_a \rho)}}$.

Superoperator

- Linear map that maps density operators to density operators (Kraus representation):

$$S(\rho) = \sum_\mu M_\mu \rho M_\mu^\dagger$$

where $\sum_\mu M_\mu^\dagger M_\mu = I$

- The operator sum representation follows from the unitary representation. Furthermore, given the operator sum representation of a superoperator, it is always possible to construct a corresponding unitary representation.

- A superoperator is invertible only if it is unitary. Decoherence causes an irrevocable loss of quantum information.

2. MBQC

Measurement-based quantum computing

What's so special about measurement based quantum computing ?

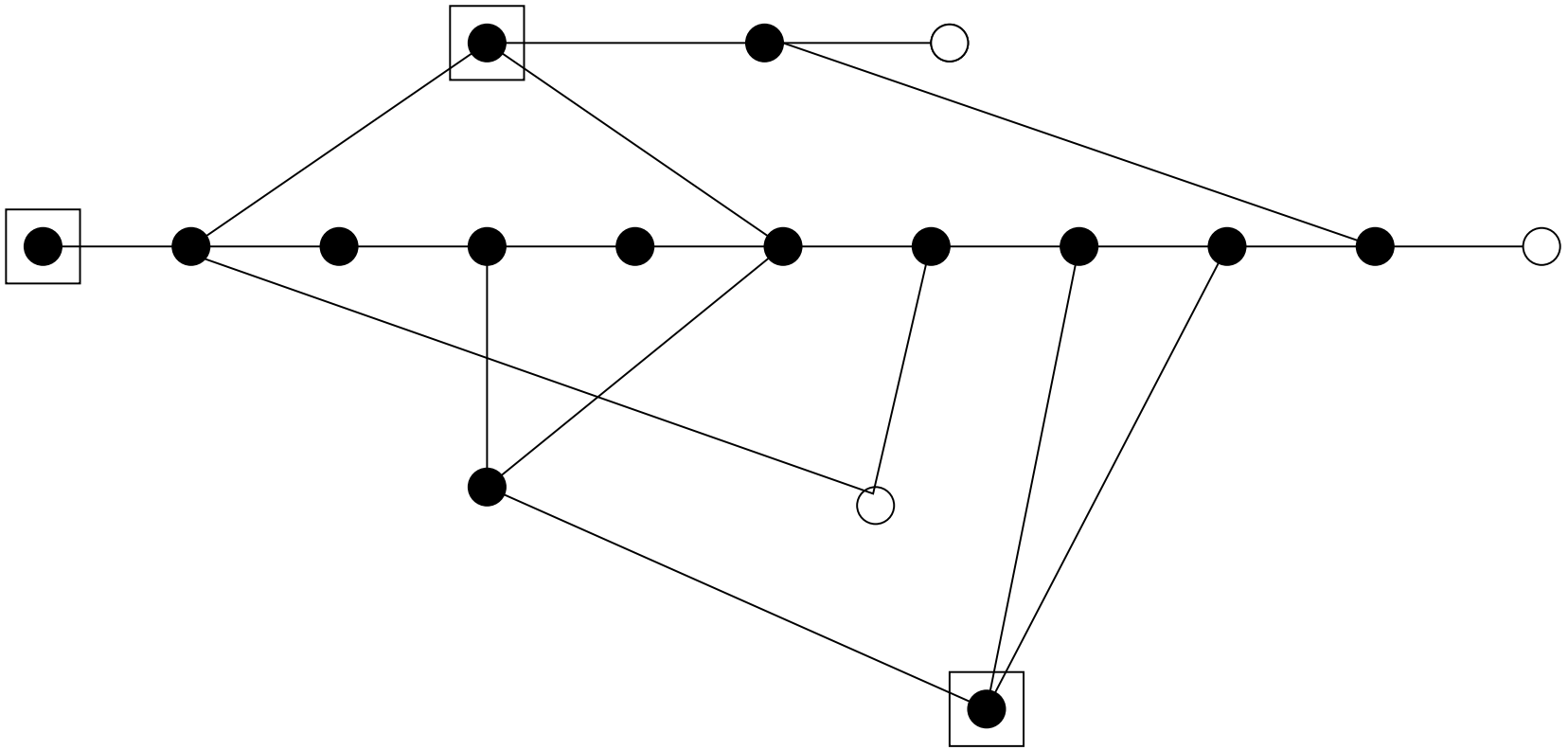
Usually measurements are thought of as something one does at the end of the computation, not an integral part of the computation; with measurement based models the situation is very different, measurements play a central role. However, measuring induces non-deterministic evolutions. This probabilistic drift can be controlled.

3. Introduction

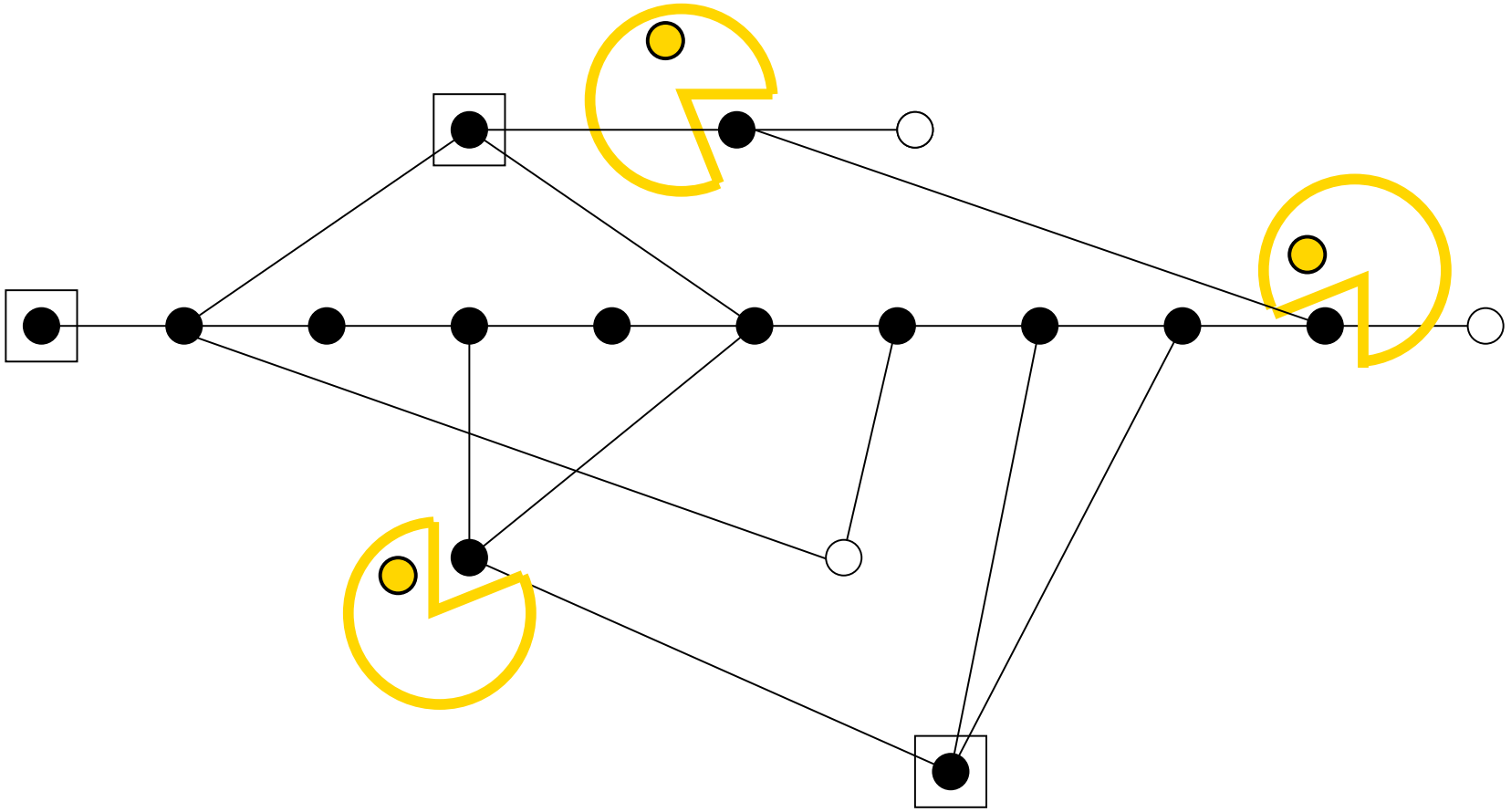
Basic commands

- *New qubits*, to prepare the auxiliary qubits: N
- *Entanglements*, to build the quantum channel: E
- *Measurements*, to propagate (manipulate) qubits: M
- *Corrections*, to make the computation deterministic: C

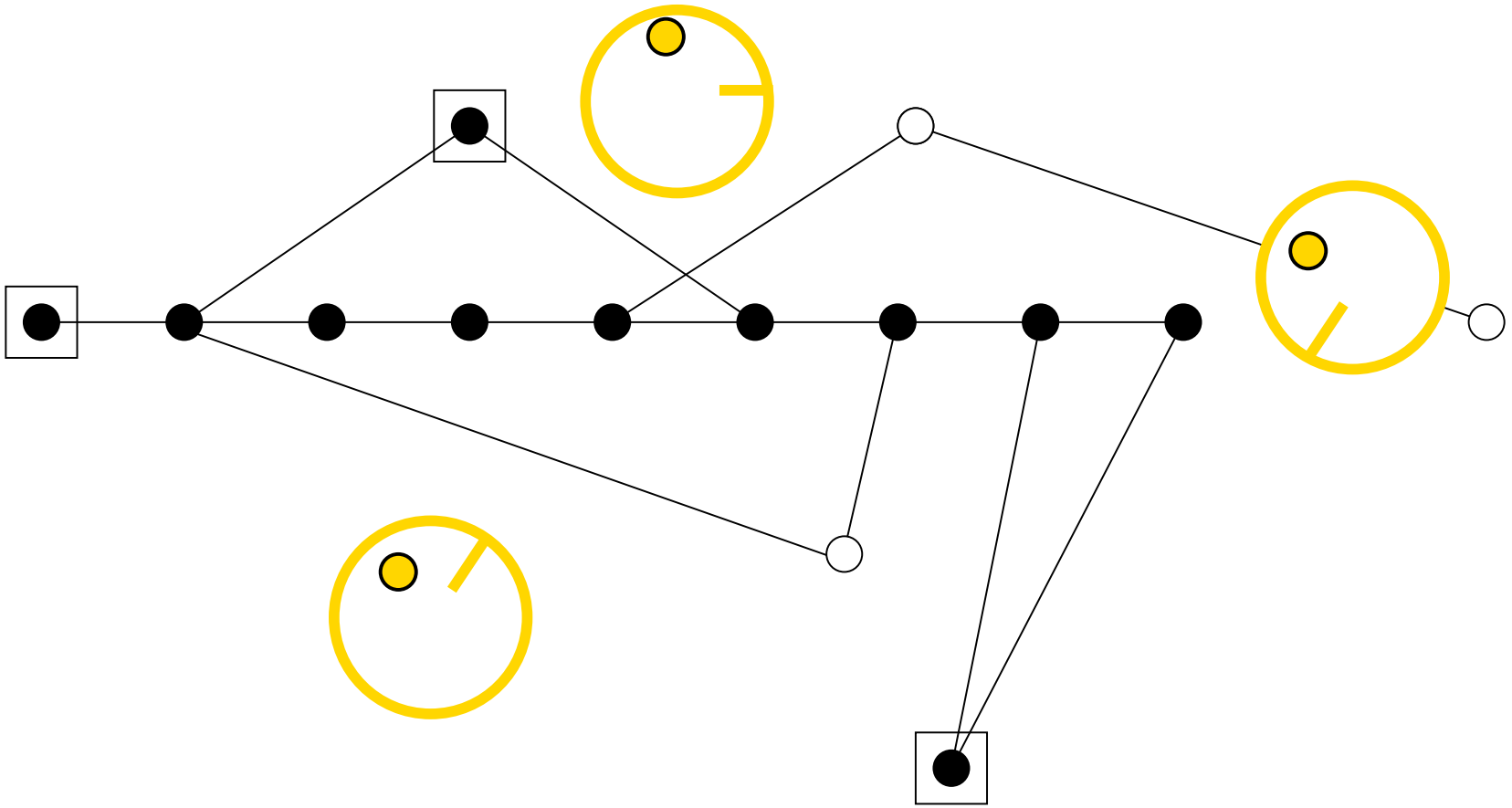
Quantum Pacman



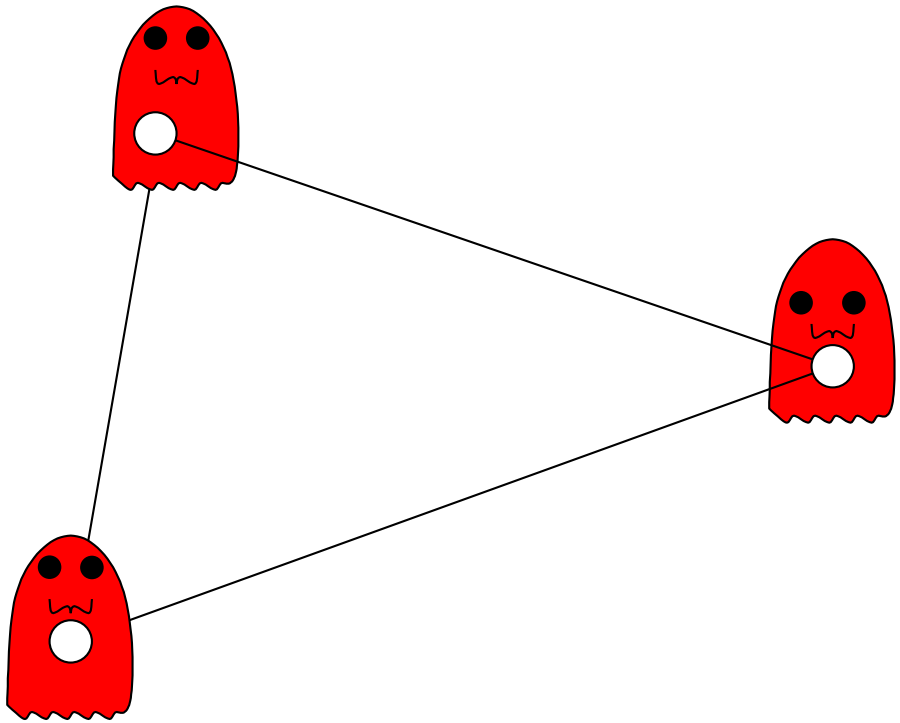
Quantum Pacman



Quantum Pacman



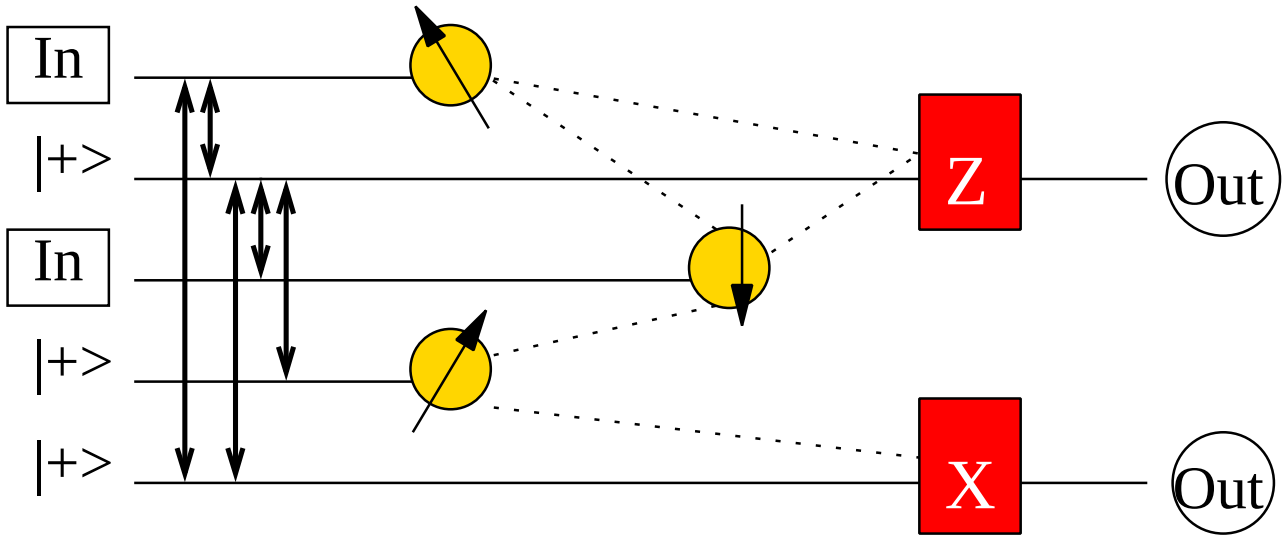
Quantum Pacman



Model Requirements

- Close under compositions
- Universality
- Standardisation
  — Execution in the $NEMC$ order

Circuit Picture



4. A Formal Language

Basic commands

- *Preparations* N_i^α
- *Entanglements* build the quantum resource : $E_{ij} := \wedge Zij$
- *Measurements* consume the resource: $M_i^\alpha := \{\langle \pm_\alpha |\}$
- *Corrections* make the computation deterministic: X_i, Z_i

Dependent commands

The measurement outcome $s_i \in \mathbb{Z}_2$:
— 0 refers to the $\langle +_\alpha|$ projection,
— 1 refers to the $\langle -_\alpha|$ projection.

The M and C commands may be parameterized by a *signal*, that is an expression of the form $\sum_i s_i$ (sum is evaluated in $\mathbb{Z}_2$).

- $[M_i^\alpha]^s = M_i^{(-1)^s \alpha} = M_i^\alpha X_i^s$ X-action
- ${}_t[M_i^\alpha] = M_i^{t\pi+\alpha} = M_i^\alpha Z_i^s$ Z-action

with $X^0 = Z^0 = I$, $X^1 = X$, $Z^1 = Z$.

By extension, a measurement can be made doubly dependent:

$$ {}_t[M_i^\alpha]^s \;=\; M_i^{t\pi+(-1)^s\alpha} $$

U-action

If U maps orthonormal basis $\mathcal{B}$ to $\mathcal{A}$ then:

$$M^{\mathcal{A}} = U M^{\mathcal{B}} U^{\dagger}$$

- X-action:

$$X|+_{\alpha}\rangle = |+_{-\alpha}\rangle$$
$$X|-_{\alpha}\rangle = -|-_{-\alpha}\rangle$$

- Z-action:

$$Z|+_{\alpha}\rangle = |+_{\alpha+\pi}\rangle$$
$$Z|-_{\alpha}\rangle = |-_{\alpha+\pi}\rangle$$

5. Patterns of computation

Specification

The basic computation unit consists of three finite lists: computation space V, inputs I, outputs O * and a finite sequence of V-commands $A_n \ldots A_1$.

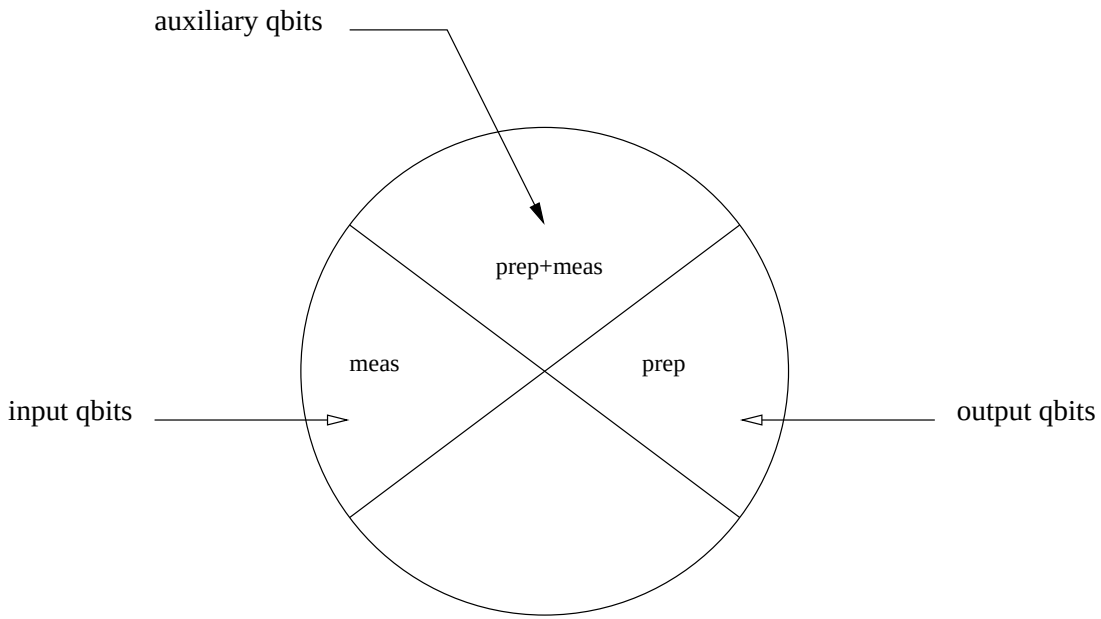
Note that inputs and outputs may overlap, and this leads to optimization, in the sense of using fewer qubits.

Example: pattern $\mathfrak{H} := (\{1,2\},\{1\},\{2\}, X_2^{s1} M_1^x E_{12} N_2)$ implements Hadamard H.

*$V \supseteq I \cup O$

Qubit classes in a pattern

The qubits used in a pattern fall in four classes:
— the ones that are prepared and measured (auxiliary qubits)
— the ones that are only measured (inputs, non outputs)
— the ones that are only prepared (non inputs, outputs)
— the ones that are neither prepared nor measured (inputs and outputs)



Pattern conditions

One subjects patterns to various conditions:
—[(D0)] no command depends on outcomes not yet measured
—[(D1)] no command acts on a qubit already measured
—[(D2)] a qubit i is measured if and only if i is not an output

We assume that all patterns satisfy the *definiteness* conditions (D0), (D1) and (D2)=:(D)

5.1 Computing a pattern

State space

Besides quantum states which are vectors in some $\mathfrak{H}_V$, one needs a classical state recording the outcomes of the successive measurements one does in a pattern:

$$\mathcal{S} \;:=\; \cup_{V,W} \mathfrak{H}_V \times \mathbb{Z}_2^W$$

where V, W range over finite sets.

In other words a computation state is a pair q, Γ, where q is a quantum state and Γ is a map from some W to the outcome space $\mathbb{Z}_2$. We call this classical component Γ an *outcome map* and denote by $\varnothing$ the unique map in $\mathbb{Z}_2^{\varnothing}$.

Commands as actions

For any signal s and classical state $\Gamma \in \mathbb{Z}_2^W$, such that the domain of s is included in W, we take s_Γ to be the value of s given by the outcome map Γ.

That is to say, if $s = \sum_I s_i$, then $s_\Gamma := \sum_I \Gamma(i)$ where the sum is taken in $\mathbb{Z}_2$. Also if $\Gamma \in \mathbb{Z}_2^W$, and $x \in \mathbb{Z}_2$, we define:

$$\Gamma[x/i](i) = x,\ \Gamma[x/i](j) = \Gamma(j) \text{ for } j \neq i$$

which is a map in $\mathbb{Z}_2^{W \cup \{i\}}$.

Commands as actions (continued)

We may now see each of our commands as acting on $\mathcal{S}$:

$$
\begin{aligned}
q, \Gamma &\xrightarrow{N_i^\alpha} && q \otimes |{+}\alpha\rangle_i, \Gamma \\
q, \Gamma &\xrightarrow{E_{ij}} && \wedge Z_{ij} q, \Gamma \\
q, \Gamma &\xrightarrow{X_i^s} && X_i^{s_\Gamma} q, \Gamma \\
q, \Gamma &\xrightarrow{Z_i^s} && Z_i^{s_\Gamma} q, \Gamma \\
q, \Gamma &\xrightarrow{{}_t[M_i^\alpha]^s} && \langle {+}\alpha_\Gamma|_i q, \Gamma[0/i] \\
q, \Gamma &\xrightarrow{{}_t[M_i^\alpha]^s} && \langle {-}\alpha_\Gamma|_i q, \Gamma[1/i]
\end{aligned}
$$

where $\alpha_\Gamma = (-1)^{s_\Gamma}\alpha + t_\Gamma \pi$.

Condition (D) makes sure that the command indices are in V, and s_Γ and t_Γ are always well-defined.

Computation branches

Let $\mathfrak{P}$ be a pattern with computation space V, inputs I, outputs O and command sequence $A_n \ldots A_1$.

A complete pattern computation starts with some input state q in $\mathfrak{H}_I$, together with the empty outcome map $\varnothing$. The input state q is then tensored as specified by the preparation instructions (which can always be pushed to the start) with as many $|+_\alpha\rangle$s as there are non-inputs in V, so as to obtain a state in the full space $\mathfrak{H}_V$.

Then E, M and C commands in $\mathfrak{P}$ are applied in sequence from right to left:

$$\begin{array}{ccccccc} \mathfrak{H}_I & & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & & & & \mathfrak{H}_O \\ \downarrow & & & & & & \uparrow \\ \mathfrak{H}_I \times \mathbb{Z}_2^{\varnothing} & \xrightarrow{prep} & \mathfrak{H}_V \times \mathbb{Z}_2^{\varnothing} & \xrightarrow{CME} & \mathfrak{H}_O \times \mathbb{Z}_2^{V \setminus O} & & \end{array}$$

$\mathfrak{P}$-branch

If m is the number of measurements, which is also the number of non outputs, then the run may follow 2^m different branches. Each branch is associated with a unique binary string $\mathbf{s}$ of length m, representing the classical outcomes of the measurements along that branch, and a unique *branch map* $A_{\mathbf{s}}$ representing the linear transformation from $\mathfrak{H}_I$ to $\mathfrak{H}_O$ along that branch. This map is obtained from the operational semantics via the sequence (q_i, Γ_i) with $1 \leq i \leq n+1$, such that:

$$q_1, \Gamma_1 = q \otimes |+ \ldots +\rangle, \varnothing$$
$$q_{n+1} = q' \neq 0$$
$$\text{and for all } i \leq n : q_i, \Gamma_i \xrightarrow{A_i} q_{i+1}, \Gamma_{i+1}.$$

Denotational Semantics

Definition 1 *A pattern $\mathfrak{P}$ realizes a map on density matrices ρ given by $\rho \mapsto \sum_{\mathbf{s}} A_{\mathbf{s}}^{\dagger}(\rho) A_{\mathbf{s}}$. We write $[\![\mathfrak{P}]\!]$ for the map realized by $\mathfrak{P}$.*

Proposition 2 *Each pattern realizes a completely positive trace preserving map.*

Determinism

Definition 3 *A pattern is said to be* deterministic *if it realizes a cptp-map that sends pure states to pure states. A pattern is said to be* strongly deterministic *when branch maps are equal.*

This is equivalent to saying that for a deterministic pattern branch maps are proportional, that is to say, for all $q \in \mathfrak{H}_I$ and all $\mathbf{s_1}$, $\mathbf{s_2} \in \mathbb{Z}_2^n$, $A_{\mathbf{s_1}}(q)$ and $A_{\mathbf{s_2}}(q)$ differ only up to a scalar. For a strongly deterministic pattern we have for all $\mathbf{s_1}$, $\mathbf{s_2} \in \mathbb{Z}_2^n$, $A_{\mathbf{s_1}} = A_{\mathbf{s_2}}$.

Proposition 4 *If a pattern is strongly deterministic, then it realizes a unitary embedding.*

Patterns combination

Next thing, one needs to combine patterns.

- Patterns may be *composed* if $V_1 \cap V_2 = O_1 = I_2$.

  ** $\mathfrak{H} \circ \mathfrak{H}$: $X_3^{s_2} M_2^0 E_{23} X_2^{s_1} M_1^0 E_{12}$ implements $H \circ H = I$.

- Patterns may be *tensored* if $V_1 \cap V_2 = I_1 \cap I_2 = O_1 \cap O_2 = \varnothing$.

  ** $\mathfrak{H} \otimes \mathfrak{H}$: $X_4^{s_3} M_3^0 E_{34} X_2^{s_1} M_1^0 E_{12}$ implements $H \otimes H$.

6. Universality

A universal set for unitaries on $\mathbb{C}^2$

$$J(\alpha) := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$

Some nice equations:

$$\begin{aligned}
J(\alpha)J(0)J(\beta) &= J(\alpha+\beta) \\
J(\alpha)J(\pi)J(\beta) &= e^{i\alpha} Z\, J(\beta-\alpha) \\
XJ(\alpha) &= J(\alpha+\pi) = J(\alpha)Z \\
H &= J(0) \\
P(\alpha) &= J(0)J(\alpha)
\end{aligned}$$

The J-Decomposition

- [Theorem]. Any unitary operator on $\mathbb{C}^2$ can be written:

$$U = e^{i\alpha} J(0) J(\beta) J(\gamma) J(\delta)$$

for some α, β, γ and δ in $\mathbb{R}$.

- [Theorem] The set $\{J(\alpha), \wedge Z\}$ is universal

Note also that $J(0)$, $J(\frac{\pi}{4})$ and $\wedge Z$ is approximately universal (in the sense, that every unitary over $\mathfrak{H}_n$ can be approximated up to an arbitrary ϵ normwise).

Generating Patterns

The trivial implementations of our unitary generators:

$$\mathfrak{J}(\alpha) \;:=\; X_2^{s1} M_1^{-\alpha} E_{12}$$

Note that:

— These patterns are indeed among the simplest possible

— There is only one single dependency overall.

7. Standardisation

EMC condition

Another condition:
—[(EMC)] commands occur preparation first, then Es, then Ms, then Cs

Condition (EMC) is of a completely different nature. Patterns not respecting it will be called *wild*.

We introduce the measurement calculus to turn any given wild pattern into an equivalent (EMC) form.

We call this procedure *standardisation*.

$$X_5^{s_4} Z_5^{s_3} \quad {}_{s_2}[M_4^0]\ {}_{s_1}[M_3^\alpha]^{s_2}\ [M_2^\beta]^{s_1}\ M_1^\gamma \quad E_{45} E_{34} E_{23} E_{12}$$

Classical Control Global Operation

The Calculus

$$
\begin{aligned}
E_{ij}\ X_i^s &\Rightarrow X_i^s Z_j^s\ E_{ij} \\
E_{ij}\ Z_i^s &\Rightarrow Z_i^s\ E_{ij}
\end{aligned}
$$

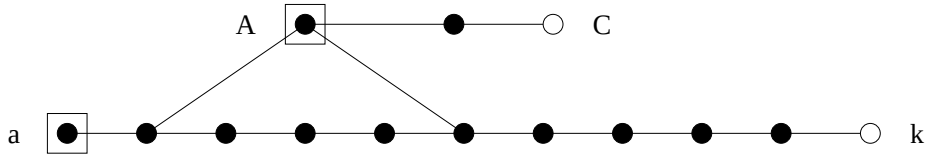
$$
\begin{aligned}
{}_t[M_i^\alpha]^s\ X_i^r &\Rightarrow {}_t[M_i^\alpha]^{s+r} \\
{}_t[M_i^\alpha]^s\ Z_i^r &\Rightarrow {}_{r+t}[M_i^\alpha]^s
\end{aligned}
$$

Wild controlled-U

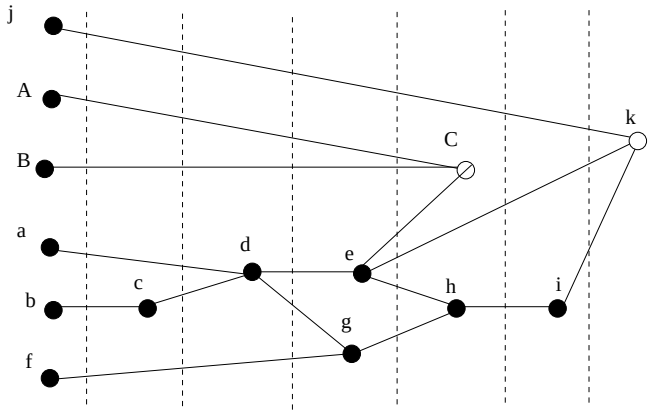
$$X_C^{s_B} M_B^0 E_{BC} X_B^{s_A} M_A^{-\alpha'} E_{AB} X_k^{s_j} M_j^0 E_{jk} X_j^{s_i} M_i^{-\beta-\pi} E_{ij}$$
$$X_i^{s_h} M_h^{\frac{\gamma}{2}} E_{hi} X_h^{s_g} M_g^{\frac{\pi}{2}} E_{gh} X_g^{s_f} M_f^0 E_{fg} E_{Af} X_f^{s_e} M_e^{-\frac{\pi}{2}} E_{ef}$$
$$X_e^{s_d} M_d^{-\frac{\gamma}{2}} E_{de} X_d^{s_c} M_c^{\frac{\pi+\delta+\beta}{2}} E_{cd} X_c^{s_b} M_b^0 E_{bc} E_{Ab} X_b^{s_a} M_a^{\frac{\beta-\delta+\pi}{2}} E_{ab}$$

Parallel controlled-U

$$Z_k^{s_i+s_g+s_e+s_c+s_a} X_k^{s_j+s_h+s_f+s_d+s_b} X_C^{s_B} Z_C^{s_A+s_e+s_c}$$
$$M_B^0 M_A^{-\alpha'} M_j^0 [M_i^{\beta-\pi}]^{s_h+s_f+s_d+s_b} [M_h^{-\frac{\gamma}{2}}]^{s_g+s_e+s_c+s_a} [M_g^{\frac{\pi}{2}}]^{s_f+s_d+s_b}$$
$$M_f^0 [M_e^{-\frac{\pi}{2}}]^{s_d+s_b} [M_d^{\frac{\gamma}{2}}]^{s_c+s_a} [M_c^{\frac{\pi-\delta-\beta}{2}}]^{s_b} M_b^0 M_a^{\frac{-\beta+\delta+\pi}{2}}$$
$$E_{BC} E_{AB} E_{jk} E_{ij} E_{hi} E_{gh} E_{fg} E_{Af} E_{ef} E_{de} E_{cd} E_{bc} E_{ab} E_{Ab}$$



Entanglement Graph

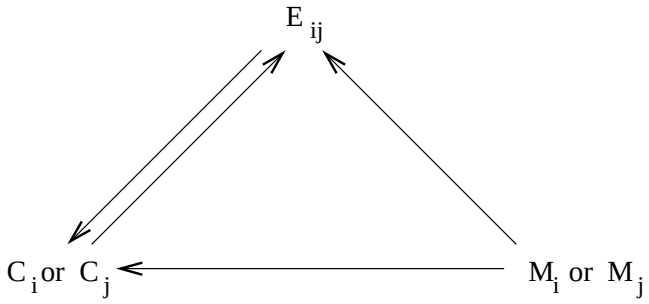


Execution Graph

Execution graph of a pattern, $G(\mathfrak{P})$

- The vertex set of all commands

- The Pattern-edges are defined based on the order of the appearance of commands in $\mathfrak{P}$



- Signal-edges are defined based on the dependencies between commands in $\mathfrak{P}$

$$
\begin{array}{lcl}
{}_t[M_i]^s & \longrightarrow & Domain(s,t) \\
C_i^s & \longrightarrow & Domain(s)
\end{array}
$$

Depth Complexity, $d(\mathfrak{P})$

The length of the longest directed path in $G(\mathfrak{P})$.

- [Theorem] If $\mathfrak{P} \Rightarrow^{\star} \mathfrak{P}'$ where $\mathfrak{P}'$ is an EMC-pattern: $d(\mathfrak{P}') \leq d(\mathfrak{P})$.

EMC form and depth complexity

- Parallel graph preparation:

Depth Complexity = Maximum degree of the entanglement graph

- Parallel measurements:

Depth Complexity = The length of the longest feed-forward chain

- Parallel corrections:

Depth Complexity = 1 (final round)

A generic scheme for parallelizing

Classical Circuit $\longrightarrow$ Reversible Circuit $\longrightarrow$ Quantum Circuit $\longrightarrow$ Wild pattern $\longrightarrow$ EMC pattern $\longrightarrow$ Quantum Circuit $\longrightarrow$ Classical Circuit

- We know that $NC \subset P$, the other direction is an open problem.
  - New approach based on the above parallelization scheme :

$$P \subset QNC \ ? \ \ BQP = QNC \ ?$$

Summary

- Standard quantum computing models are *sequential*
- Measurement based quantum computing is *parallel*

8. Determinism

Flow

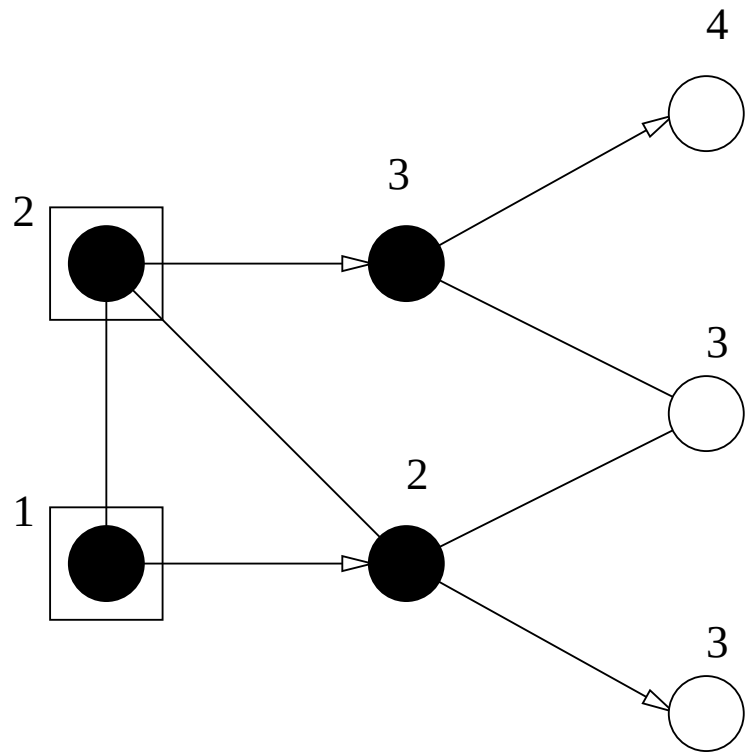
An entanglement graph with inputs and outputs, (G, I, O), has *flow*, if there exists $f : O^c \to I^c$ such that:

- $(i, f(i)) \in G$,
- there exist a partial order $>$ such that:

a) $f(i) > i$,

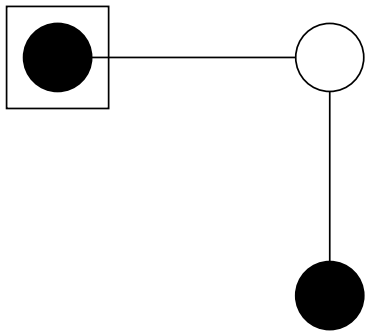
b) for all $k \neq i$ neighbour of $f(i)$ in G, $k > i$.

Flow example



no-Flow example

Here is a geometry with no flow:



Determinism Theorem

Anachronical measurements ${}_{s_i}[M_i^\alpha] = M_i^\alpha Z_i^{s_i}$ (reverse MC) are deterministic, since they are *projections*.

- [Theorem]. If (G, I, O) has flow, then the following pattern is deterministic:

$$\prod_{i \in O^c} (X_{f(i)}^{s_i} \prod_{k \in N_G(f(i)) \setminus \{i\}} Z_k^{s_i} M_i^{\alpha_i}) E_G$$

and computes $\prod_{i \in O^c} {}_{s_i}[M_i^\alpha] E_G$

Proof

First we remark three things:

$$
\begin{aligned}
{}_{s_i}[M_i^\alpha] &= M_i^\alpha Z_i^{s_i} && && (1)\\
Z_i^{s_i} E_{ij} &= X_j^{s_i} E_{ij} X_j^{s_i} && \text{(reverse } EC\text{)} && (2)\\
X_j^{s_i}(|+\rangle) &= |+\rangle && && (3)
\end{aligned}
$$

(we restrict to $|+\rangle$ preparations for the moment, more later)

Proof (continued)

Next we consider the totally positive branch:

$$
\begin{aligned}
&(\textstyle\prod_{i\in O^c} s_i[M_i^{\alpha_i}])E_G && =_1\\
&(\textstyle\prod_{i\in O^c} M_i^{\alpha_i})(\prod_{i\in O^c} Z_i^{s_i})E_G && =\\
&\cdots Z_i^{s_i}E_{if(i)}\textstyle\prod_{k\neq i,k\in N_G(f(i))} E_{f(i)k}E_{G'_i} && =_2\\
&\cdots X_{f(i)}^{s_i}E_{if(i)}X_{f(i)}^{s_i}\textstyle\prod_{k\neq i,k\in N_G(f(i))} E_{f(i)k}E_{G'_i} && =_{EC}\\
&\cdots X_{f(i)}^{s_i}E_{if(i)}\textstyle\prod_{k\neq i,k\in N_G(f(i))} E_{f(i)k}X_{f(i)}^{s_i}\textstyle\prod_{k\neq i,k\in N_G(f(i))} Z_k^{s_i}E_{G'_i} && =\\
&\cdots X_{f(i)}^{s_i}\textstyle\prod_{k\neq i,k\in N_G(f(i))} Z_k^{s_i}E_{if(i)}\textstyle\prod_{k\neq i,k\in N_G(f(i))} E_{f(i)k}E_{G'_i}X_{f(i)}^{s_i} && =_3\\
&\cdots X_{f(i)}^{s_i}\textstyle\prod_{k\neq i,k\in N_G(f(i))} Z_k^{s_i}E_G &&
\end{aligned}
$$

Remarks

The intuition of the proof is that the reverse EC equation converts an anachronical Z correction at i, into a pair of a 'future' X correction, the one sent to $f(i)$ (so in the future, by condition (a)) and a 'past' X correction, sent to the past, until it reaches a preparation, where it is absorbed because of equation (3).

The criterion is only depending on the geometry (not the choice of the measurement angles).

It relies on $|+\rangle$ preparations; see next for the extension.

It is not a necessary condition: $M_1^0 M_3^\alpha E_{23} E_{12} N_3^0$ with inputs $\{1\}$ and outputs $\{2\}$ is deterministic when $\alpha = 0$, and actually constant.

Graphs with flow

- The choice of angles are not important
- It is enough to compute the positive branch
- The combinations of two such graphs has flow
- Blind quantum computing

9. Adjoint pattern

Dealing with $|+_\alpha\rangle$ prep

This supposes a slight extension of the model, namely to add new command z-rotation $Z(\alpha)$.

The new Calculus rules:

$$Z_i(\alpha)\ E_{ij} = E_{ij}\ Z_i(\alpha)$$

$$M_i^\alpha\ Z_i(\beta) = M_i^{\alpha-\beta}$$

The $Z(\alpha)$ doesn't commute with the X-action, since $-\alpha-\beta \neq -(\alpha-\beta)$ (except of course when $\beta = \pi$ which is the usual case of a Z-action).

Determinicity with α-preps

Define $X_i(\alpha) = Z_i(\alpha) X_i Z_i(-\alpha)$, one has an analog of the fixpoint equation:

$$X_i(\alpha)^s \, |+_\alpha\rangle \;\; = \;\; |+_\alpha\rangle$$

to annihilate the 'past' correction, and, one also has an analog of the transfer equation:

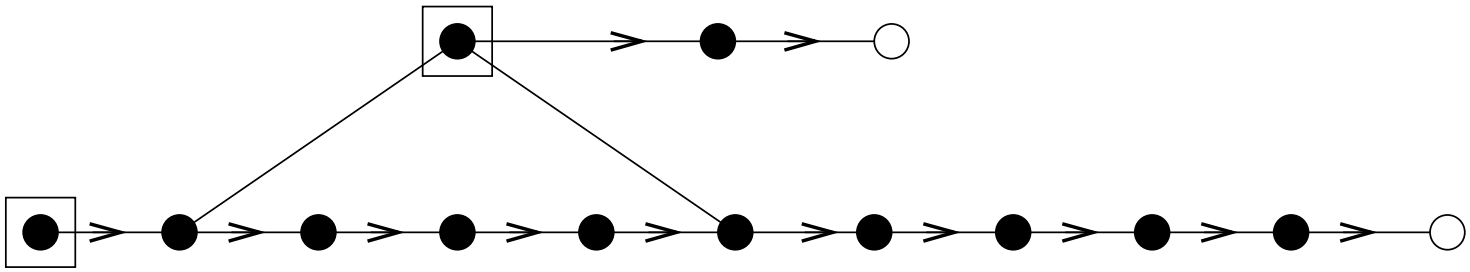
$$X_i(\alpha)^s \, E_{ij} = E_{ij} \, X_i(\alpha)^s Z_i^s$$

so everything works in the same way.

Note that the choice of the correction $X_i(\alpha)$ will depend now on i's preparation angle.

bi-Flow

An entanglement graph with inputs and outputs has *bi-flow* if both (G, I, O) and (G, O, I) has flow.



- [Theorem] If (G, I, O) has bi-flow and implements the partial isometry f, then the pattern (G, O, I) implements its $f^\dagger$:

$\mathfrak{P}$-branches

- Forgetting about the classical control, a branch can be rewritten as:

$$\mathfrak{H}_I \xrightarrow{N} \mathfrak{H}_V \xrightarrow{U} \mathfrak{H}_V \xrightarrow{P} \mathfrak{H}_O$$

where:
— N is the preparation (hence the adjoint of a projection),
— U is a unitary (including entanglement and corrections),
— and P is a projection (the product of the measurement components used in that branch).

- The *mirror branch* implementing $f^\dagger$ is given by:

$$\mathfrak{H}_O \xrightarrow{P^\dagger} \mathfrak{H}_V \xrightarrow{U^\dagger} \mathfrak{H}_V \xrightarrow{N^\dagger} \mathfrak{H}_I$$

Since $\wedge Z$ and Pauli corrections are self-adjoint, and preparations and projections are symmetric under adjunction, this branch belongs to the *adjoint pattern* $\mathfrak{P}^\dagger$, with inputs and outputs exchanged.

Pattern adjunction (examples)

Hadamard:

$$\begin{aligned} \mathfrak{H} &= X_2^{s_2} M_1^0 E_{12} N_2^0 \\ \mathfrak{H}^\dagger &= X_1^{s_2} M_2^0 E_{12} N_1^0 \end{aligned}$$

so $\mathfrak{H}$ is self-adjoint with inputs $\{2\}$, and outputs $\{1\}$.

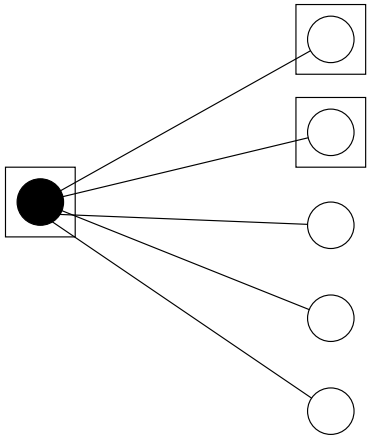
Likewise for $J(\alpha)$:

$$\begin{aligned} \mathfrak{J}(\alpha) &= X_2^{s_2} M_1^{-\alpha} E_{12} N_2 \\ \mathfrak{J}(\alpha)^\dagger &= X_1^{s_2} M_2^0 E_{12} N_1^{-\alpha} \end{aligned}$$

10. Star decomposition

Extended $J(\alpha)$

- Partial isometry and in fact a unitary embedding.



- [Theorem] Given a geometry (G, I, O) with flow one can decompose it to the combinations of extended $J(\alpha)$ and conversely.

11. Pauli measurements

Alternative equivalent model

- *Preparations*: $N_i^{\frac{\pi}{4}} := |+_{\frac{\pi}{4}}\rangle_i$ and $N_i := |+\rangle_i$
- *Entanglements*: $E_{ij} := \wedge Zij$
- *Measurements*: M_i^0 and $M_i^{\frac{\pi}{2}}$
- *Corrections*: X_i and $Z(\frac{\pi}{2})_i$
- *Flipping*: F_i flips the measurement outcome at i.

New action :

$$\begin{aligned} M_i^0\ Z(\tfrac{\pi}{2})i &= M_i^{-\frac{\pi}{2}} = F_i M_i^{\frac{\pi}{2}} \\ M_i^{\frac{\pi}{2}}\ Z(\tfrac{\pi}{2})i &= M_i^0 \end{aligned}$$

New Calculus rules

$$
\begin{array}{lcl}
E_{ij}\ Z(\frac{\pi}{2})_i^s & = & Z(\frac{\pi}{2})_i^s\ E_{ij} \\
N_i^{\frac{\pi}{4}}\ X_i^s & = & Z(\frac{\pi}{2})_i^s X_i^s\ N_i^{\frac{\pi}{4}} \\
N_i^{\frac{\pi}{4}}\ Z(\frac{\pi}{2})_i^s & = & Z(\frac{\pi}{2})_i^s\ N_i^{\frac{\pi}{4}}
\end{array}
$$

- For all $\mathfrak{P}$, there exists a unique NEMC $\mathfrak{P}'$, such that $\mathfrak{P} \Rightarrow^\star \mathfrak{P}'$

Universality

- J_0 (which is H), $J_{\frac{\pi}{4}}$, and $\wedge Z$ is approximately universal.

$$
\begin{aligned}
\wedge\mathfrak{Z} &:= E_{12} \\
\mathfrak{J}_0 &:= X_2^{s_1} M_1^0 E_{12} \\
\mathfrak{J}_{\frac{\pi}{4}} &:= X_2^{s_1} M_1^{-\frac{\pi}{4}} E_{12} \\
&= X_2^{s_1} M_1^0 E_{12}\ N_1^{\frac{\pi}{4}} \\
&= X_4^{s_3} M_3^0 E_{34}\ N_3^{\frac{\pi}{4}} Z_3^{s_2} X_3^{s_1} M_2^0 M_1^0 E_{12} E_{23} \\
&= X_4^{s_3} Z_4^{s_1} F_3^{s_2} {}_{s_1}[M_3^0] M_2^0 M_1^0 E_{34} E_{23} E_{12} N_3^{\frac{\pi}{4}} \\
&= X_4^{s_3+s_2} Z_4^{s_1} {}_{s_1}[M_3^0] M_2^0 M_1^0 E_{34} E_{23} E_{12} N_3^{\frac{\pi}{4}}
\end{aligned}
$$

Error Propagation

$$X_4^{s_3} Z_4^{s_1} F_3^{s_2} {}_{s_1}[M_3^0] M_2^0 M_1^0 \qquad E_{34} E_{23} E_{12} N_3^{\frac{\pi}{4}}$$

Classical Correlation

Quantum Correlation

- Magical relations:

$$\begin{aligned} M_i^0 X_i &= M_i^0 \\ M_i^0 Z_i &= F_i M_i^0 \end{aligned}$$

$$M_i^{\frac{\pi}{2}} X_i = M_i^{\frac{\pi}{2}} Z_i = F_i M_i^{\frac{\pi}{2}}$$