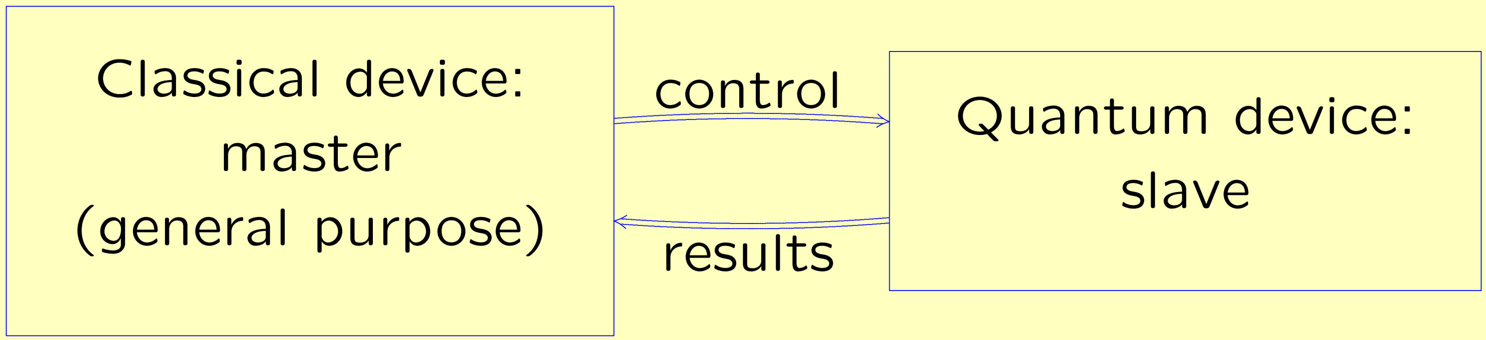
Categorical models of quantum computation

Peter Selinger

Dalhousie University
Halifax, Canada

Part I: Quantum Computation

The QRAM abstract machine [Knill96]



- General-purpose classical computer controls a special quantum hardware device

- Quantum device provides a bank of individually addressable qubits.

- Left-to-right: instructions.

- Right-to-left: results.

Linear Algebra Review

- Scalars $\lambda \in \mathbb{C}$, column vectors $u \in \mathbb{C}^n$, matrices $A \in \mathbb{C}^{n\times m}$.

- Adjoint $A^* = (\overline{a_{ji}})_{ij}$, trace $\operatorname{tr} A = \sum_i a_{ii}$, norm $\|A\|^2 = \sum_{ij} |a_{ij}|^2$.

- Unitary matrix $S \in \mathbb{C}^{n\times n}$ if $S^*S = I$.
  Change of basis: $B = SAS^* \Rightarrow \operatorname{tr} B = \operatorname{tr} A$, $\|B\| = \|A\|$.

- Hermitian matrix $A \in \mathbb{C}^{n\times n}$: if $A = A^*$.
  Hermitian positive: $u^*Au \geq 0$ for all $u \in \mathbb{C}^n$.
  Diagonalization: $A = SDS^*$, S unitary, D real diagonal.

- Tensor product $A \otimes B$, e.g. $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes B = \begin{pmatrix} 0 & B \\ -B & 0 \end{pmatrix}$.

Quantum computation: States

Consider the complex vector space $\mathbb{C}^2$, with basis $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$.

- state of one qubit: $\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$ (*superposition* of $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$).

- state of two qubits: $\alpha|\mathbf{00}\rangle + \beta|\mathbf{01}\rangle + \gamma|\mathbf{10}\rangle + \delta|\mathbf{11}\rangle$.

- *independent*: $(a|\mathbf{0}\rangle + b|\mathbf{1}\rangle) \quad \otimes \quad (c|\mathbf{0}\rangle + d|\mathbf{1}\rangle) \quad =$
  $ac|\mathbf{00}\rangle + ad|\mathbf{01}\rangle + bc|\mathbf{10}\rangle + bd|\mathbf{11}\rangle$.

- otherwise *entangled*.

Lexicographic convention

Identify the basis states $|\mathbf{00}\rangle$, $|\mathbf{01}\rangle$, $|\mathbf{10}\rangle$, $|\mathbf{11}\rangle$ with the standard basis vectors

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

in the *lexicographic* order.

Note: we use *column vectors* for states.

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \alpha|\mathbf{00}\rangle + \beta|\mathbf{01}\rangle + \gamma|\mathbf{10}\rangle + \delta|\mathbf{11}\rangle.$$

Quantum computation: Operations

- unitary transformation
- measurement

Unitary operations

Given an n-qubit state $v \in \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$.

To apply the unitary operation $U : \mathbb{C}^2 \to \mathbb{C}^2$ to qubit i means

$$v' \;=\; (\underbrace{I \otimes \ldots \otimes I}_{i-1} \otimes U \otimes \underbrace{I \otimes \ldots \otimes I}_{n-i})\; v$$

To apply the unitary operation $W : \mathbb{C}^4 \to \mathbb{C}^4$ to qubits $i, i+1$ means

$$v' \;=\; (\underbrace{I \otimes \ldots \otimes I}_{i-1} \otimes W \otimes \underbrace{I \otimes \ldots \otimes I}_{n-i-1})\; v$$

Some standard unitary gates

Unary: Binary:

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad N_c = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & N \end{array}\right),$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H_c = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & H \end{array}\right),$$

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad V_c = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & V \end{array}\right),$$

$$W = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}, \qquad W_c = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & W \end{array}\right), \qquad X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Measurement

$$\begin{tikzcd}
& \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \arrow[dl, "|\alpha|^2"', "\mathbf{0}"] \arrow[dr, "\mathbf{1}"', "|\beta|^2"] & \\
\alpha|\mathbf{0}\rangle & & \beta|\mathbf{1}\rangle
\end{tikzcd}$$

Two Measurements

$$
\begin{tikzcd}[column sep=small]
 & & & \alpha|\mathbf{00}\rangle+\beta|\mathbf{01}\rangle+\gamma|\mathbf{10}\rangle+\delta|\mathbf{11}\rangle \arrow[dll, "|\alpha|^2+|\beta|^2"', "\mathbf{0}"] \arrow[drr, "\mathbf{1}"', "|\gamma|^2+|\delta|^2"] & & & \\
 & \alpha|\mathbf{00}\rangle+\beta|\mathbf{01}\rangle \arrow[dl, "\frac{|\alpha|^2}{|\alpha|^2+|\beta|^2}"', "\mathbf{0}"] \arrow[dr, "\mathbf{1}"', "\frac{|\beta|^2}{|\alpha|^2+|\beta|^2}"] & & & & \gamma|\mathbf{10}\rangle+\delta|\mathbf{11}\rangle \arrow[dl, "\frac{|\gamma|^2}{|\gamma|^2+|\delta|^2}"', "\mathbf{0}"] \arrow[dr, "\mathbf{1}"', "\frac{|\delta|^2}{|\gamma|^2+|\delta|^2}"] & \\
\alpha|\mathbf{00}\rangle & & \beta|\mathbf{01}\rangle & & \gamma|\mathbf{10}\rangle & & \delta|\mathbf{11}\rangle
\end{tikzcd}
$$

Note: Normalization convention.

Pure vs. mixed states

A mixed state is a (classical) probability distribution on quantum states.

Ad hoc notation:

$$\frac{1}{2}\left\{\begin{pmatrix} \alpha \\ \beta \end{pmatrix}\right\} + \frac{1}{2}\left\{\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}\right\}$$

Note: A mixed state is a description of our *knowledge* of a state. An actual closed quantum system is always in a (possibly unknown) pure state.

Density matrices (von Neumann)

Represent the pure state $v = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$ by the matrix

$$vv^* = \begin{pmatrix} \alpha\bar{\alpha} & \alpha\bar{\beta} \\ \beta\bar{\alpha} & \beta\bar{\beta} \end{pmatrix} \in \mathbb{C}^{2\times 2}.$$

Represent the mixed state $\lambda_1 \{v_1\} + \ldots + \lambda_n \{v_n\}$ by

$$\lambda_1 v_1 v_1^* + \ldots + \lambda_n v_n v_n^*.$$

This representation is not one-to-one, e.g.

$$\frac{1}{2}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\} + \frac{1}{2}\left\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} .5 & 0 \\ 0 & .5 \end{pmatrix}$$

$$\frac{1}{2}\left\{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\} + \frac{1}{2}\left\{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right\} = \frac{1}{2}\begin{pmatrix} .5 & .5 \\ .5 & .5 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} .5 & -.5 \\ -.5 & .5 \end{pmatrix} = \begin{pmatrix} .5 & 0 \\ 0 & .5 \end{pmatrix}$$

But these two mixed states are indistinguishable.

Quantum operations on density matrices

Unitary:

$$v \mapsto Uv \qquad\qquad vv^* \mapsto Uvv^*U^* \qquad\qquad A \mapsto UAU^*$$

Measurement:

$$\begin{tikzcd}
& \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \arrow[dl, "|\alpha|^2"', "\mathbf{0}"] \arrow[dr, "\mathbf{1}"', "|\beta|^2"] & \\
\begin{pmatrix}\alpha \\ 0\end{pmatrix} & & \begin{pmatrix}0 \\ \beta\end{pmatrix}
\end{tikzcd}
\qquad
\begin{tikzcd}
& \begin{pmatrix}\alpha\bar{\alpha} & \alpha\bar{\beta} \\ \beta\bar{\alpha} & \beta\bar{\beta}\end{pmatrix} \arrow[dl, "\alpha\bar{\alpha}"', "\mathbf{0}"] \arrow[dr, "\mathbf{1}"', "\beta\bar{\beta}"] & \\
\begin{pmatrix}\alpha\bar{\alpha} & 0 \\ 0 & 0\end{pmatrix} & & \begin{pmatrix}0 & 0 \\ 0 & \beta\bar{\beta}\end{pmatrix}
\end{tikzcd}
\qquad
\begin{tikzcd}
& \begin{pmatrix}a & b \\ c & d\end{pmatrix} \arrow[dl, "a"', "\mathbf{0}"] \arrow[dr, "\mathbf{1}"', "d"] & \\
\begin{pmatrix}a & 0 \\ 0 & 0\end{pmatrix} & & \begin{pmatrix}0 & 0 \\ 0 & d\end{pmatrix}
\end{tikzcd}$$

A complete partial order of density matrices

Let $D_n = \{A \in \mathbb{C}^{n\times n} \mid A$ is positive hermitian and $\mathrm{tr}\, A \leq 1\}$.

Definition. We write $A \sqsubseteq B$ if $B - A$ is positive.

Theorem. The density matrices form a *complete partial order* under $\sqsubseteq$.

- $A \sqsubseteq A$
- $A \sqsubseteq B$ and $B \sqsubseteq A \Rightarrow A = B$
- $A \sqsubseteq B$ and $B \sqsubseteq C \Rightarrow A \sqsubseteq C$
- every increasing sequence $A_1 \sqsubseteq A_2 \sqsubseteq \ldots$ has a least upper bound

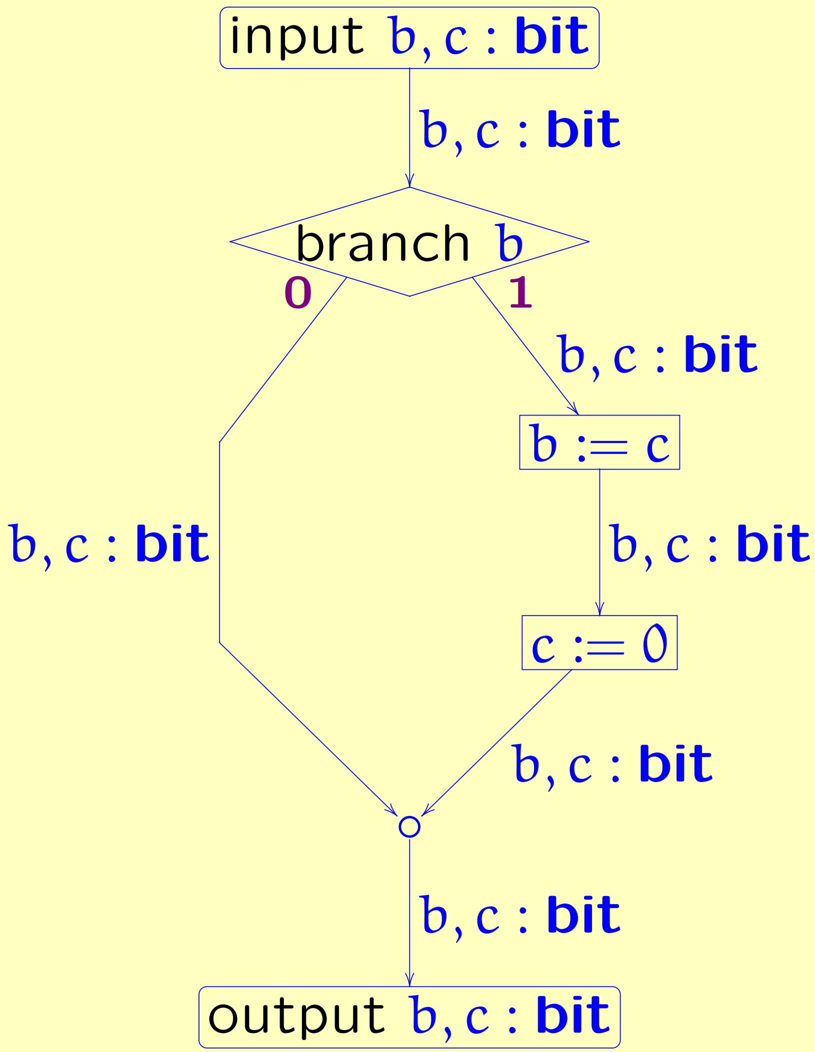
Part II: The Flow Chart Language

Earlier Quantum Programming Languages

- Knill (1996): conventions for writing pseudo-code
- Ömer (1998): scratch space management, user defined operators
- Sanders and Zuliani (2000): specification language, stepwise refinement
- Bettelli, Calarco, and Serafini (2001): based on C++

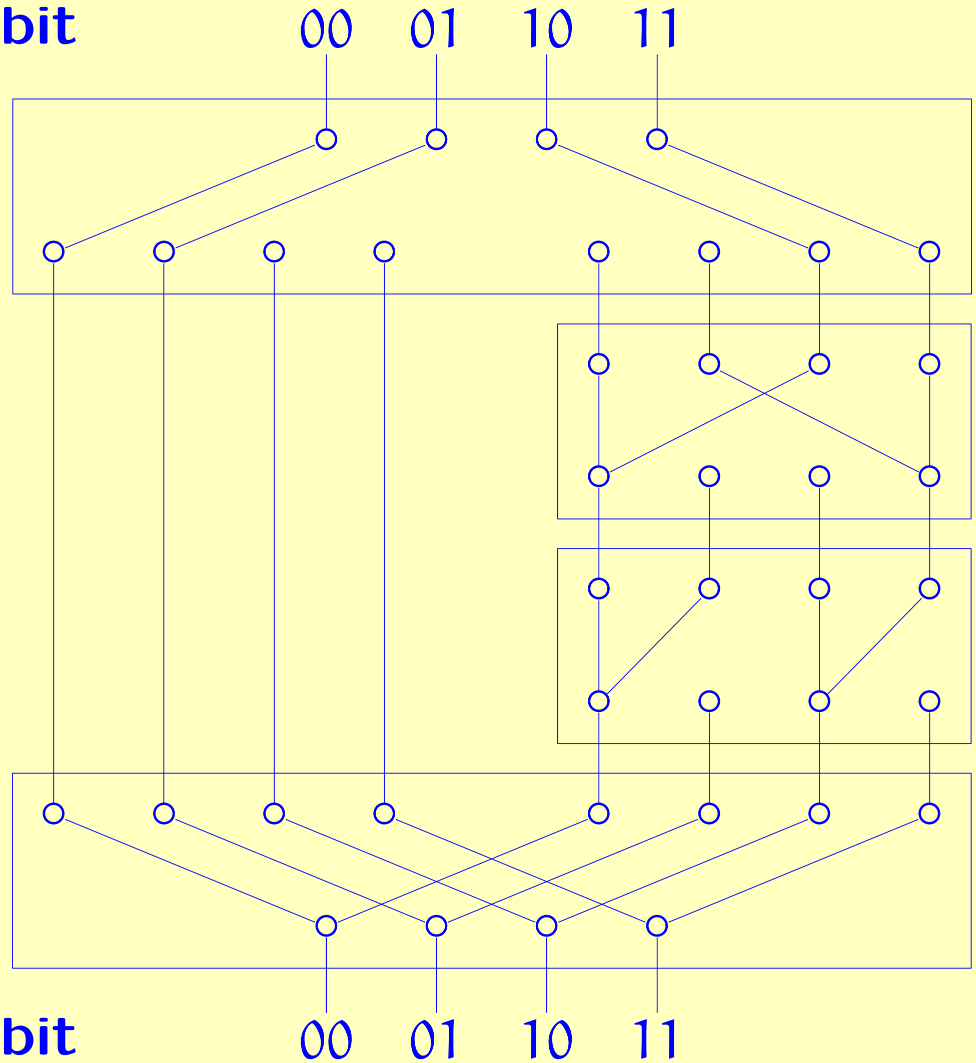
Imperative languages, run-time checks and errors, no formal semantics.

First: the classical case. A simple classical flow chart



Classical flow chart, with boolean variables expanded

input $b, c : \textbf{bit}$



$(*$ branch b $*)$

$(*\ b := c\ *)$

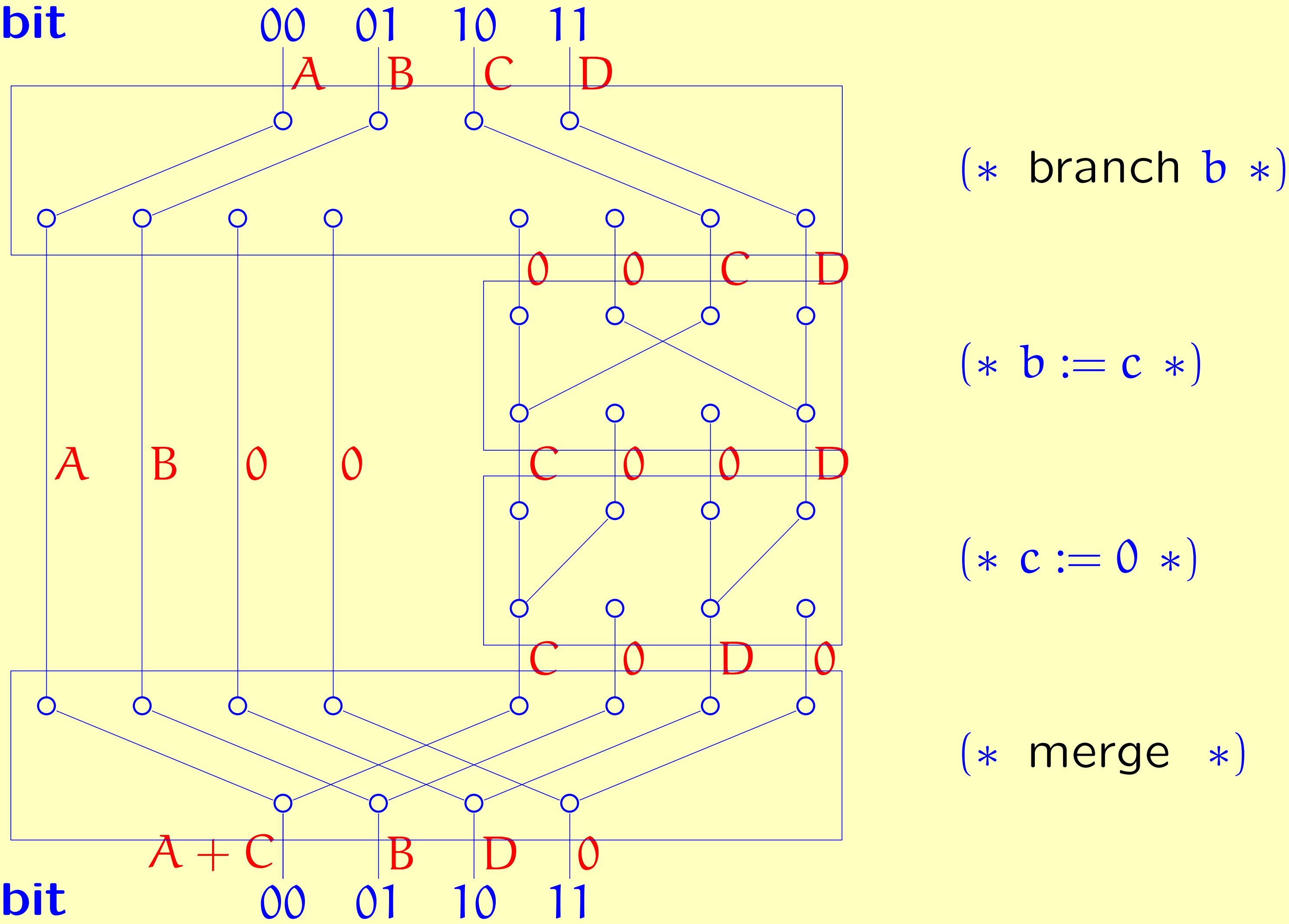
$(*\ c := 0\ *)$

$(*$ merge $*)$

output $b, c : \textbf{bit}$

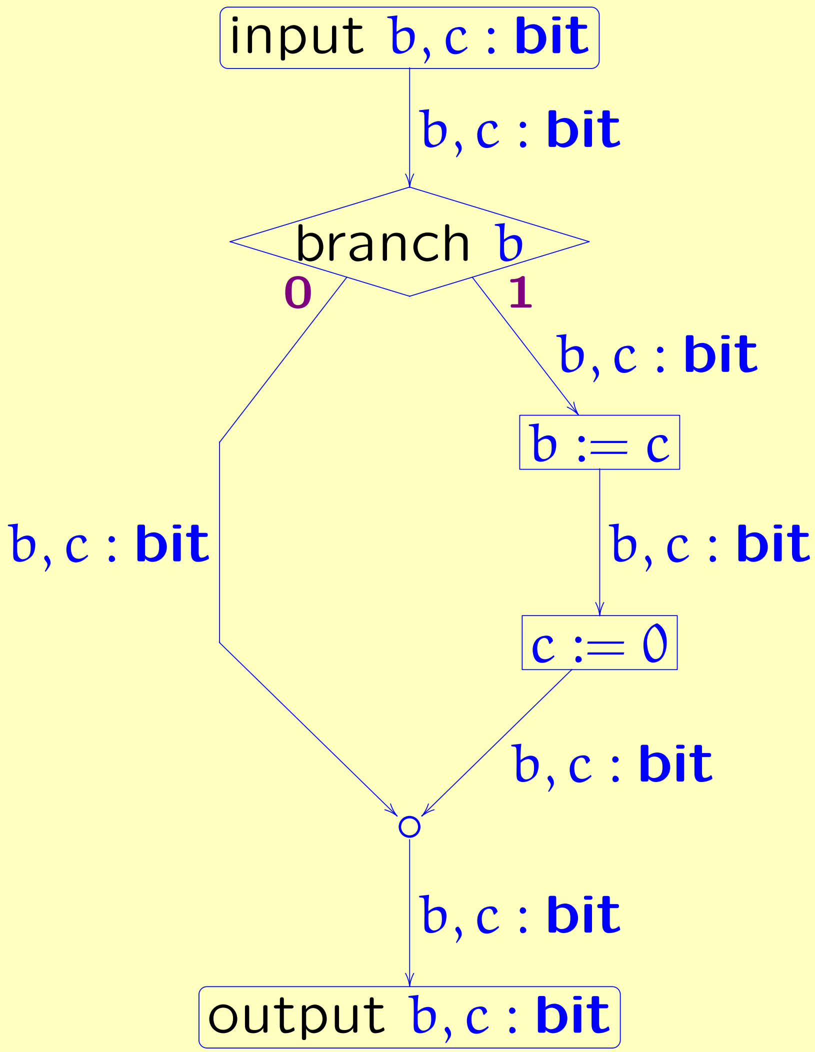
Classical flow chart, with boolean variables expanded

input $b, c : \textbf{bit}$

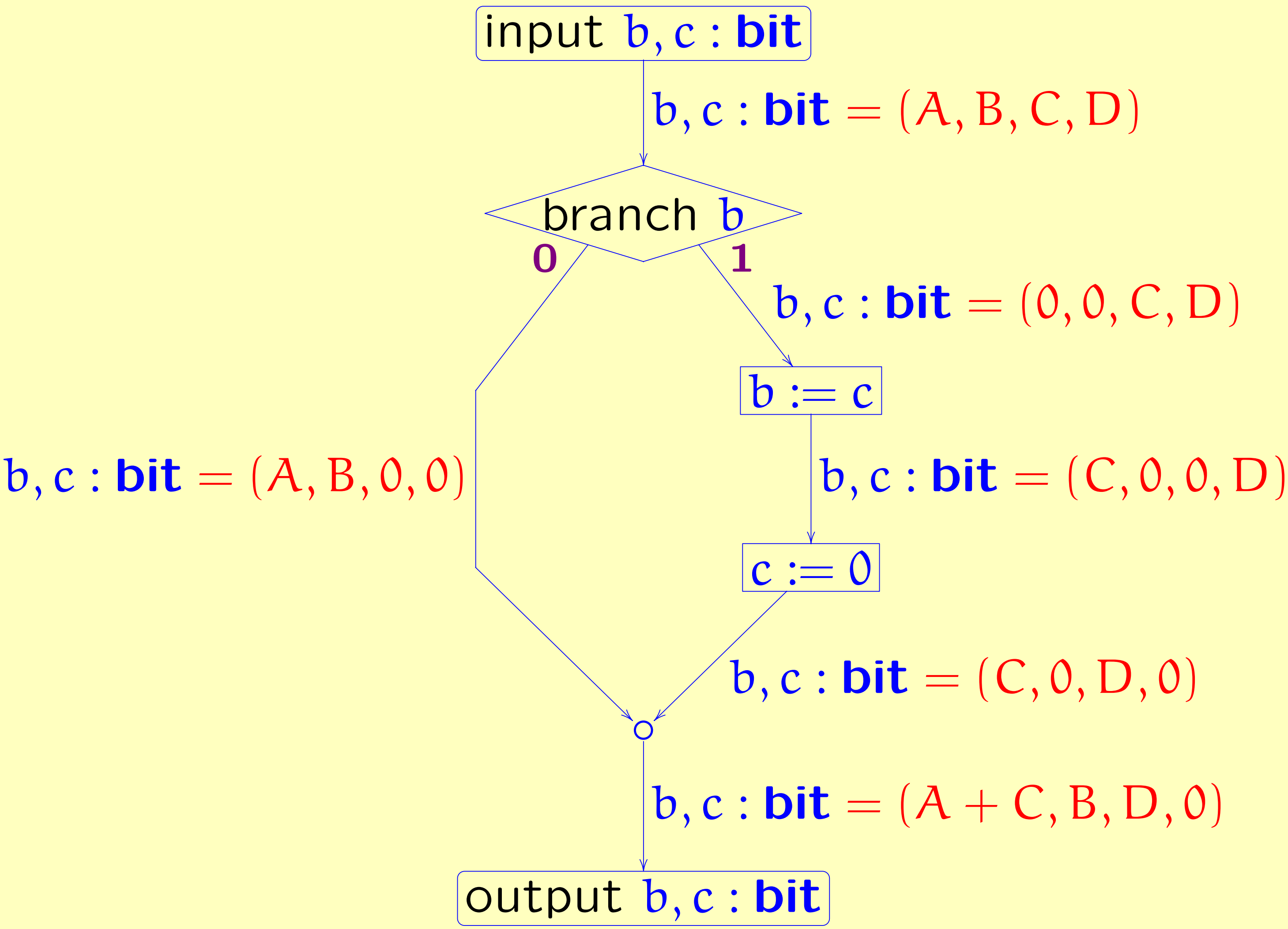


output $b, c : \textbf{bit}$

A simple classical flow chart



A simple classical flow chart



Summary of classical flow chart components

Allocate bit:

$\Gamma = A$

$\boxed{\text{new bit } b := 0}$

$b : \textbf{bit}, \Gamma = (A, 0)$

Discard bit:

$b : \textbf{bit}, \Gamma = (A, B)$

$\boxed{\text{discard } b}$

$\Gamma = A + B$

Assignment:

$b : \textbf{bit}, \Gamma = (A, B)$

$\boxed{b := 0}$

$b : \textbf{bit}, \Gamma = (A + B, 0)$

$b : \textbf{bit}, \Gamma = (A, B)$

$\boxed{b := 1}$

$b : \textbf{bit}, \Gamma = (0, A + B)$

Branching:

$b : \textbf{bit}, \Gamma = (A, B)$

branch b

0 $b : \textbf{bit}, \Gamma = (A, 0)$

1 $b : \textbf{bit}, \Gamma = (0, B)$

Merge:

$\Gamma = A$

$\Gamma = B$

$\Gamma = A + B$

Initial:

$\Gamma = 0$

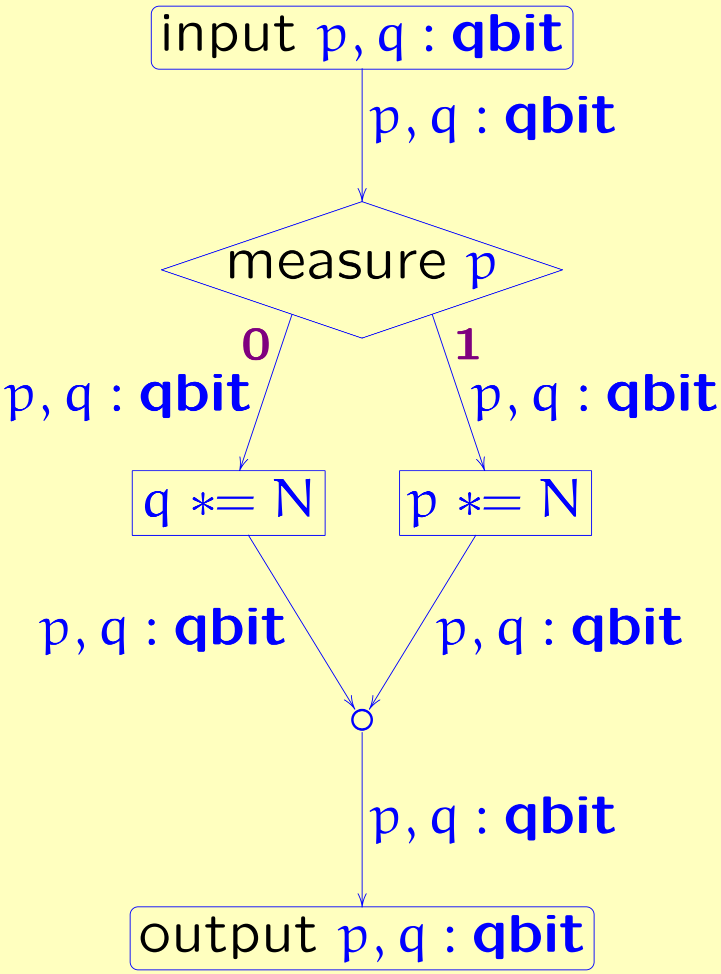
Permutation:

$b_1, \ldots, b_n : \textbf{bit} = A_0, \ldots, A_{2^n-1}$

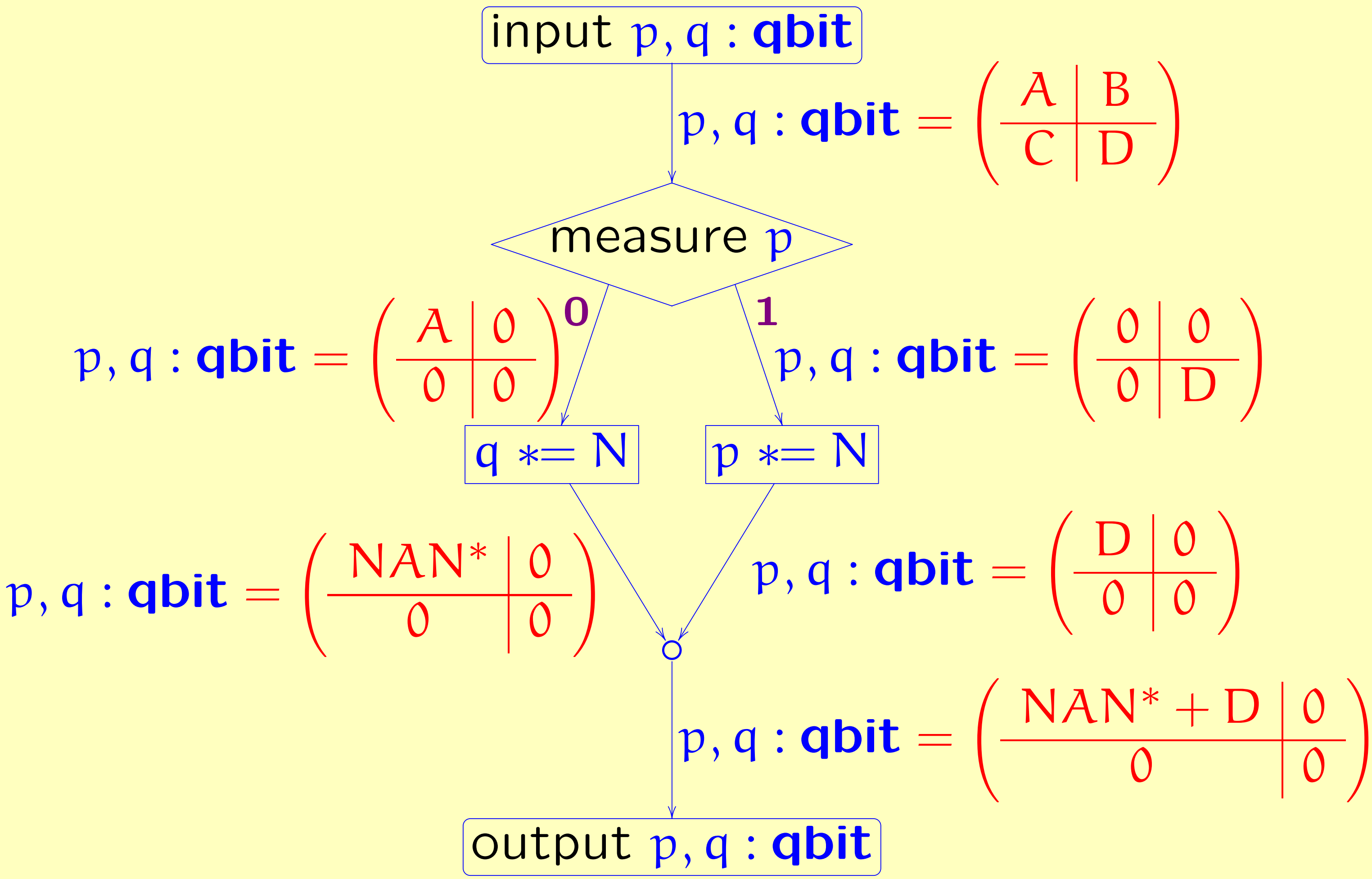
$\boxed{\text{permute } \phi}$

$b_{\phi(1)}, \ldots, b_{\phi(n)} : \textbf{bit} = A_{2^{\phi(0)}}, \ldots, A_{2^{\phi(2^n-1)}}$

The quantum case: A simple quantum flow chart



A simple quantum flow chart



Summary of quantum flow chart components

Allocate qbit:

$\Gamma = A$

new qbit $q := 0$

$q : \textbf{qbit}, \Gamma = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right)$

Discard qbit:

$q : \textbf{qbit}, \Gamma = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$

discard q

$\Gamma = A + D$

Unitary transformation:

$\bar{q} : \textbf{qbit}, \Gamma = A$

$\bar{q} \mathrel{*}= S$

$\bar{q} : \textbf{qbit}, \Gamma = (S \otimes I) A (S \otimes I)^*$

Measurement:

$q : \textbf{qbit}, \Gamma = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$

measure q

0: $q : \textbf{qbit}, \Gamma = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right)$

1: $q : \textbf{qbit}, \Gamma = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & D \end{array}\right)$

Merge:

$\Gamma = A$ $\Gamma = B$

$\Gamma = A + B$

Initial:

$\Gamma = 0$

Permutation:

$q_1, \ldots, q_n : \textbf{qbit} = (a_{ij})_{ij}$

permute ϕ

$q_{\phi(1)}, \ldots, q_{\phi(n)} : \textbf{qbit} = (a_{2^{\phi}(i), 2^{\phi}(j)})_{ij}$

Combining classical data with quantum data

Consider typing contexts of the form

$$b_1 : \mathbf{bit}, \ldots, b_n : \mathbf{bit}, q_1 : \mathbf{qbit}, \ldots, q_m : \mathbf{qbit}.$$

Definition. A *state* for the above typing context is a tuple

$$(A_0, \ldots, A_{2^n-1})$$

of 2^n density matrices of dimension $2^m \times 2^m$.

Summary of language features:

- our language is *functional* (no side effects) and *statically typed* (no run-time errors).

- it combines *quantum and classical features* (the compiler can separate them again).

- it has *high-level features* (such as loops, recursion, and structured data types) [not shown in this talk]

- there is a *compositional denotational semantics* [next slides].

Part III: Semantics

The denotation of a quantum flow chart

The denotation of a flow chart is a function that maps (tuples of) matrices to (tuples of) matrices.

Example: the denotation of the quantum flow chart from p.22 is the function

$$F\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) = \left(\begin{array}{c|c} NAN^* + D & 0 \\ \hline 0 & 0 \end{array}\right).$$

Question: Which functions can occur?

Superoperators

1) *linear*

2) *positive:* A positive $\Rightarrow F(A)$ positive

3) *completely positive:* $F \otimes \mathrm{id}_n$ positive for all n

4) *trace non-increasing:* A positive $\Rightarrow \mathrm{tr}\, F(A) \leq \mathrm{tr}(A)$

Theorem: The above conditions are necessary and sufficient.

Characterization of completely positive maps

Let $F : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$ be a linear map. We define its *characteristic matrix* as

$$\chi_F = \left(\begin{array}{c|c|c} F(E_{11}) & \cdots & F(E_{1n}) \\ \hline \vdots & \ddots & \vdots \\ \hline F(E_{n1}) & \cdots & F(E_{nn}) \end{array}\right).$$

Theorem (Characteristic Matrix). F is completely positive if and only if χ_F is positive.

Another, more well-known, characterization is the following:

Theorem (Kraus Representation Theorem): F is completely positive if and only if it can be written in the form

$$F(A) = \sum_i B_i A B_i^*, \qquad \text{for some matrices } B_i.$$

The category CPM of completely positive maps

Objects: finite dimensional Hilbert spaces

Morphisms: $f : V \to W$ is a completely positive map

$$f : V^* \otimes V \to W^* \otimes W.$$

Let $\mathbf{CPM}^{\oplus}$ be the biproduct completion.

The category Q of superoperators: Full subcategory of $\mathbf{CPM}^{\oplus}$ of trace-non-increasing maps.

The interpretation of flow charts takes place in **Q**.

Structural and denotational equivalence

Definition. An *elementary quantum flow chart category* is

- a symmetric monoidal category with finite coproducts
- a trace for $\oplus$ (a la [Joyal/Street/Verity])
- such that $A \otimes (-)$ is a traced monoidal functor for every object A,
- together with a distinguished object **qbit** and morphisms $\nu : I \oplus I \to \mathbf{qbit}$ and $\mu : \mathbf{qbit} \to I \oplus I$, such that $\mu \circ \nu = \mathrm{id}$.

Definition. Two quantum flow charts X, Y are *structurally equivalent* if for every elementary quantum flow chart category $\mathbf{C}$ and every interpretation η of basic operator symbols, $[\![X]\!]_\eta = [\![Y]\!]_\eta$.

We say X and Y are *denotationally equivalent* if $[\![X]\!] = [\![Y]\!]$ for the canonical interpretation in the category $\mathbf{Q}$ of signatures and superoperators.

Overview of some recent research

- **Quantum process calculi.** Lalire-Jorrand (2004), Gay-Nagarajan (2004), Adão-Mateus (2005)
- **Higher-order quantum computation.** Van Tonder (2003, 2004), Selinger-Valiron (2004), Altenkirch-Grattage (2004)
- **Categorical quantum computation.** Abramsky-Coecke (2004), Selinger (2005)
- **Measurement based quantum computation.** Danos-D'Hondt-Kashefi-Panangaden (2004, 2005)
- **Quantum specification.** Zuliani (2001-2004), D'Hondt-Panangaden (2004), Tafliovich (2004)
- **Quantum coherent spaces.** Girard (2003), Selinger (2004)