Quantum Programming

Peter Selinger

Dalhousie University
Halifax, Canada

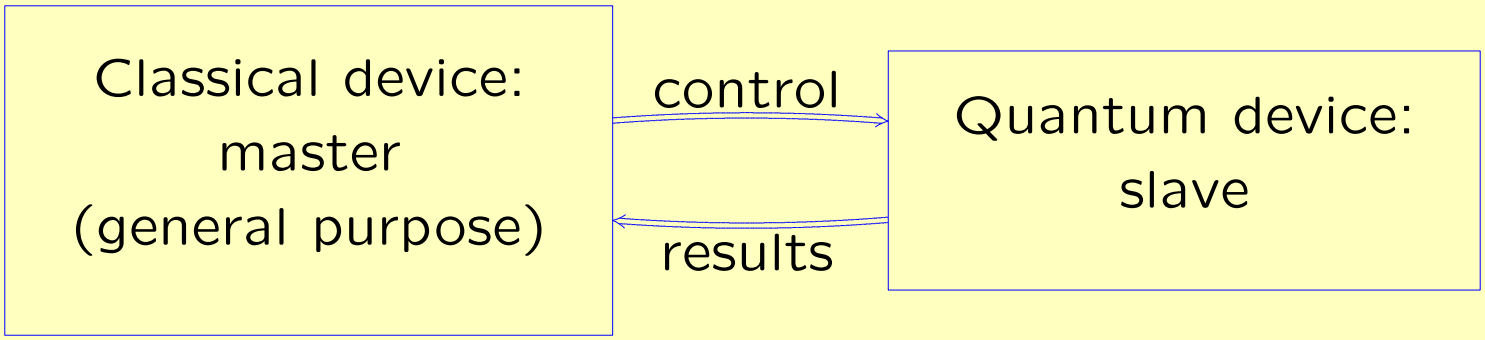
ProbProgSchool 2017, Braga, June 3, 2017

Part I: Quantum Computation

Linear Algebra Review

- Scalars $\lambda \in \mathbb{C}$, column vectors $u \in \mathbb{C}^n$, matrices $A \in \mathbb{C}^{n \times m}$.
- Adjoint $A^\dagger = (\overline{a_{ji}})_{ij}$, 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 $S^\dagger S = I$.
  Change of basis: $B = SAS^\dagger \Rightarrow \operatorname{tr} B = \operatorname{tr} A$, $\|B\| = \|A\|$.
- Hermitian matrix $A \in \mathbb{C}^{n \times n}$: if $A = A^\dagger$.
  Hermitian positive: $u^\dagger A u \geq 0$ for all $u \in \mathbb{C}^n$.
  Diagonalization: $A = SDS^\dagger$, S unitary, D real diagonal.
- Tensor product $A \otimes B$, e.g. $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes B = \begin{pmatrix} 0 & B \\ -B & 0 \end{pmatrix}$.

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.

Quantum computation: States

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

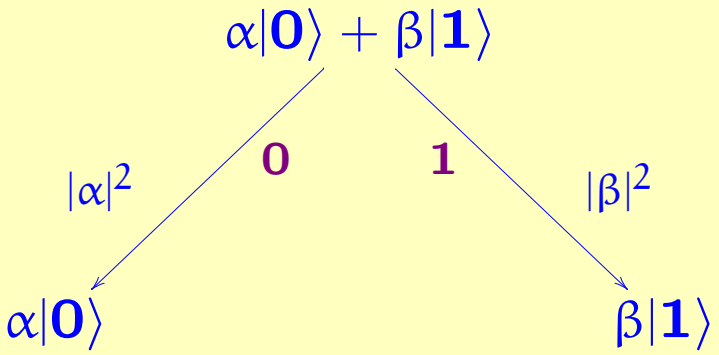
Some standard unitary gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

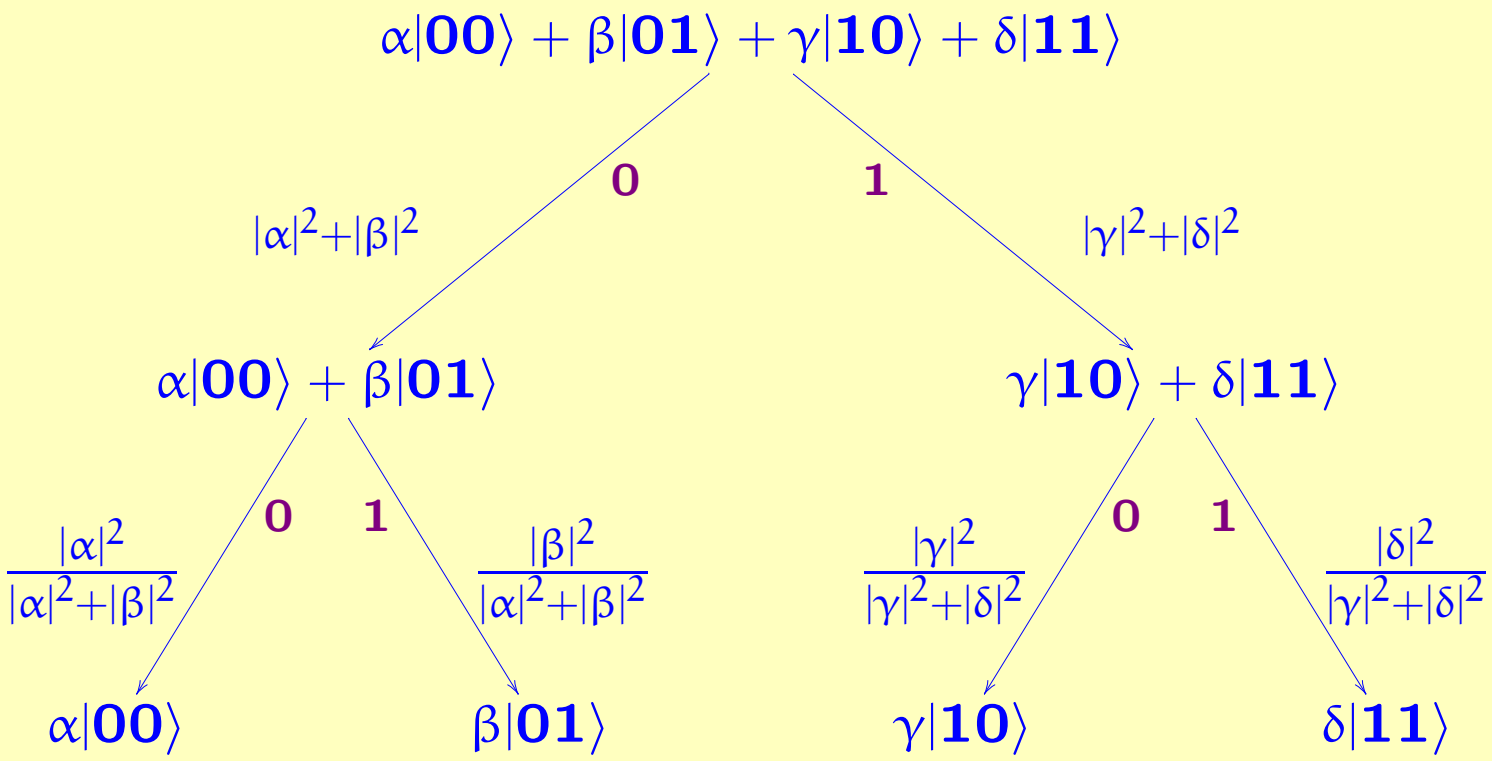
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix},$$

$$\text{CNOT} = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & X \end{array}\right) = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

Measurement



Two Measurements



Note: Normalization convention.

Part II: Density Matrices

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

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

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

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

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

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

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

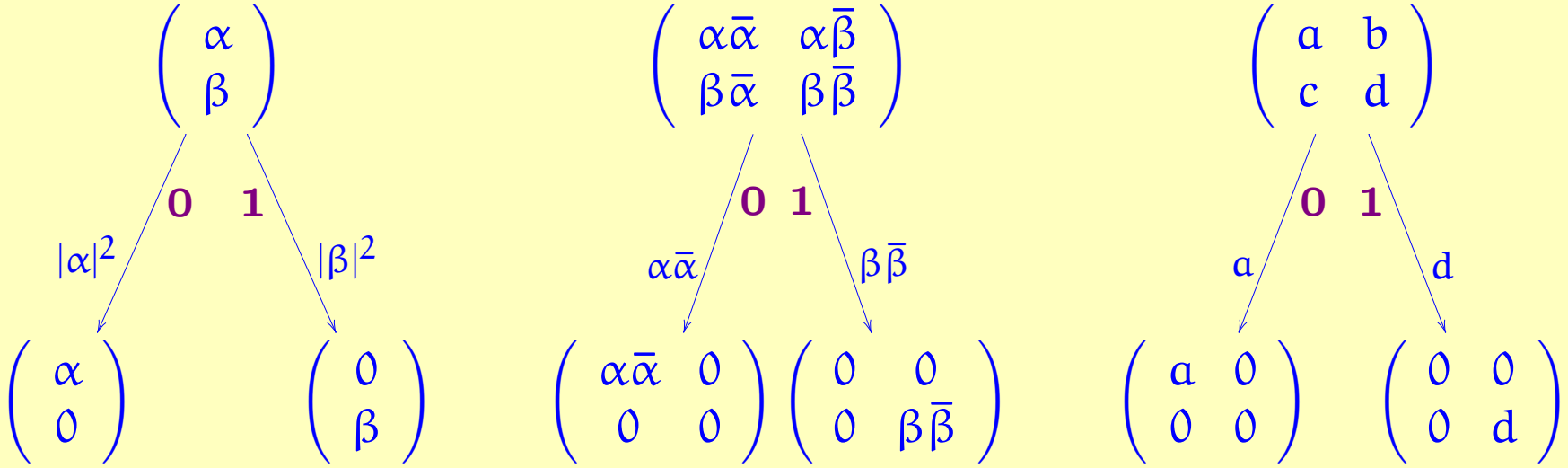
But these two mixed states are indistinguishable.

Quantum operations on density matrices

Unitary:

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

Measurement:



A complete partial order of density matrices

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

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

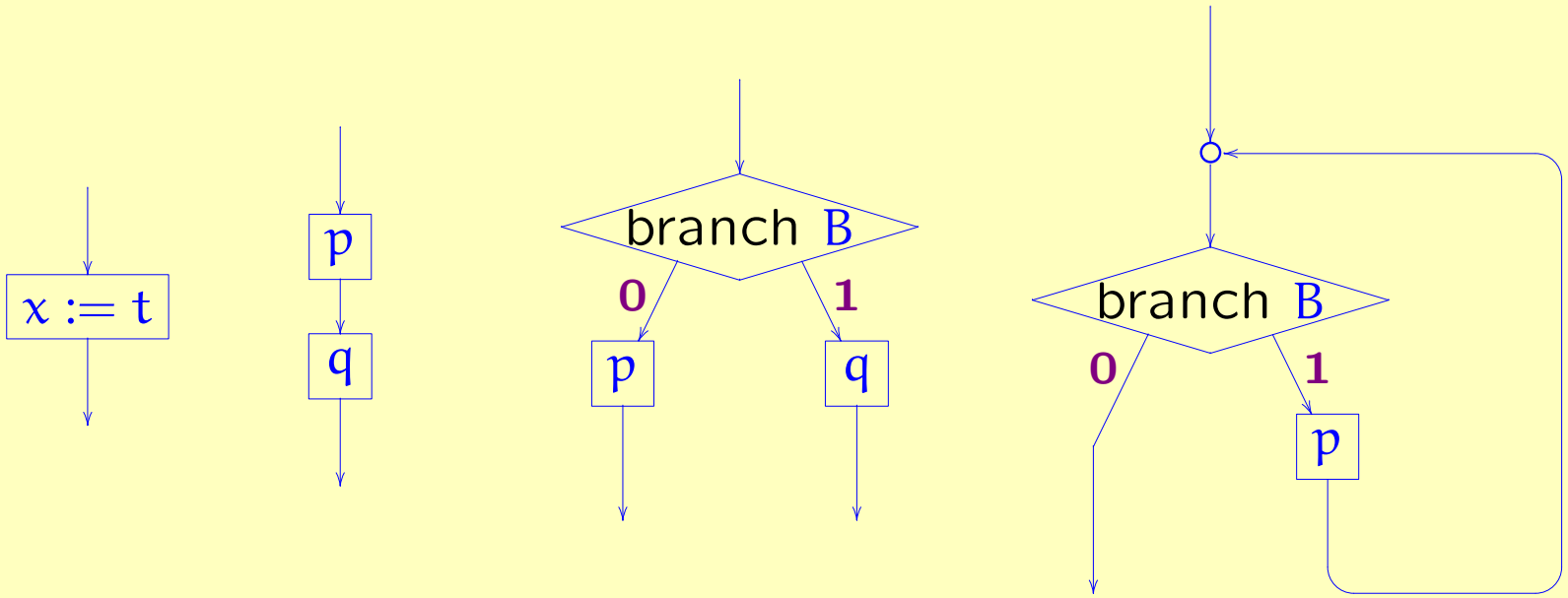
Theorem. The density matrices form a *complete partial order* under $\sqsubseteq$.

- $A \sqsubseteq A$
- $A \sqsubseteq B$ 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 III: The Flow Chart Language

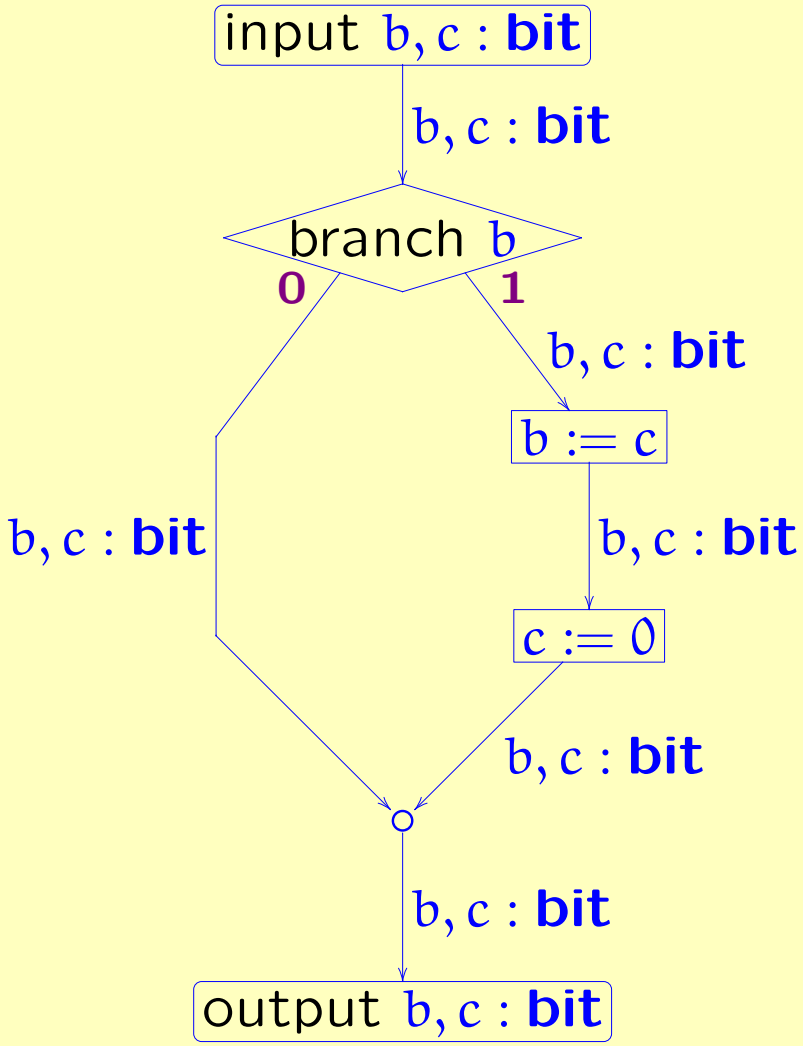
First: the classical case

Cf. the "Simple Imperative Language" from Kozen's talk



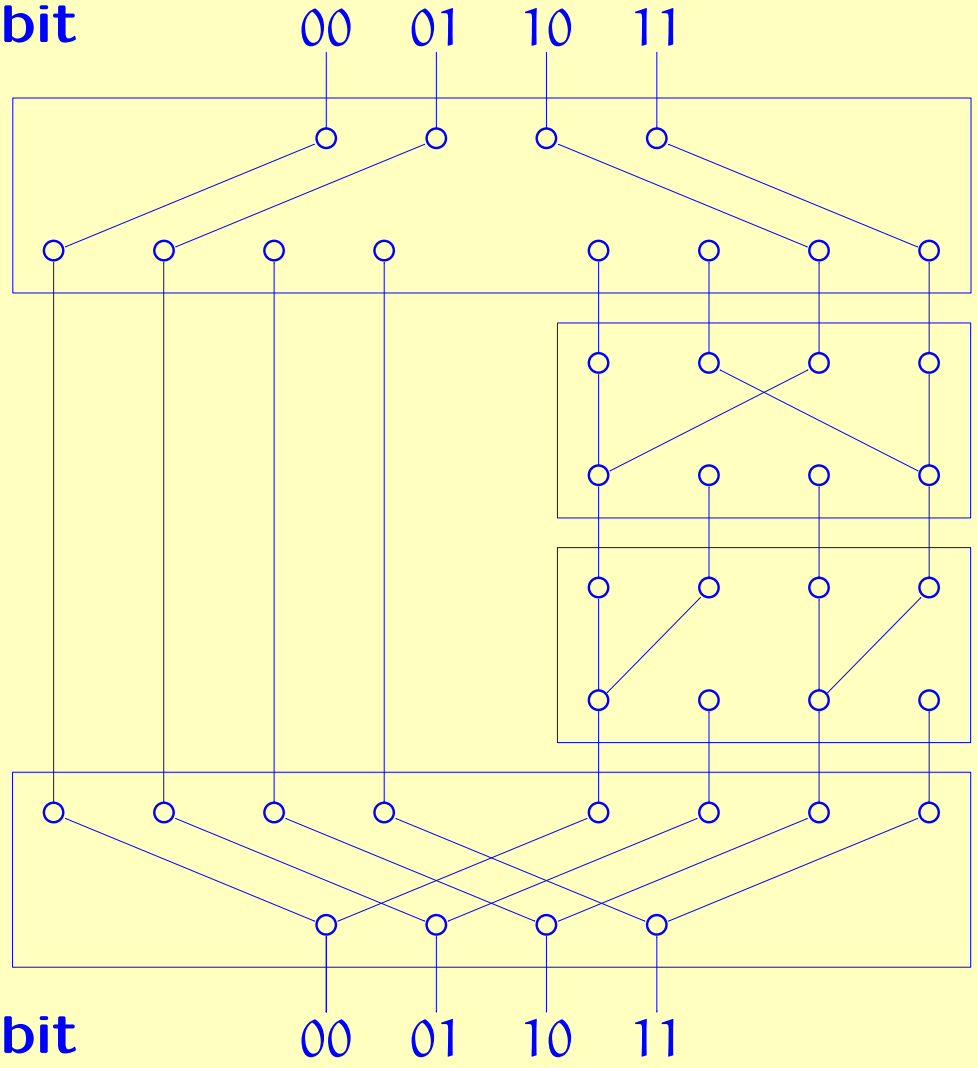
$x := t$ $\quad$ $p; q$ $\quad$ $\mathit{if}\ B\ \mathit{then}\ p\ \mathit{else}\ q$ $\quad$ $\mathit{while}\ B\ \mathit{do}\ p$

The classical case: A simple classical flow chart



Classical flow chart, with boolean variables expanded

input b, c : **bit**



output b, c : **bit**

$(*$ branch b $*)$

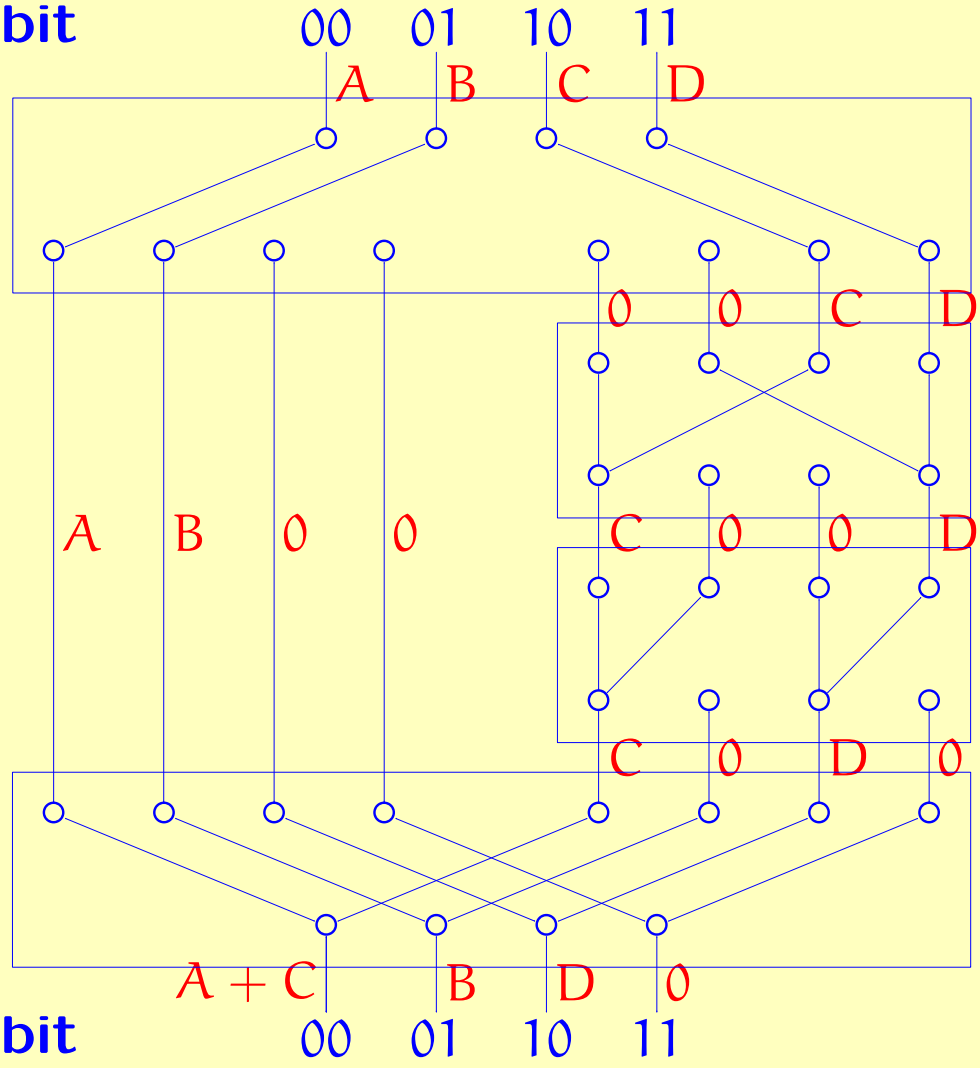
$(*$ $b := c$ $*)$

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

$(*$ merge $*)$

Classical flow chart, with boolean variables expanded

input b, c : **bit**



$(*$ branch b $*)$

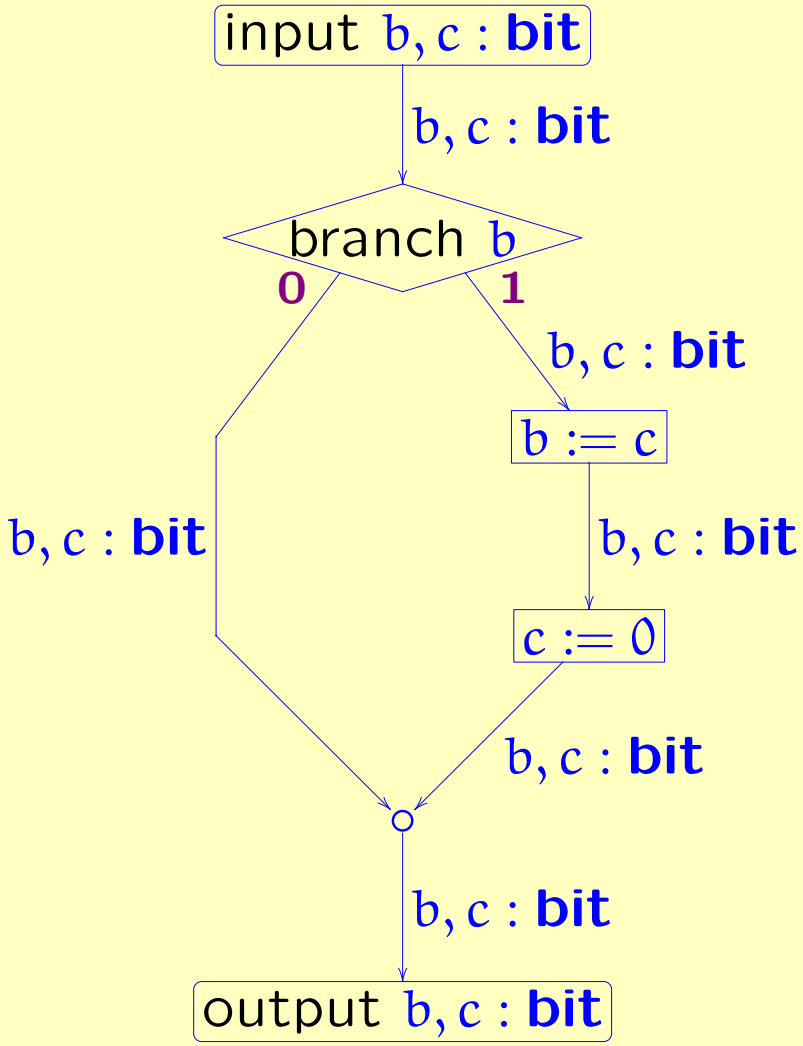
$(*$ $b := c$ $*)$

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

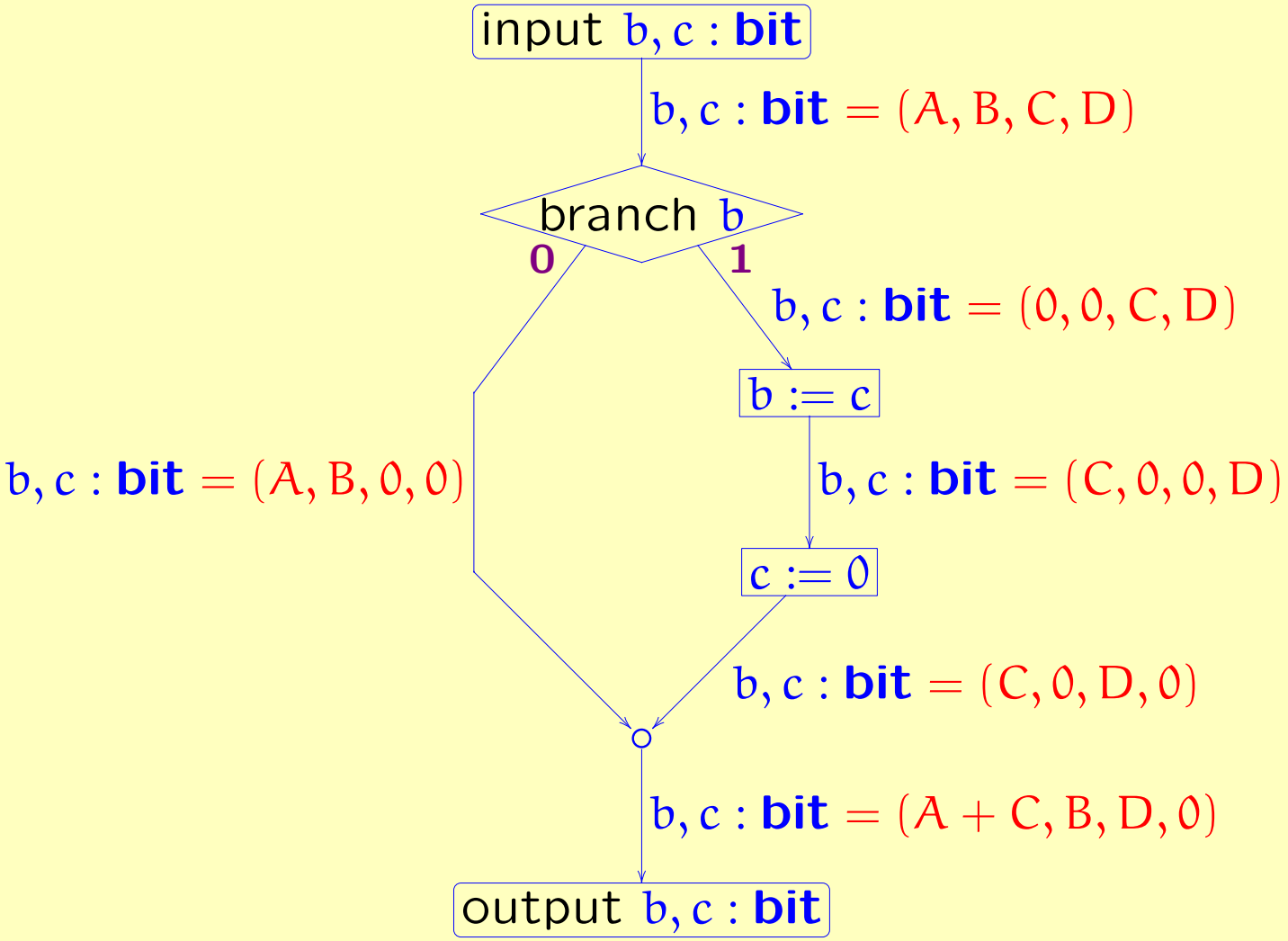
$(*$ merge $*)$

output b, c : **bit**

A simple classical flow chart

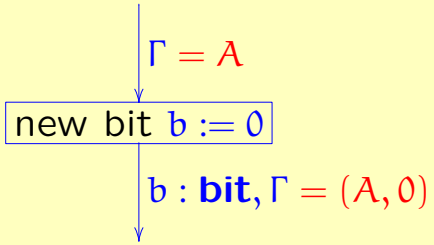


A simple classical flow chart

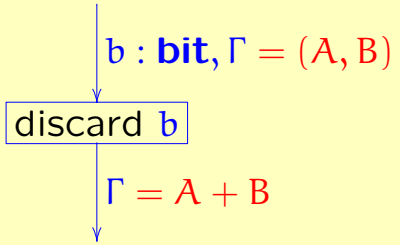


Summary of classical flow chart components

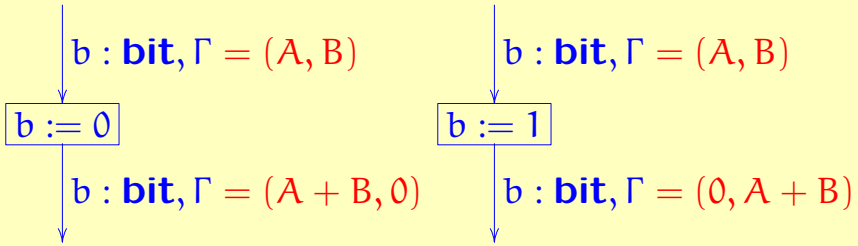
Allocate bit:



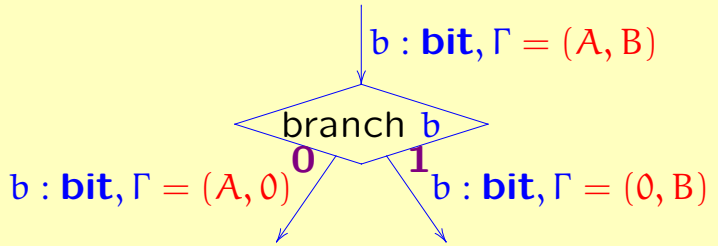
Discard bit:



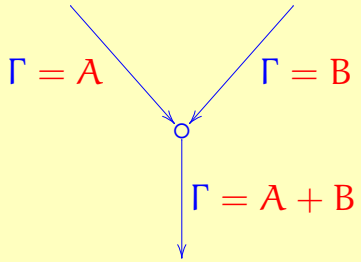
Assignment:



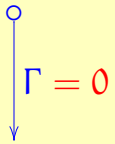
Branching:



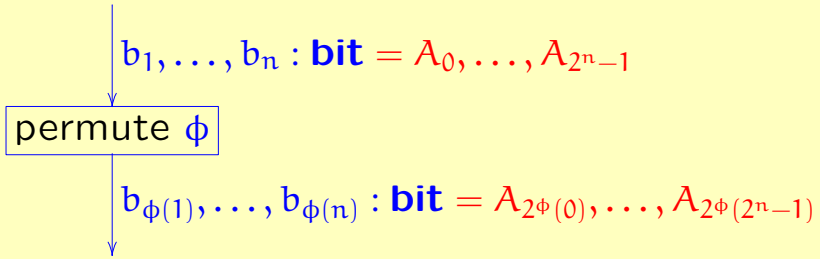
Merge:



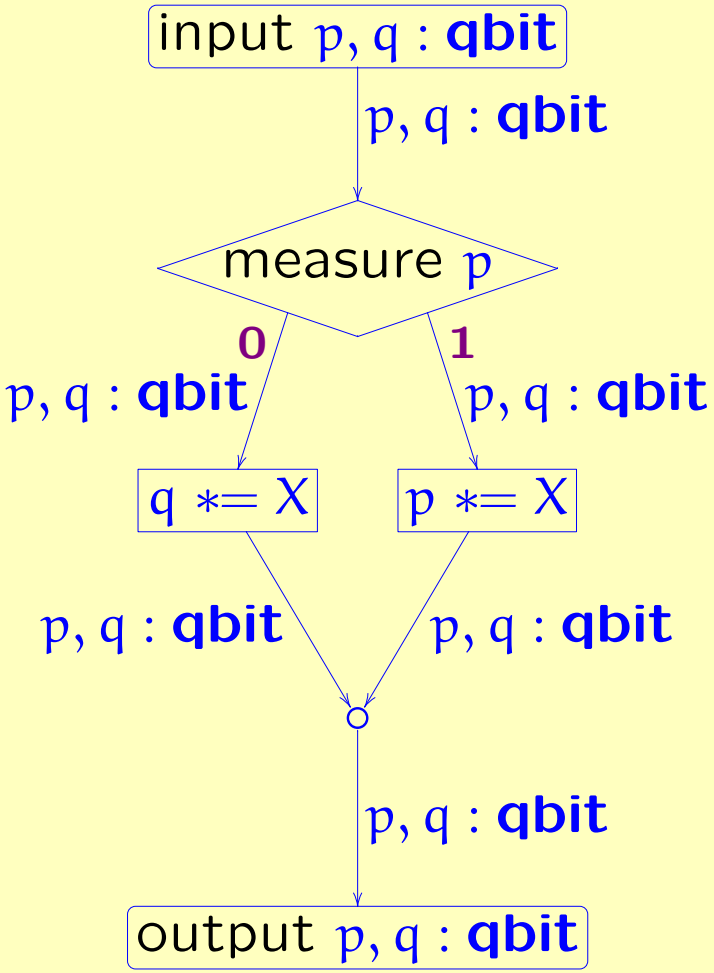
Initial:



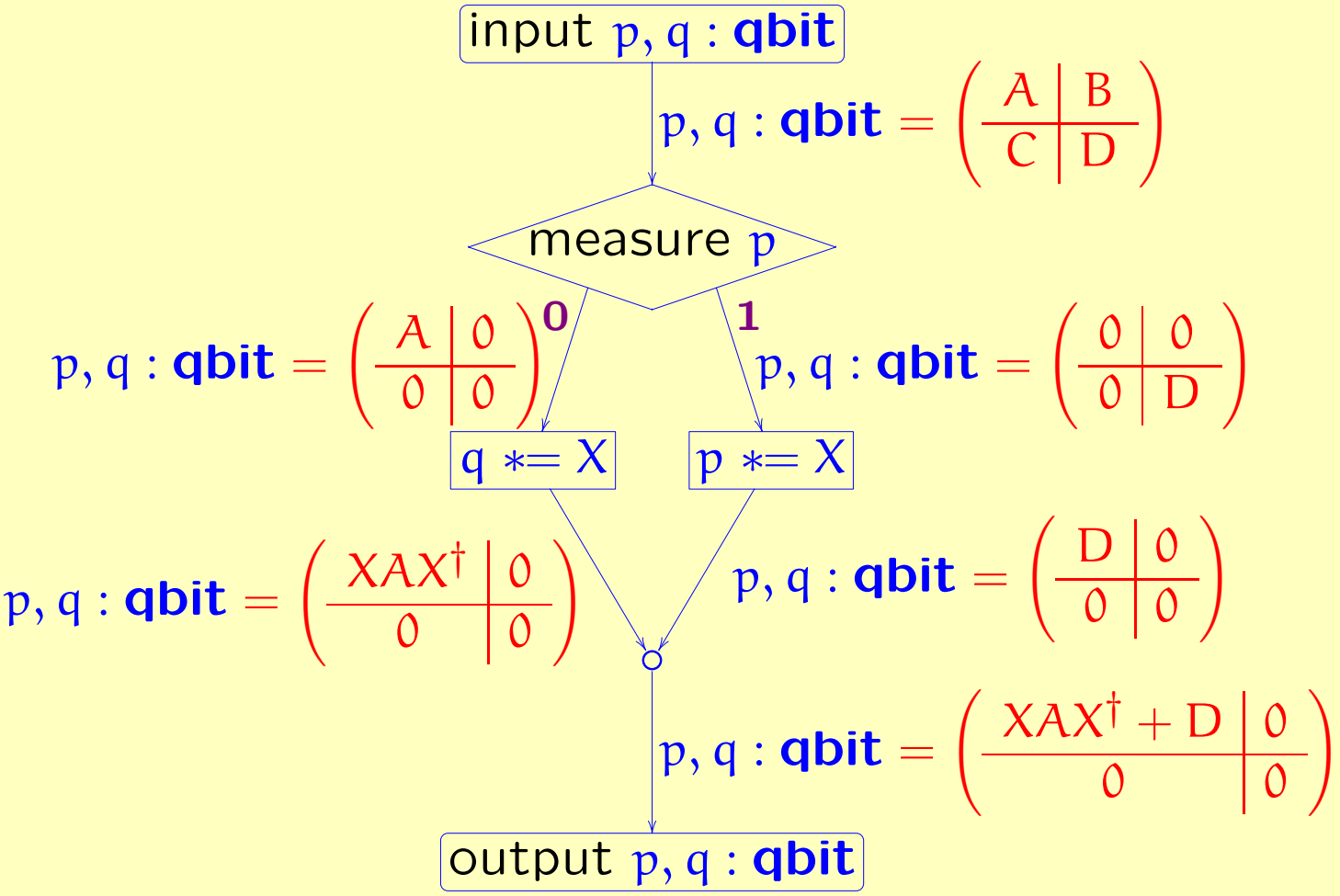
Permutation:



The quantum case: A simple quantum flow chart

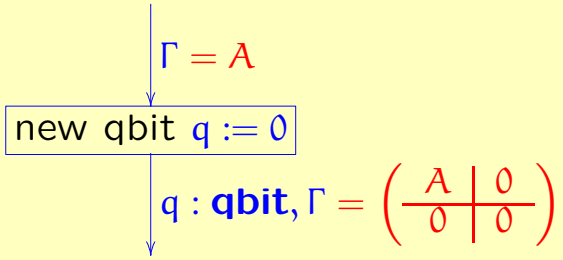


A simple quantum flow chart

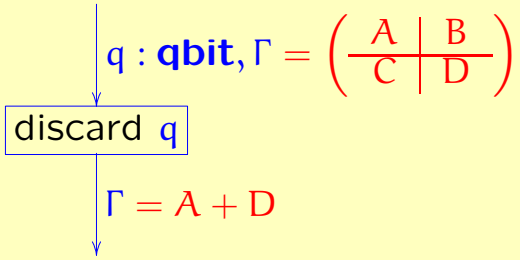


Summary of quantum flow chart components

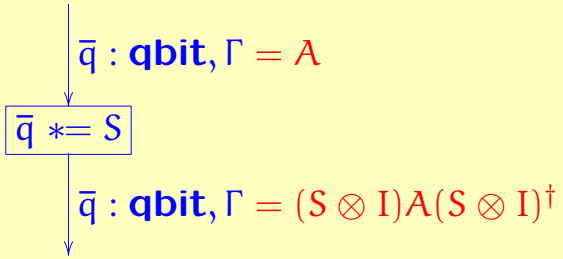
Allocate qbit:



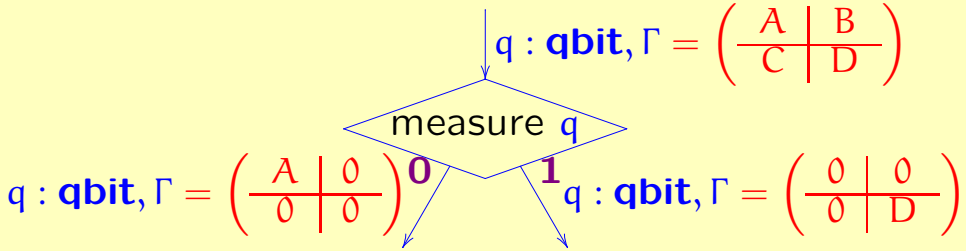
Discard qbit:



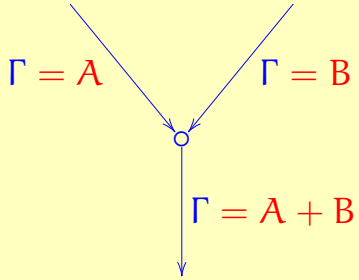
Unitary transformation:



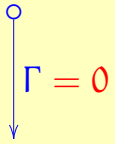
Measurement:



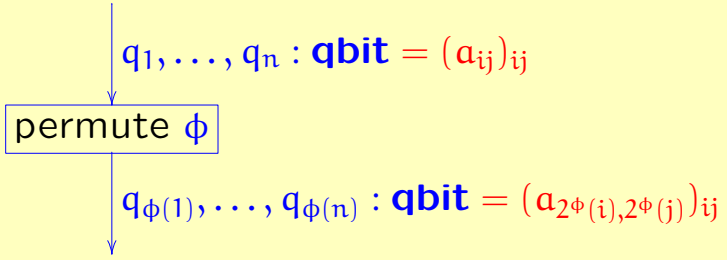
Merge:



Initial:



Permutation:



Combining classical data with quantum data

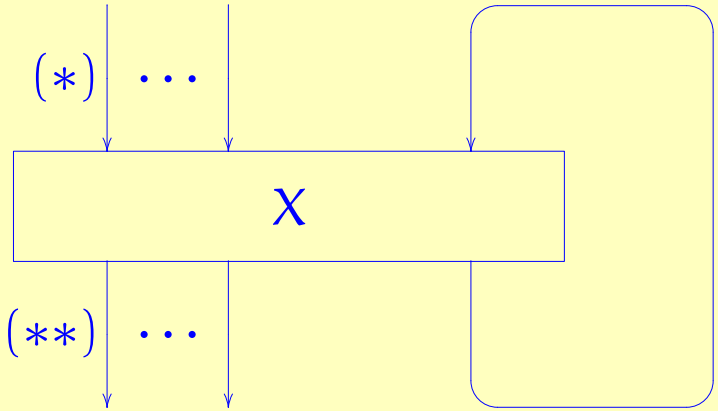
Consider typing contexts of the form

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

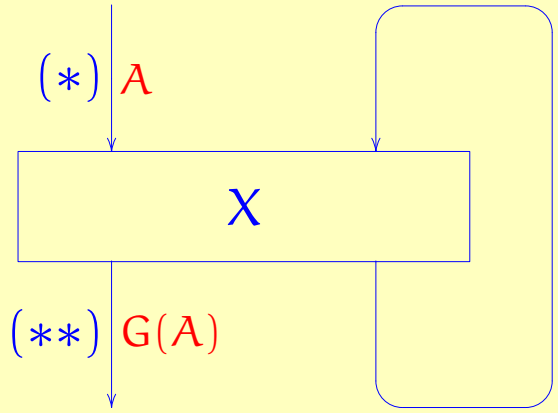
Definition. A *state* for the above typing context is a 2^n-tuple $(A_0, \ldots, A_{2^n-1})$ of density matrices, each of dimension $2^m \times 2^m$.

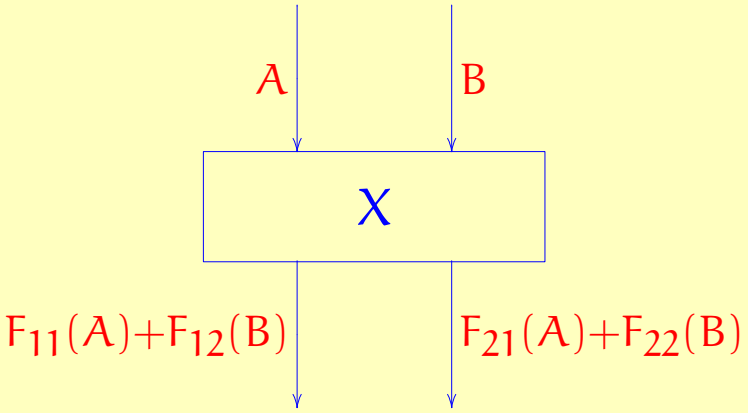
$$\begin{array}{lcl}
\mathrm{tr}\,(A_0, \ldots, A_{2^n-1}) & := & \sum_i \mathrm{tr}\, A_i, \\
(A_0, \ldots, A_{2^n-1})^\dagger & := & (A_0^\dagger, \ldots, A_{2^n-1}^\dagger), \\
S(A_0, \ldots, A_{2^n-1})S^\dagger & := & (SA_0S^\dagger, \ldots, SA_{2^n-1}S^\dagger), \\
|(A_0, \ldots, A_{2^n-1})|^2 & := & \sum_i |A_i|^2.
\end{array}$$

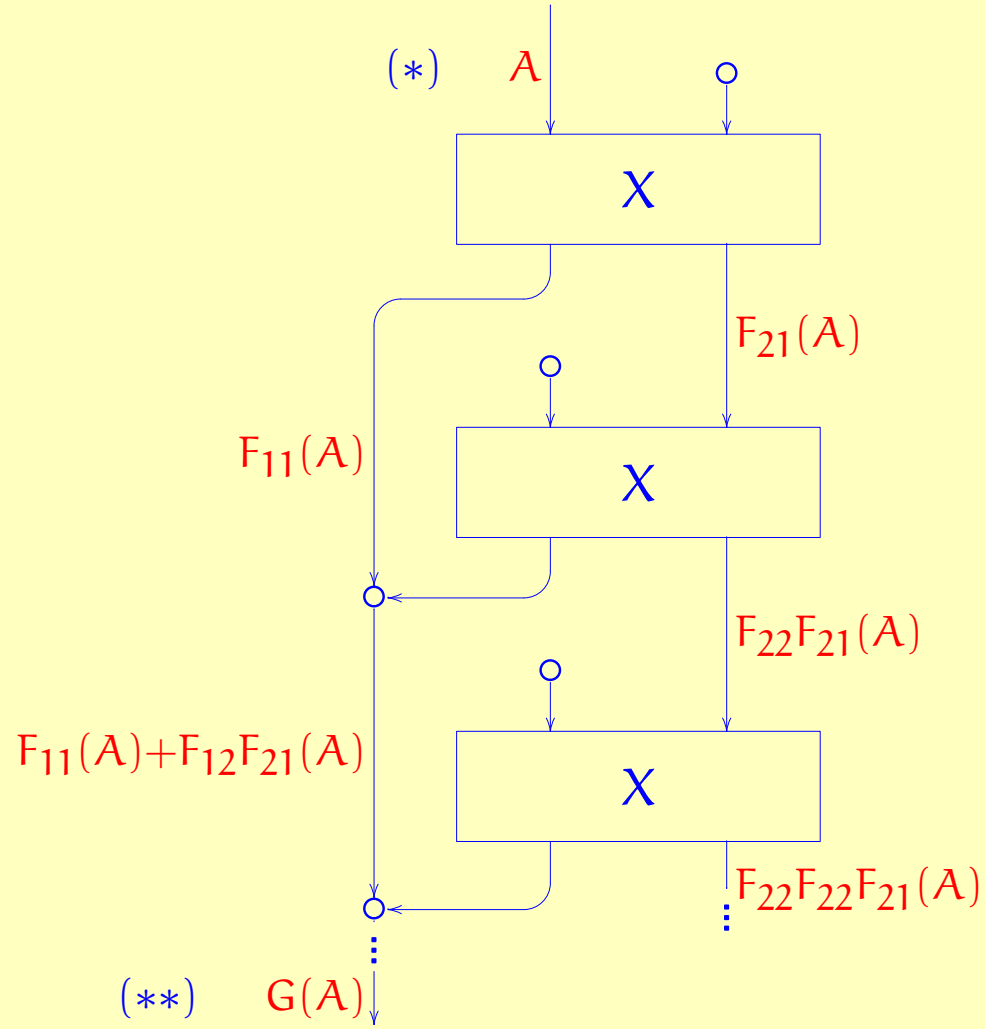
Loops



Unwinding a loop







Unwinding a loop

$$G(A) = F_{11}(A) + \sum_{i=0}^{\infty} F_{12}(F_{22}^{i}(F_{21}(A))).$$

Part IV: 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

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

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 for F to be the denotation of some flow chart.

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; Choi's theorem). 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

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

The category of superoperators

Objects: signatures $\sigma = n_1, \ldots, n_k$

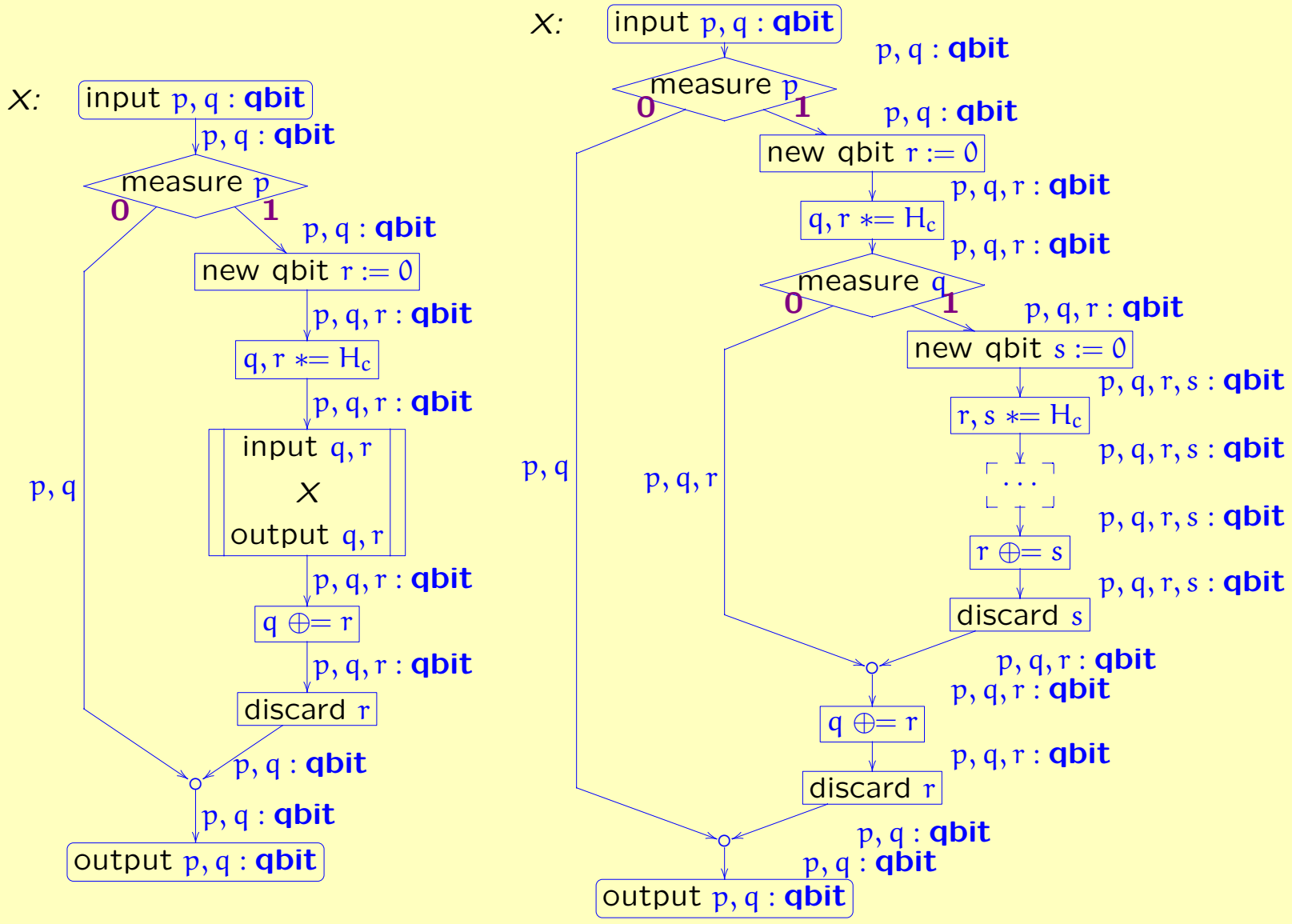
Morphisms: $f : \sigma \to \tau$ is a superoperator

$$f : \mathbb{C}^{n_1 \times n_1} \times \ldots \times \mathbb{C}^{n_k \times n_k} \to \mathbb{C}^{m_1 \times m_1} \times \ldots \times \mathbb{C}^{m_k \times m_{k'}}$$

Structure:

- symmetric monoidal category (horiz.+vert. composition)
- coproducts (merge, initial)
- CPO-enriched (fixpoints, recursion)
- traced monoidal (loops)

A recursive procedure and its unwinding



Calculating the denotation of a recursive procedure

The recursive procedure X defines a map Φ from superoperators to superoperators. Let $F_0 = 0$ and $F_{i+1} = \Phi(F_i)$. Then $G = \lim_{i\to\infty} F_i$.

In the example:

$$F_1(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, F_2(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, F_3(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} & 0 \\ 0 & 0 & 0 & \frac{1}{2}a_{33} \end{pmatrix},$$

$$F_4(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} + \frac{1}{4}a_{33} & 0 \\ 0 & 0 & 0 & \frac{1}{2}a_{33} \end{pmatrix}, F_5(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} + \frac{1}{4}a_{33} & 0 \\ 0 & 0 & 0 & \frac{1}{2}a_{33} + \frac{1}{8}a_{33} \end{pmatrix},$$

$$F_6(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} + \frac{1}{4}a_{33} + \frac{1}{16}a_{33} & 0 \\ 0 & 0 & 0 & \frac{1}{2}a_{33} + \frac{1}{8}a_{33} \end{pmatrix},$$

and so forth. The limit is

$$G(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} + \frac{1}{3}a_{33} & 0 \\ 0 & 0 & 0 & \frac{2}{3}a_{33} \end{pmatrix},$$

Continuing Kozen's "Rosetta Stone"

Deterministic	**Probabilistic**	**Quantum**
states	measures	density operators (mixed states)
predicates	measurable functions	observations
$\models$	$\int$	$\langle - \mid - \rangle$
binary relations	Markov kernels	superoperators
powerset monad	Giry monad	N/A
operational semantics	measure transformers (Cantor)	superoperators (annotation)
denotational semantics	measure transformers (Scott)	superoperators (compositional)
predicate transformers	measurable function transformers	dual superoperators

Part V: Predicate transformers

An inner product on matrices

If A and B are matrices, define

$$\langle A \mid B \rangle = \operatorname{tr} A^\dagger B.$$

Concretely, if $A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$ and $B = \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix}$, we have

$$\langle A \mid B \rangle = \bar{a}_{00} b_{00} + \bar{a}_{01} b_{01} + \bar{a}_{10} b_{10} + \bar{a}_{11} b_{11}.$$

In other words, this is just the usual "dot product" of the matrices, regarded as vectors.

Duality

Equality:

- $A = A'$ iff for all B, we have $\langle A \mid B \rangle = \langle A' \mid B \rangle$
- $B = B'$ iff for all A, we have $\langle A \mid B \rangle = \langle A \mid B' \rangle$

Positivity:

- $A \sqsupseteq 0$ iff for all $B \sqsupseteq 0$, we have $\langle A \mid B \rangle \geq 0$.
- $B \sqsupseteq 0$ iff for all $A \sqsupseteq 0$, we have $\langle A \mid B \rangle \geq 0$.

Trace / sub-unit:

- $\mathrm{tr}\, A \leq 1$ iff for all $B \sqsubseteq I$, we have $\langle A \mid B \rangle \leq 1$.
- $B \sqsubseteq I$ iff for all $\mathrm{tr}\, A \leq 1$, we have $\langle A \mid B \rangle \leq 1$.

Duality, continued

Linear maps:

- For every linear function F on matrices, there exists a unique linear function $F^\dagger$ on matrices, such that for all A, B:

$$\langle FA \mid B \rangle = \langle A \mid F^\dagger B \rangle.$$

- For every linear function G on matrices, there exists a unique linear function $G^\dagger$ on matrices, such that for all A, B:

$$\langle A \mid GB \rangle = \langle G^\dagger A \mid B \rangle.$$

States and observations

Definition.

- A *state* is a hermitian positive matrix A with $\mathrm{tr}\,\mathrm{A} \leq 1$ (i.e., a density matrix). Equivalently, the *sum* of the eigenvalues is ≤ 1.
- An *observation* is a hermitian positive matrix B with $\mathrm{B} \sqsubseteq \mathrm{I}$. Equivalently, the *maximum* of the eigenvalues is ≤ 1.

Definition.

- A *superoperator* is a completely positive map that takes states to states. Equivalently, it is trace-non-increasing.
- A *dual superoperator* is a completely positive map that takes observations to observations. Equivalently, $\mathrm{F}(\mathrm{I}) \sqsubseteq \mathrm{I}$.

F is a superoperator if and only if $\mathrm{F}^\dagger$ is a dual superoperator.

Kraus decomposition

Moreover, if a superoperator F has Kraus decomposition

$$F(A) = \sum_i S_i A S_i^\dagger,$$

then its dual superoperator $F^\dagger$ has Kraus decomposition

$$F^\dagger(B) = \sum_i S_i^\dagger B S_i.$$

Proof: trivial, because

$$\langle \sum_i S_i A S_i^\dagger \mid B \rangle = \langle A \mid \sum_i S_i^\dagger B S_i \rangle.$$

Both are, by definition, equal to $\sum_i \mathrm{tr}(S_i A S_i^\dagger B)$f.

Predicate transformer semantics for quantum computing
[D'Hondt/Panangaden 2004] [Feng/Duan/Ji/Ying 2005]

Definition. We write $A \models_p B$ for the assertion

$$\langle A \mid B \rangle \geq p.$$

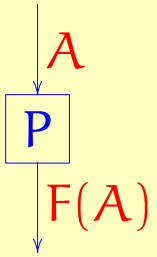
This is the probability that observation B succeeds in state A. We say that state A "satisfies" observation B with probability p.

Definition. We write $\{B_1\}\, P\, \{B_2\}$ for the assertion

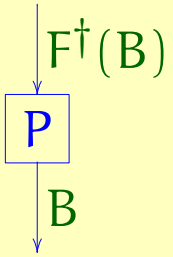
$$\text{for all } A \text{ and all } p, \quad A \models_p B_1 \quad \Rightarrow \quad P(A) \models_p B_2.$$

Informally, if state A satisfies B_1 before executing the program, then $P(A)$ satisfies B_2 after executing the program (with at least the same probability).

If a program has forward semantics given by a superoperator $\mathbb{F}$:

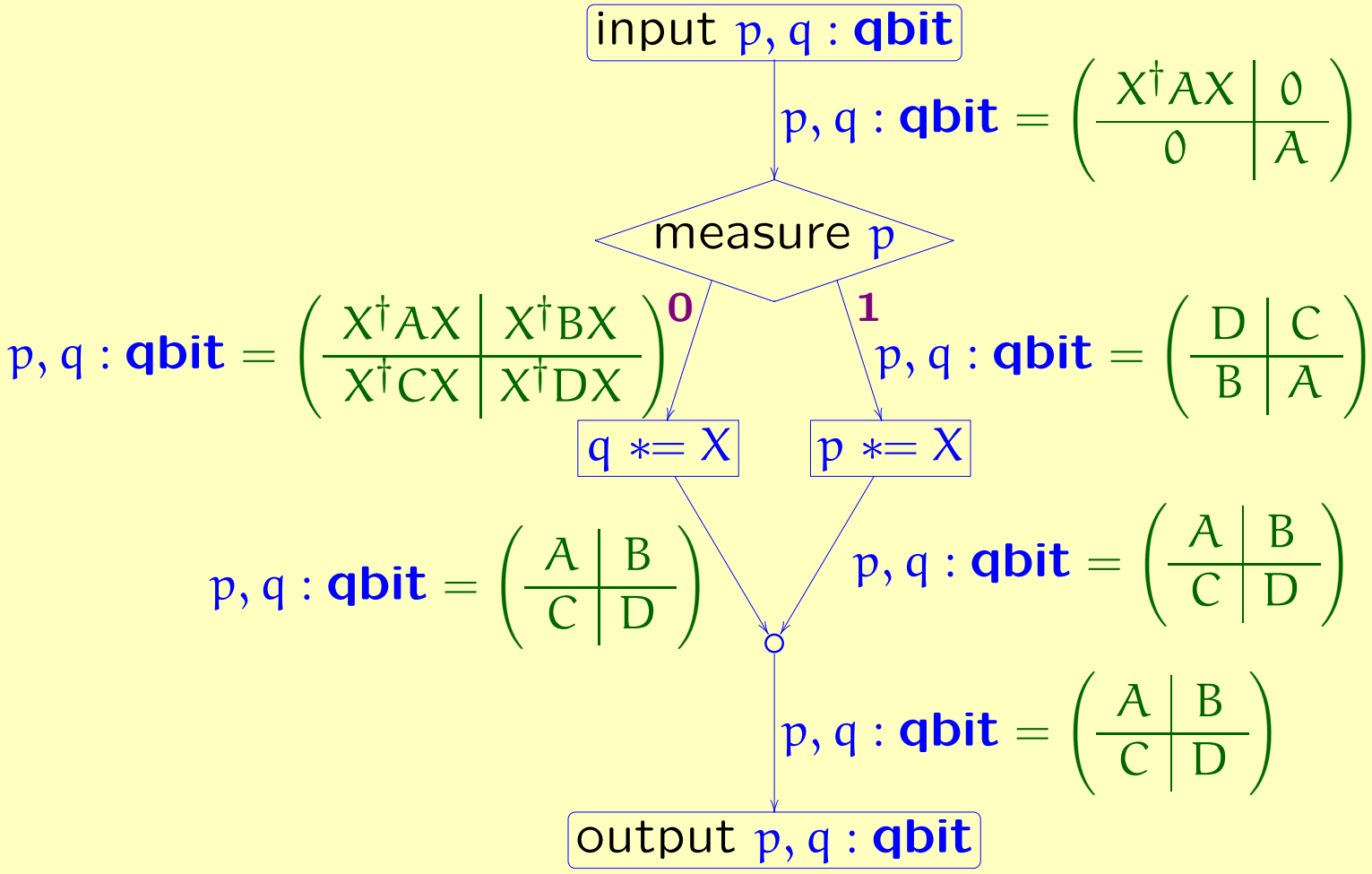


then its backwards (predicate transformer) semantics is given by the dual superoperator $\mathbb{F}^\dagger$:



Predicate transformer semantics for quantum computing

[D'Hondt/Panangaden 2004] [Feng/Duan/Ji/Ying 2005]



Weakest preconditions and weakest liberal preconditions

We have:

$$
\begin{array}{ll}
 & \{B_1\}\,P\,\{B_2\} \\
\iff & \text{for all } A,\ p, \quad A \models_p B_1 \Rightarrow P(A) \models_p B_2 \\
\iff & \text{for all } A,\ p, \quad \langle A \mid B_1 \rangle \geq p \Rightarrow \langle P(A) \mid B_2 \rangle \geq p \\
\iff & \text{for all } A, \quad \langle A \mid B_1 \rangle \leq \langle P(A) \mid B_2 \rangle \\
\iff & \text{for all } A, \quad \langle A \mid B_1 \rangle \leq \langle A \mid P^\dagger(B_2) \rangle \\
\iff & \text{for all } A, \quad \langle A \mid B_1 \rangle \leq \langle A \mid P^\dagger(B_2) \rangle \\
\iff & B_1 \sqsubseteq P^\dagger(B_2).
\end{array}
$$

So the Hoare tripe $\{B_1\}\,P\,\{B_2\}$ is equivalent to $B_1 \sqsubseteq P^\dagger(B_2)$. In other words, $P^\dagger(B_2)$ is the *weakest precondition*.

In modal notation: $\langle P \rangle B = P^\dagger(B)$.

Weakest liberal preconditions can also be defined, via $[P]B = I - \langle P \rangle (I - B)$ [Feng/Duan/Ji/Ying 2005].

Kozen's "Rosetta Stone"

Deterministic	**Probabilistic**	**Quantum**
states	measures	states $\mathbb{A}$
predicates	measurable functions	observations $\mathbb{B}$
$\models$	$\int$	$\langle - \mid - \rangle$
binary relations	Markov kernels	superoperators
powerset monad	Giry monad	N/A
operational semantics	measure transformers (Cantor)	superoperators (annotation)
denotational semantics	measure transformers (Scott)	superoperators (compositional)
predicate transformers	measurable function transformers	dual superoperators

Thanks!