Introduction to Quantum Programming

Peter Selinger

Dalhousie University
Halifax, Canada

University of Warsaw, September 24–26, 2018

Part I: Quantum Computation

Linear Algebra Review

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

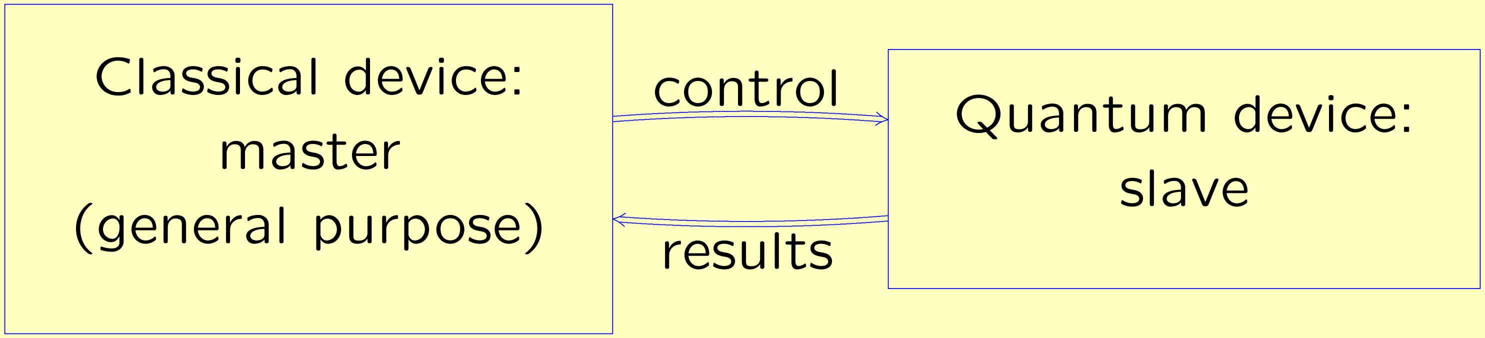
- Adjoint $A^\dagger = (\overline{a_{ji}})_{ij}$, trace $\operatorname{tr} A = \sum_i a_{ii}$, norm $\|A\|^2 = \sum_{ij} |a_{ij}|^2$.

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

- 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

Some standard unitary gates

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

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

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

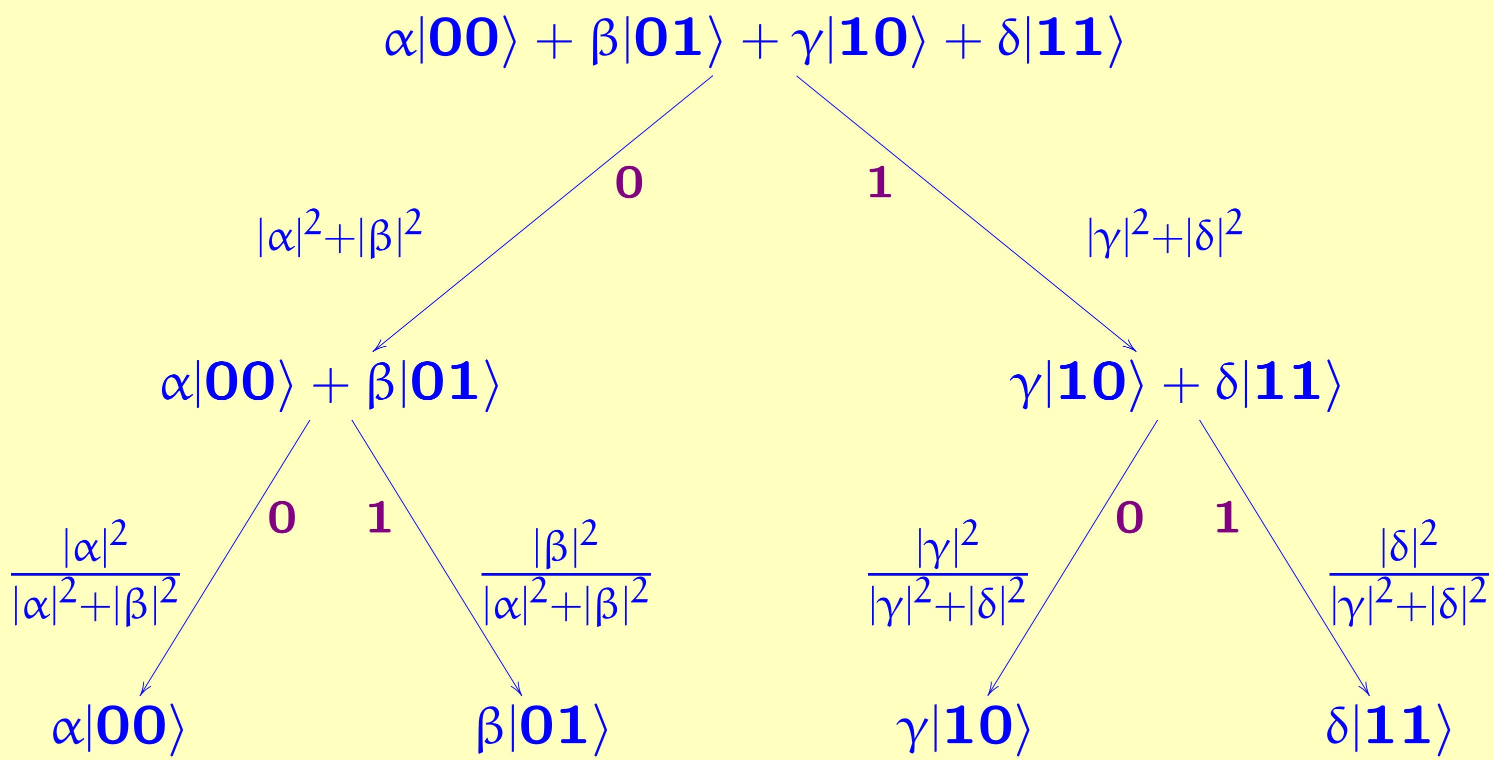
Measurement

$$\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$$

$|\alpha|^2$ **0** → $\alpha|\mathbf{0}\rangle$

1 $|\beta|^2$ → $\beta|\mathbf{1}\rangle$

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:

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

Measurement:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \qquad\qquad \begin{pmatrix} \alpha\bar\alpha & \alpha\bar\beta \\ \beta\bar\alpha & \beta\bar\beta \end{pmatrix} \qquad\qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\mathbf{0}\ \xrightarrow{|\alpha|^2} \qquad \mathbf{1}\ \xrightarrow{|\beta|^2} \qquad\qquad \mathbf{0}\ \xrightarrow{\alpha\bar\alpha} \qquad \mathbf{1}\ \xrightarrow{\beta\bar\beta} \qquad\qquad \mathbf{0}\ \xrightarrow{a} \qquad \mathbf{1}\ \xrightarrow{d}$$

$$\begin{pmatrix} \alpha \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ \beta \end{pmatrix} \qquad \begin{pmatrix} \alpha\bar\alpha & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & \beta\bar\beta \end{pmatrix} \qquad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}$$

A complete partial order of density matrices

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

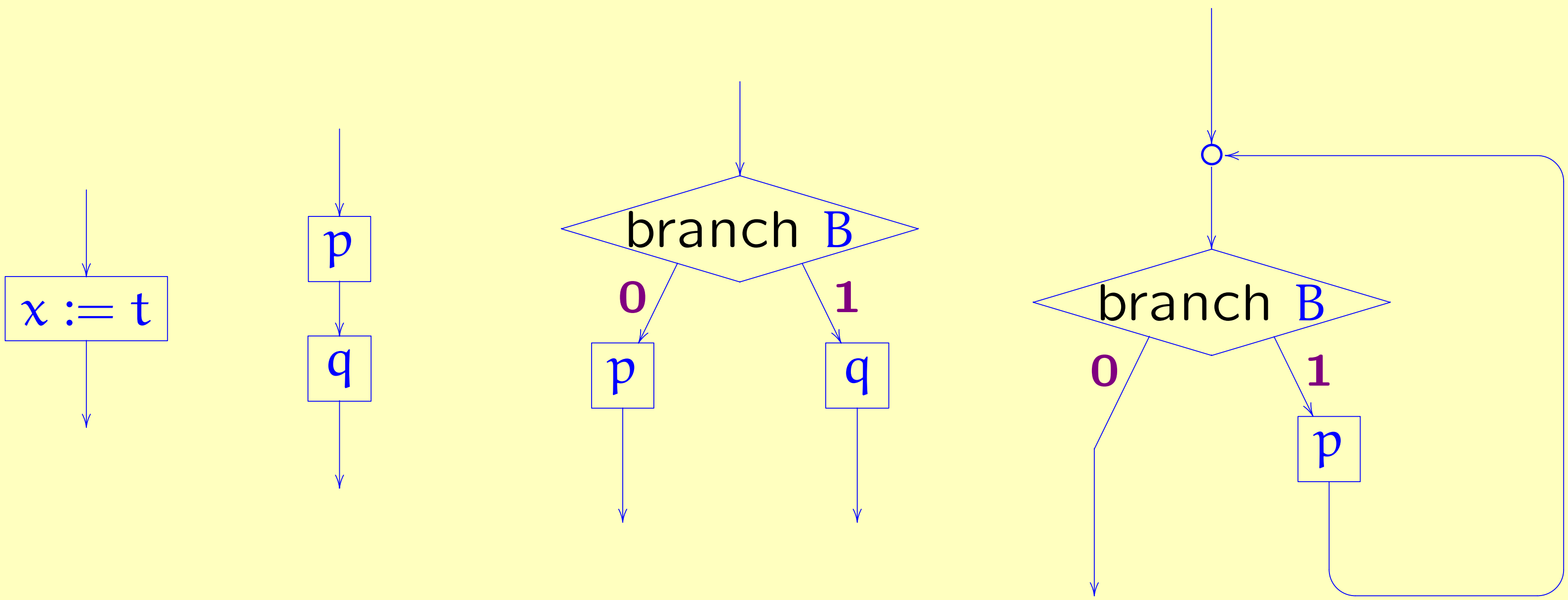
Definition. We write $A \sqsubseteq B$ if $B - A$ is positive.

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

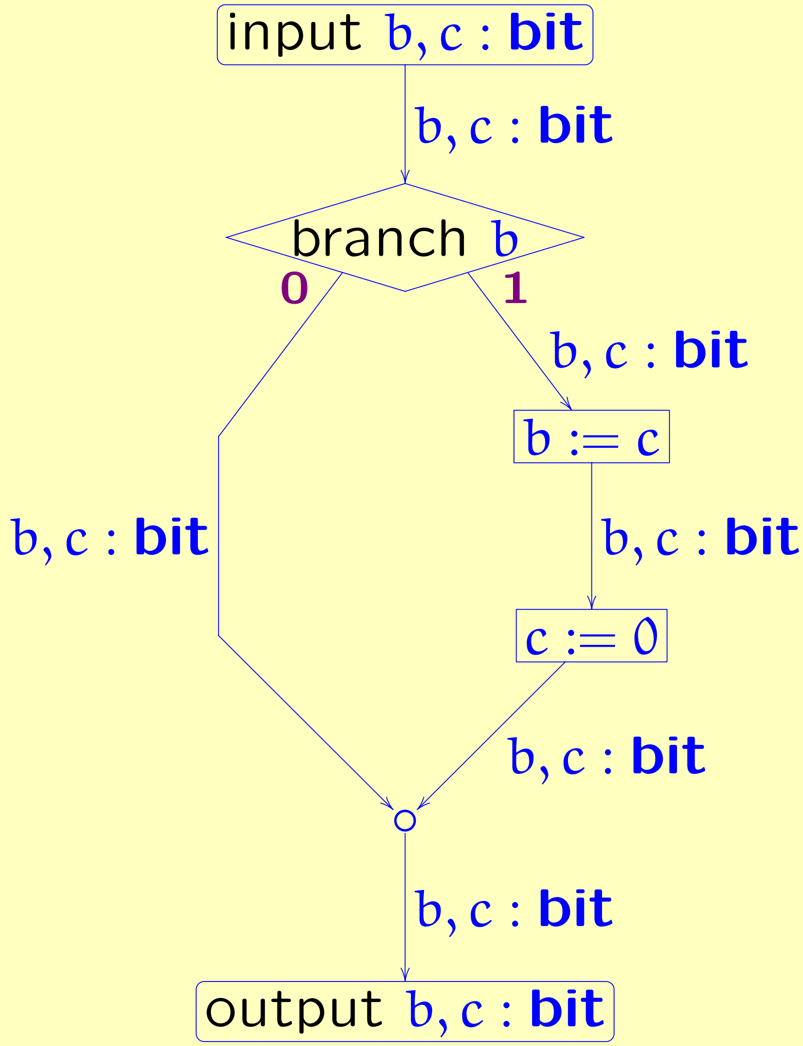
Part III: The Flow Chart Language

First: the classical case



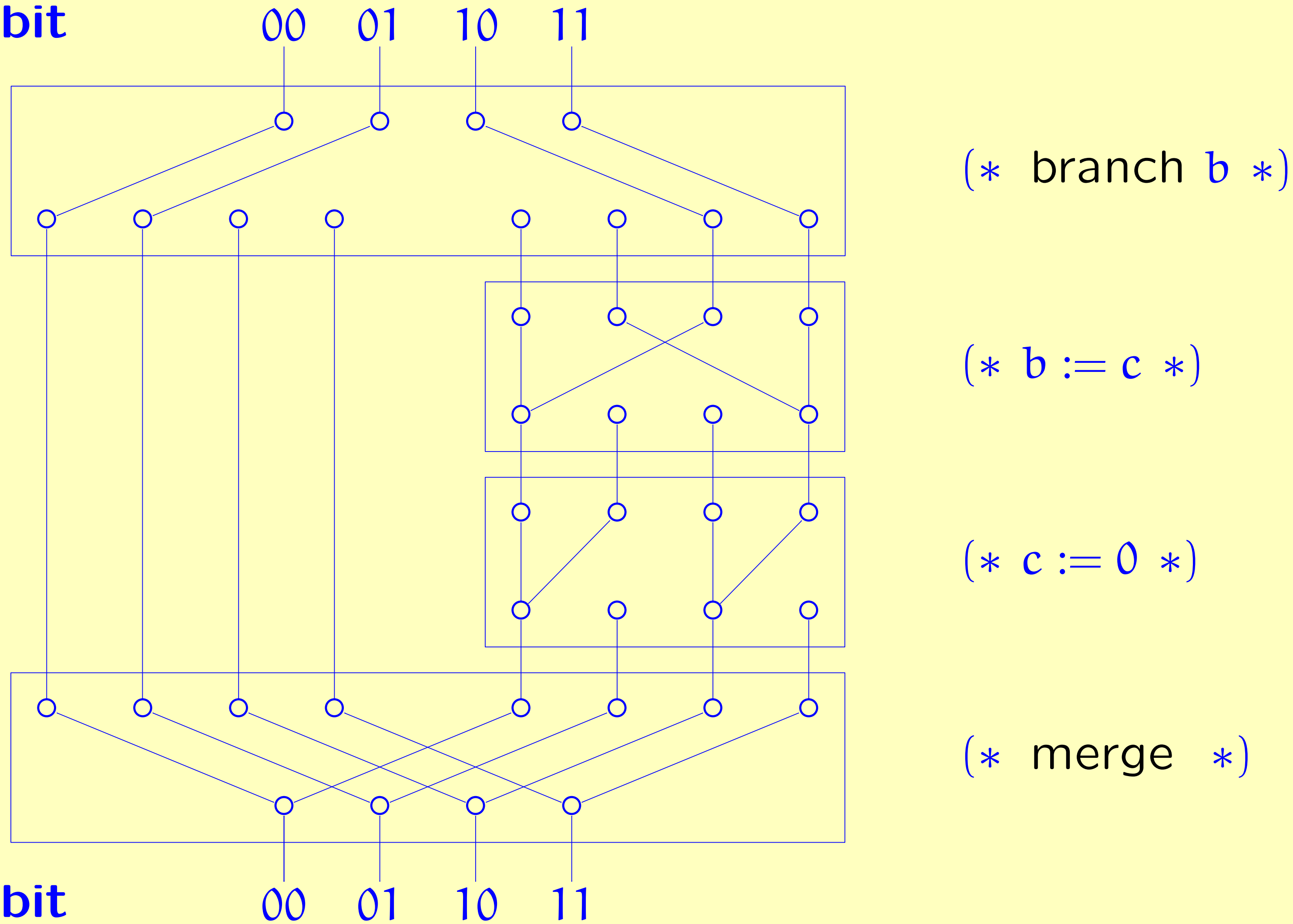
x := t   p; q   if B then p else q   while B do p

The classical case: A simple classical flow chart



Classical flow chart, with boolean variables expanded

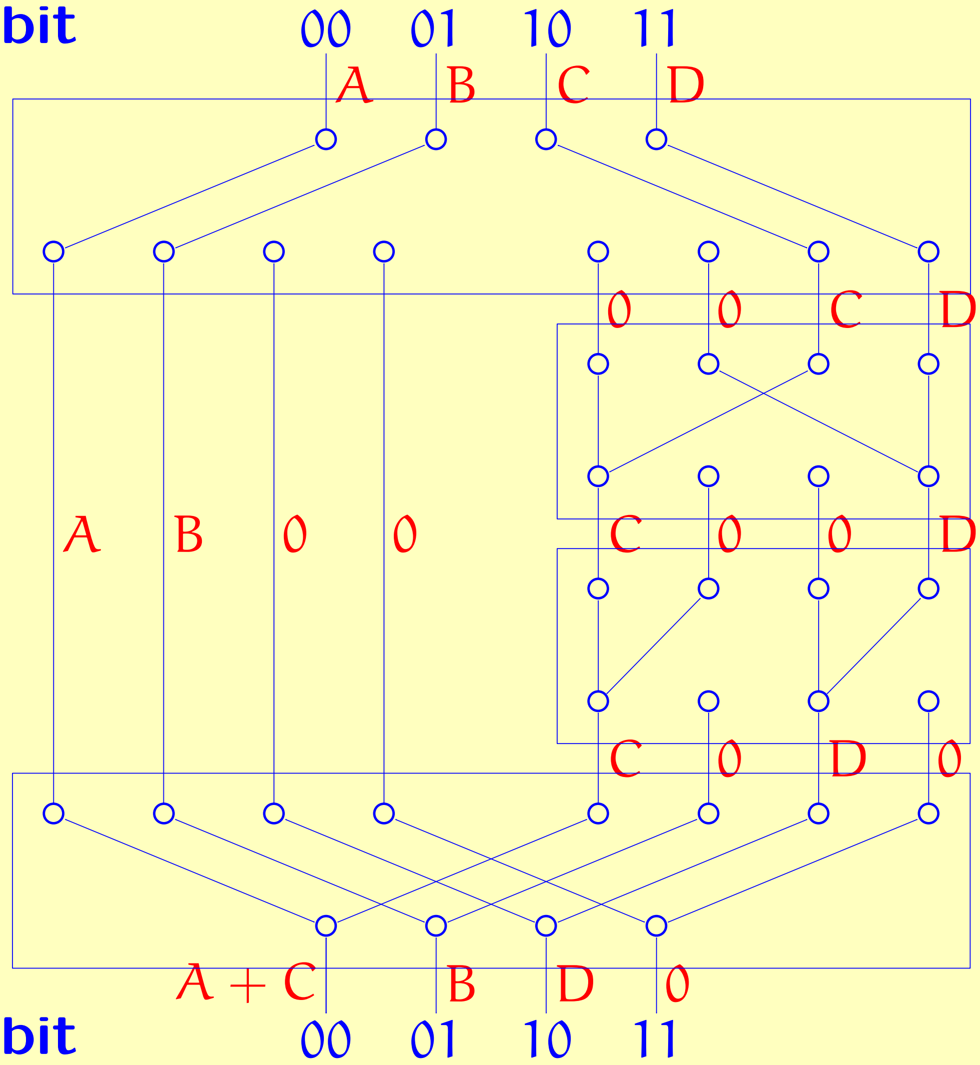
input $b, c :$ **bit**



output $b, c :$ **bit**

Classical flow chart, with boolean variables expanded

input $b, c :$ **bit**



(* branch b *)

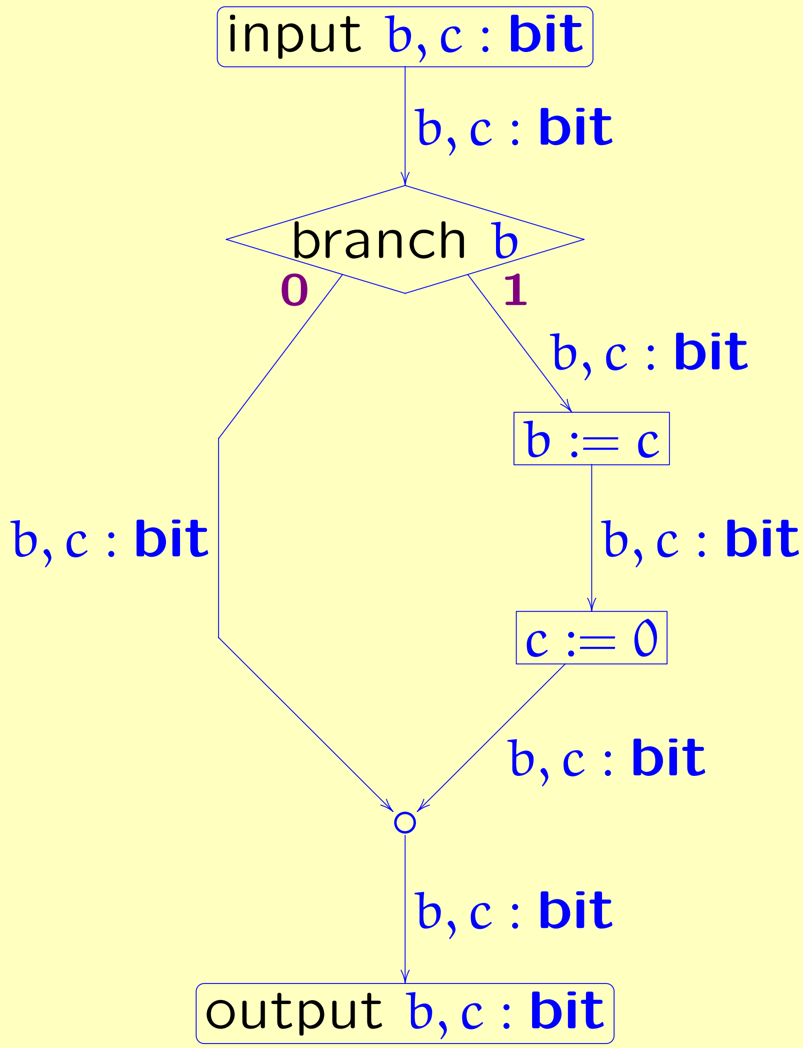
(* $b := c$ *)

(* $c := 0$ *)

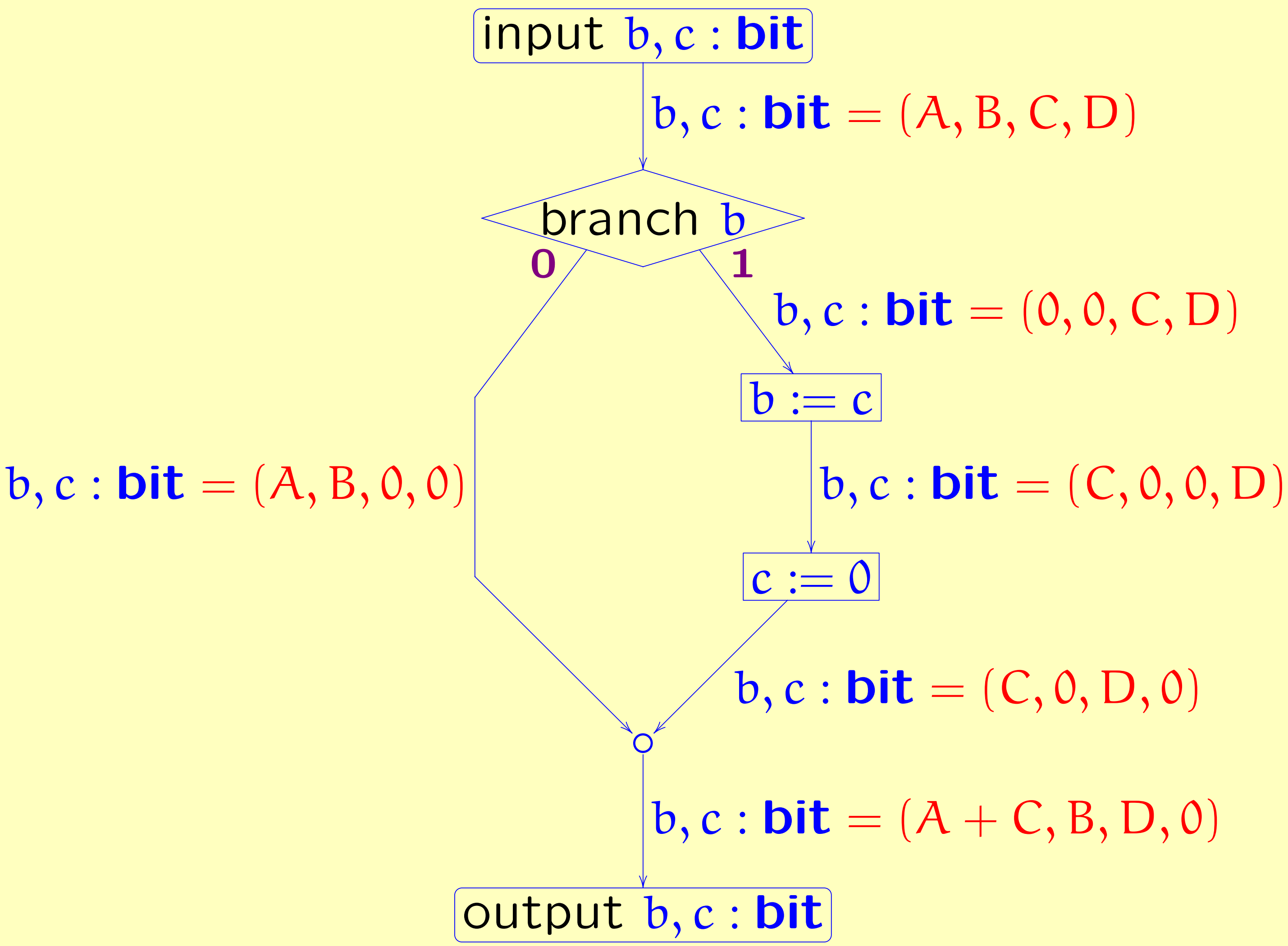
(* merge *)

output $b, c :$ **bit**

A simple classical flow chart

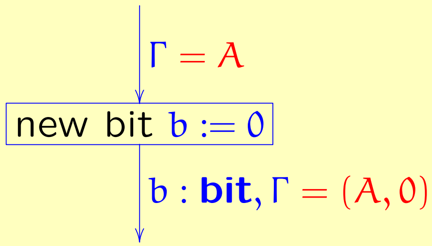


A simple classical flow chart

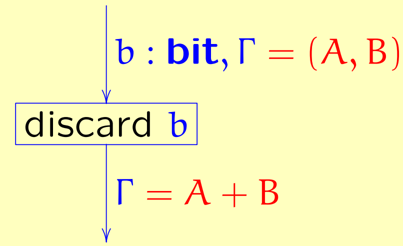


Summary of classical flow chart components

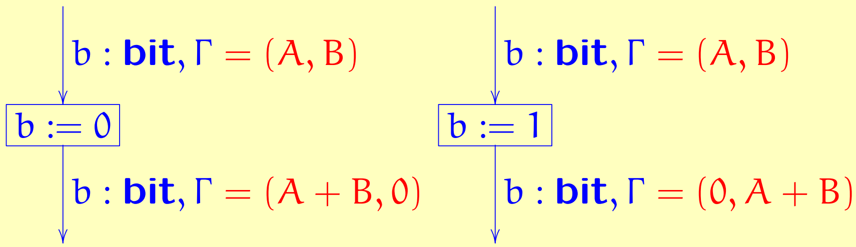
Allocate bit:



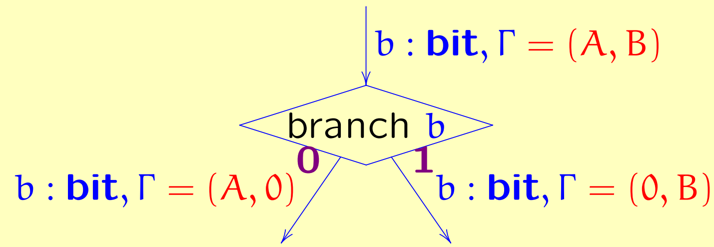
Discard bit:



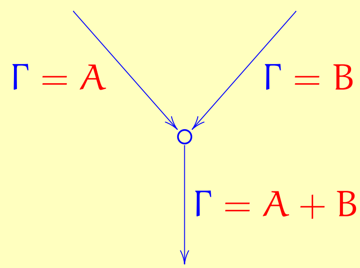
Assignment:



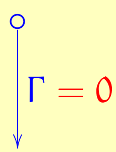
Branching:



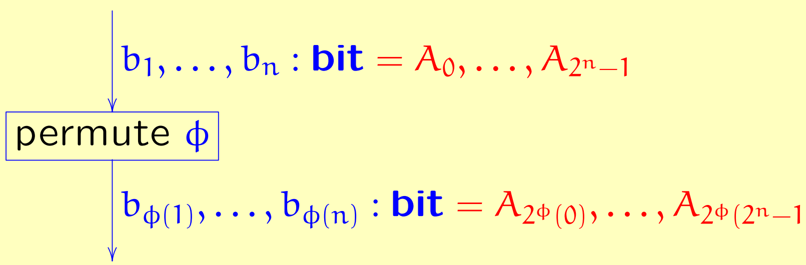
Merge:



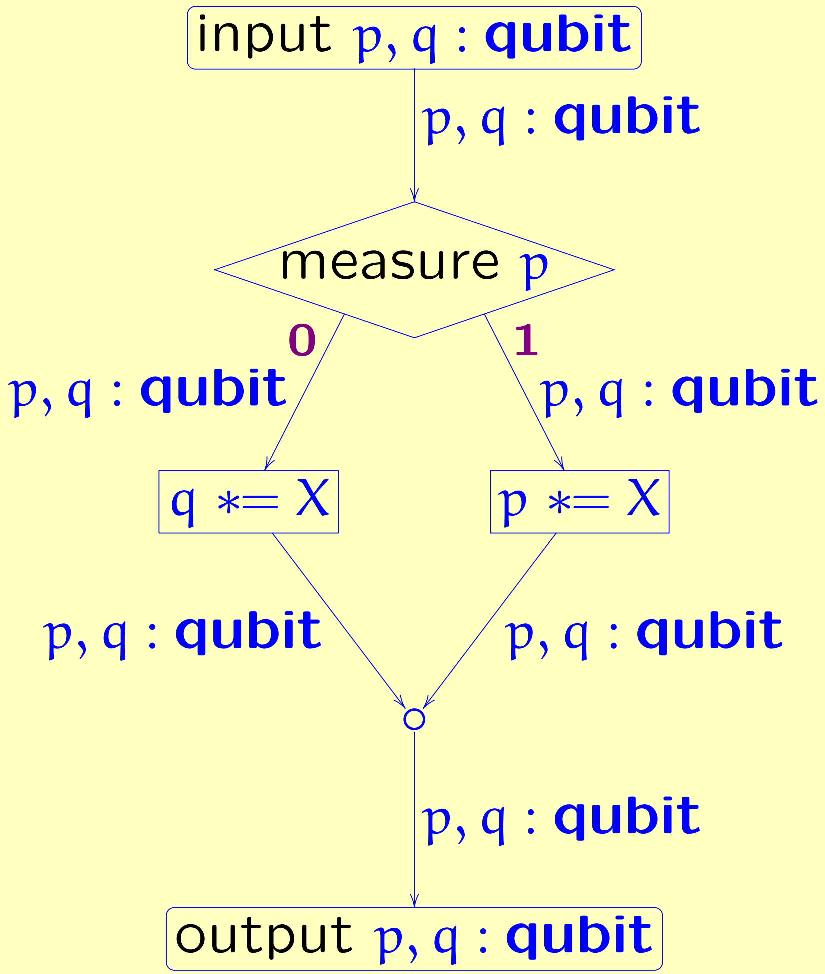
Initial:



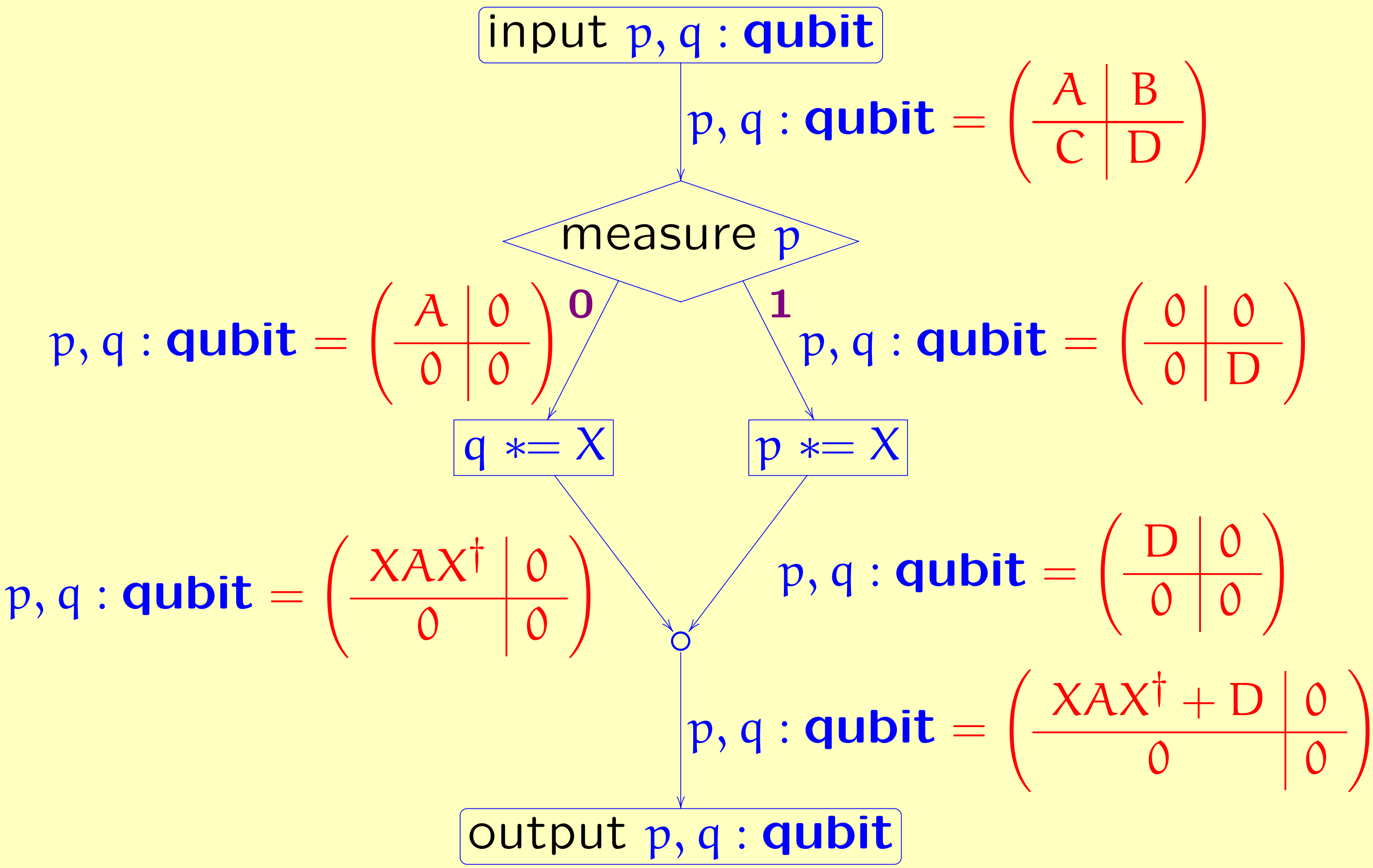
Permutation:



The quantum case: A simple quantum flow chart

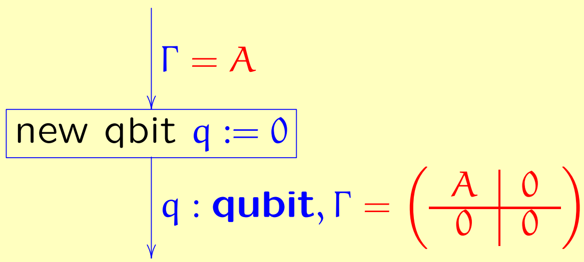


A simple quantum flow chart

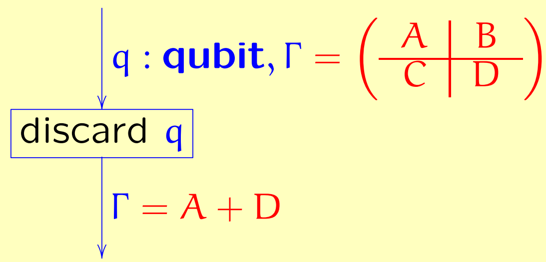


Summary of quantum flow chart components

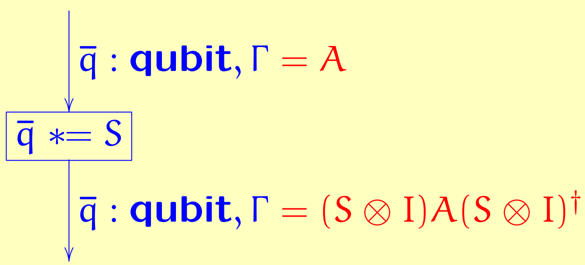
Allocate qbit:



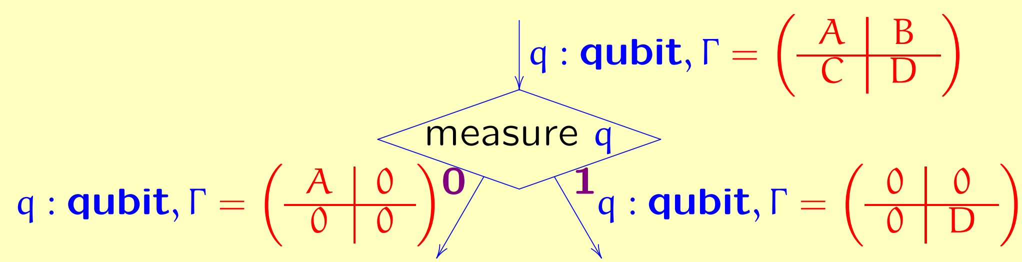
Discard qbit:



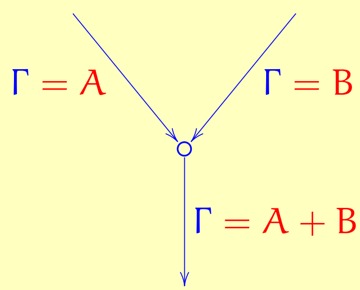
Unitary transformation:



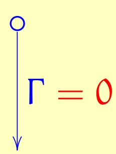
Measurement:



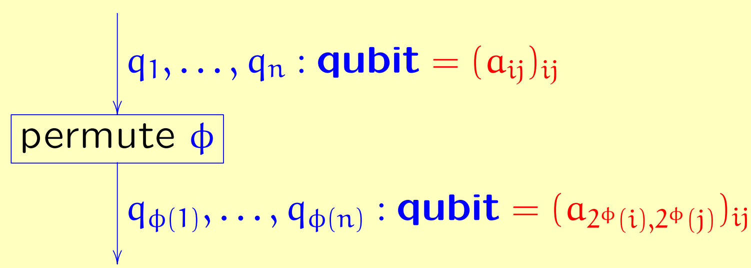
Merge:



Initial:



Permutation:



Combining classical data with quantum data

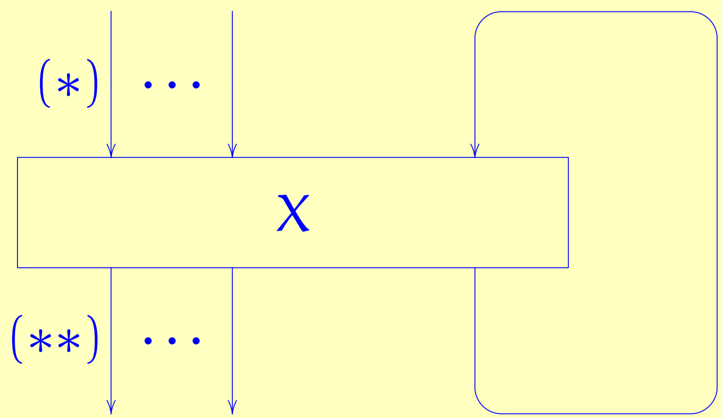
Consider typing contexts of the form

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

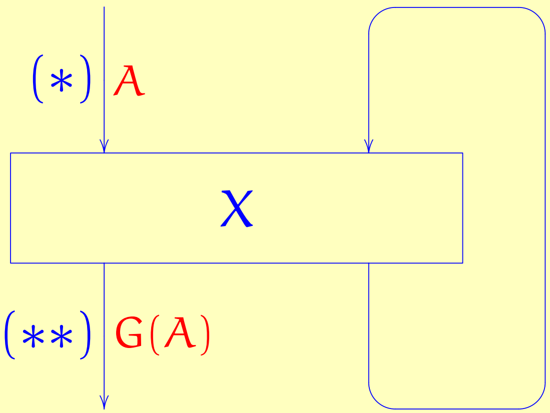
Definition. A *state* for the above typing context is a 2^n-tuple $(A_0, \ldots, A_{2^n-1})$ of density matrices, each of dimension $2^m \times 2^m$.

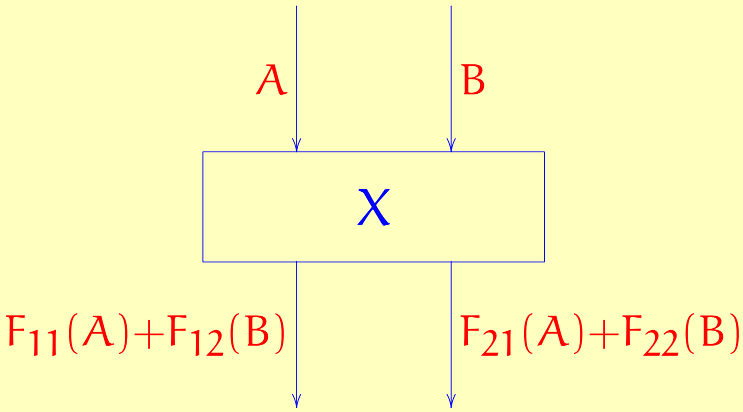
$$\begin{array}{lcl} \mathrm{tr}\,(A_0, \ldots, A_{2^n-1}) & := & \sum_i \mathrm{tr}\, A_i, \\ (A_0, \ldots, A_{2^n-1})^\dagger & := & (A_0^\dagger, \ldots, A_{2^n-1}^\dagger), \\ S(A_0, \ldots, A_{2^n-1})S^\dagger & := & (SA_0S^\dagger, \ldots, SA_{2^n-1}S^\dagger), \\ |(A_0, \ldots, A_{2^n-1})|^2 &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

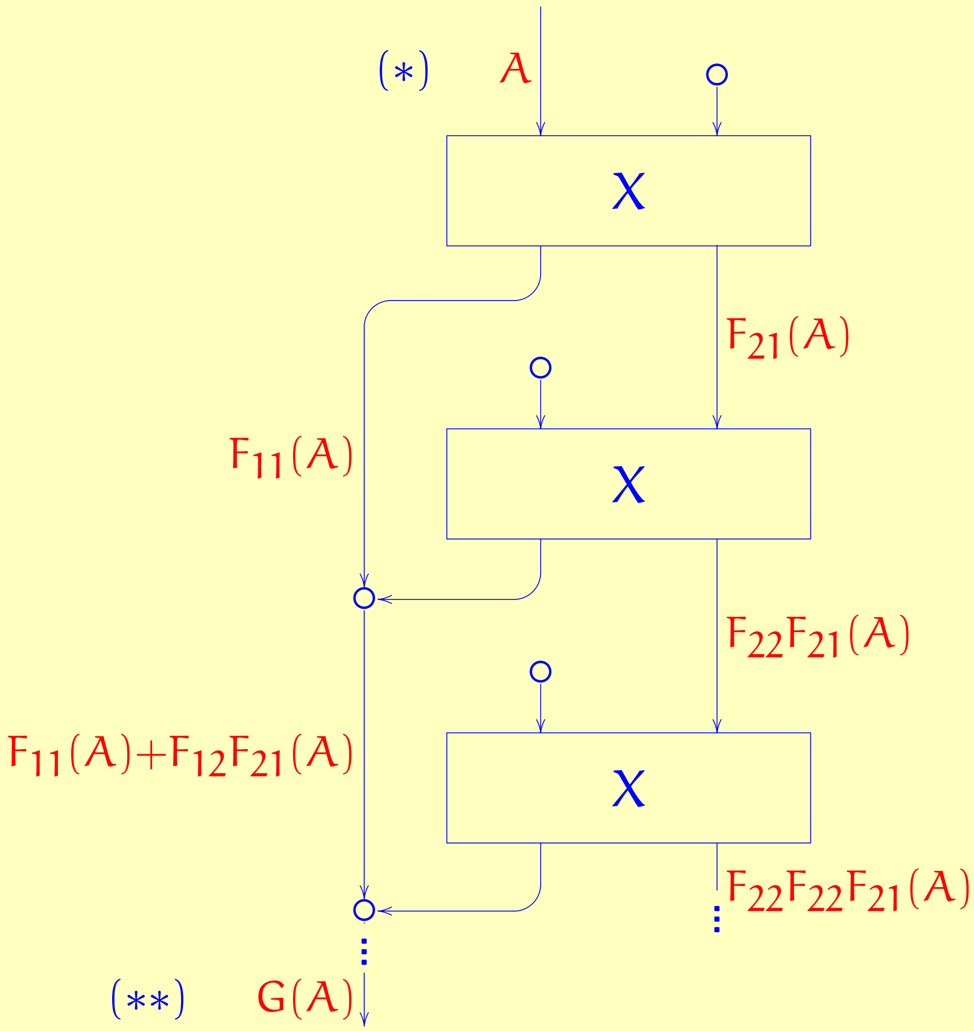
Loops



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

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

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-Jamiołkowski 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 $\sigma = n_1, \ldots, n_k$

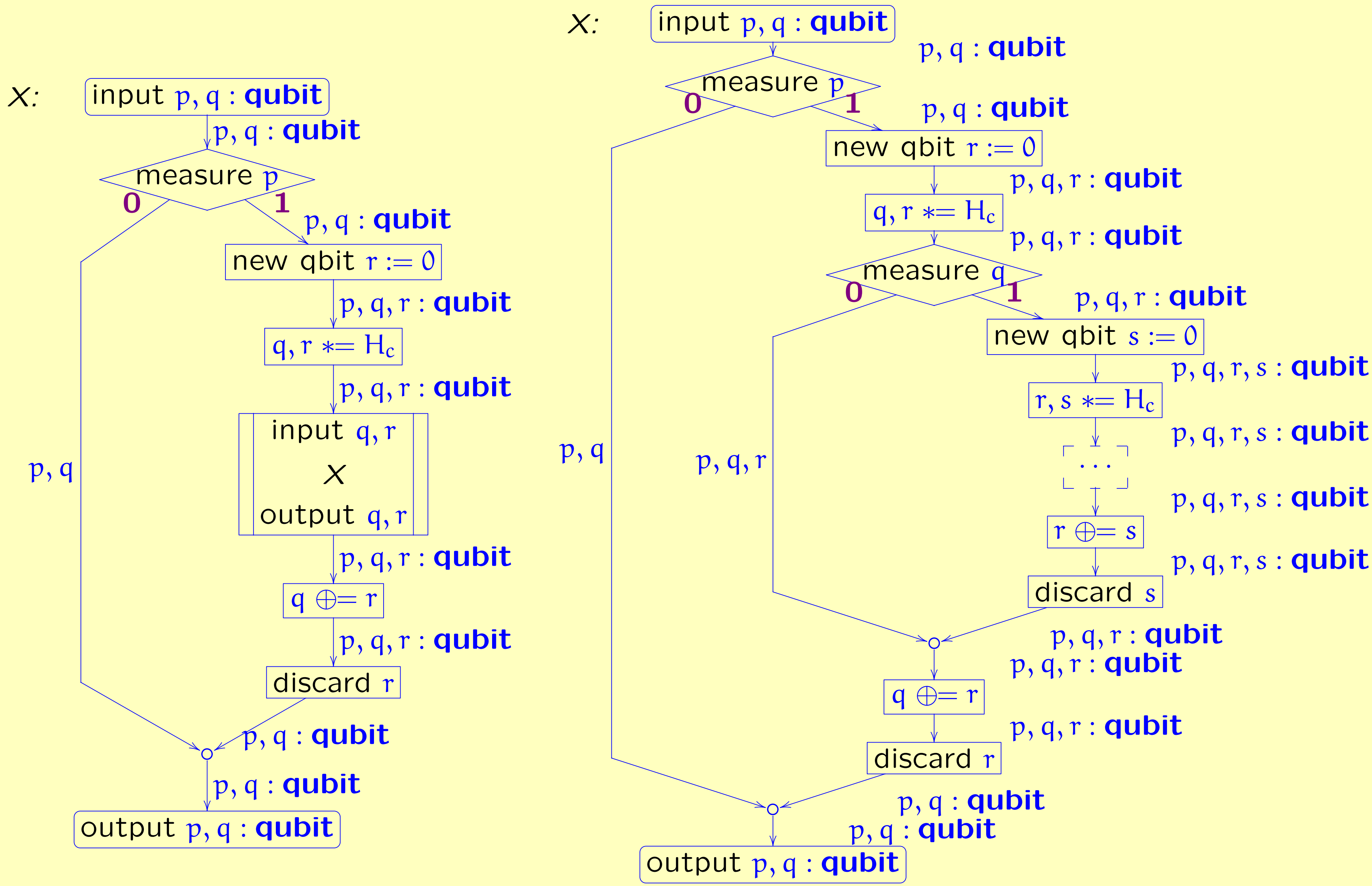
Morphisms: $f : \sigma \to \tau$ is a superoperator

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

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:

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

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

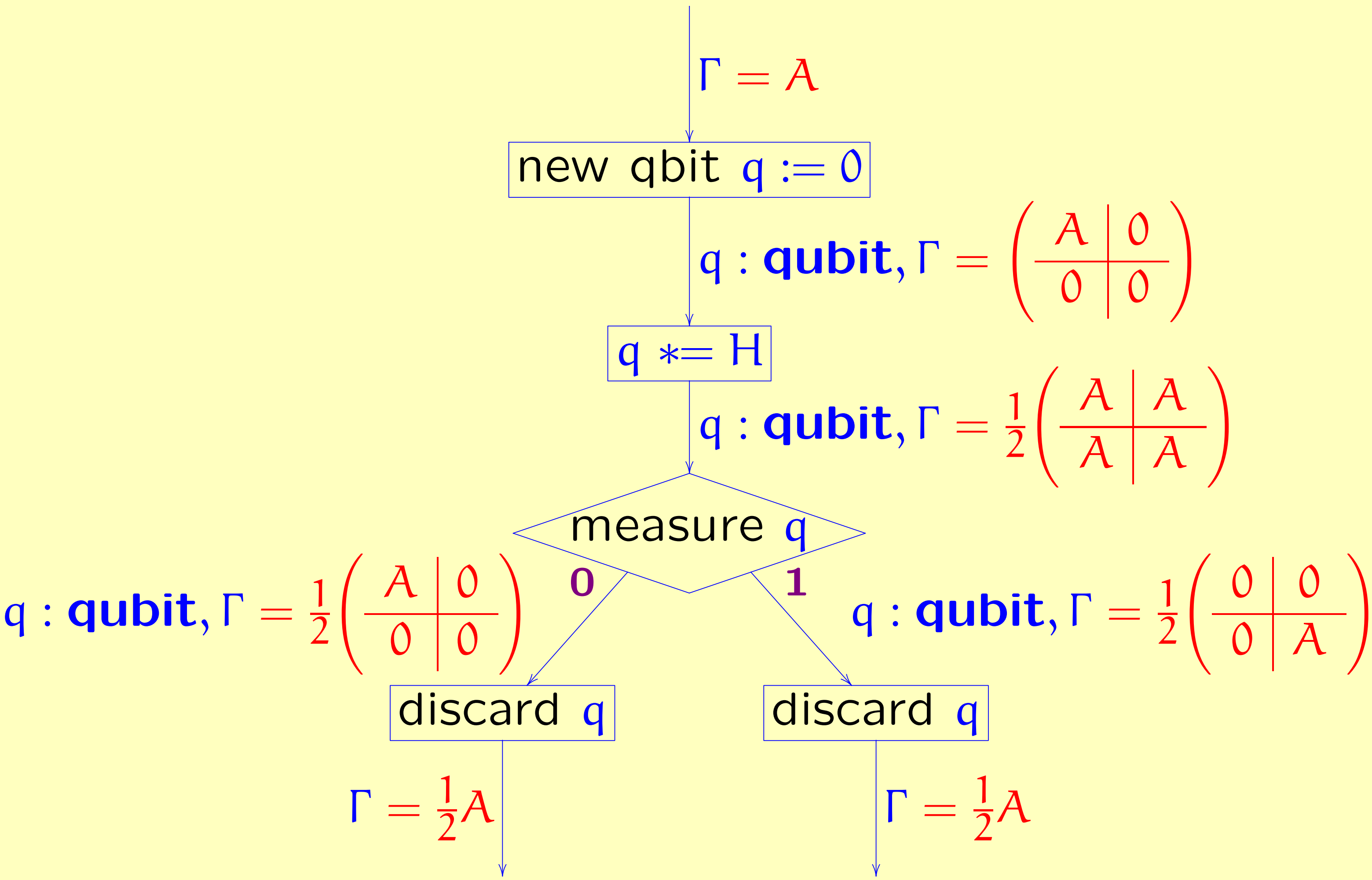
$$F_6(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} + \frac{1}{4}a_{33} + \frac{1}{16}a_{33} & 0 \\ 0 & 0 & 0 & \frac{1}{2}a_{33} + \frac{1}{8}a_{33} \end{pmatrix},$$

and so forth. The limit is

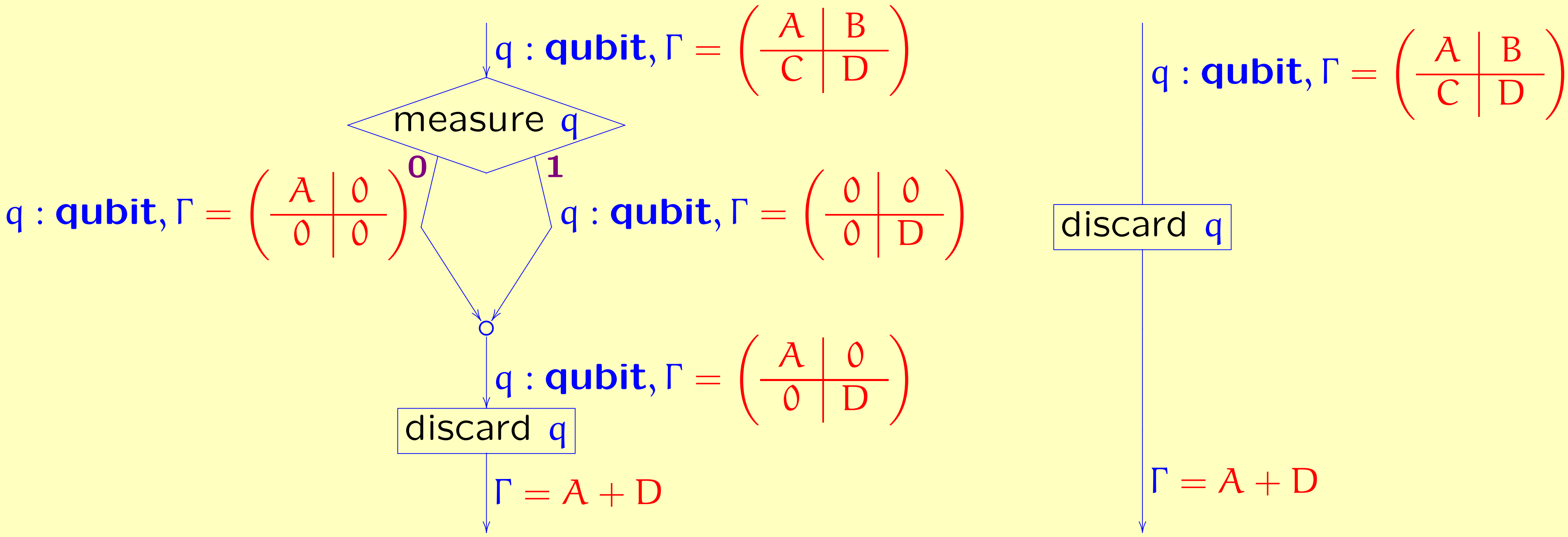
$$G(A) = \begin{pmatrix} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} + \frac{1}{3}a_{33} & 0 \\ 0 & 0 & 0 & \frac{2}{3}a_{33} \end{pmatrix},$$

More examples

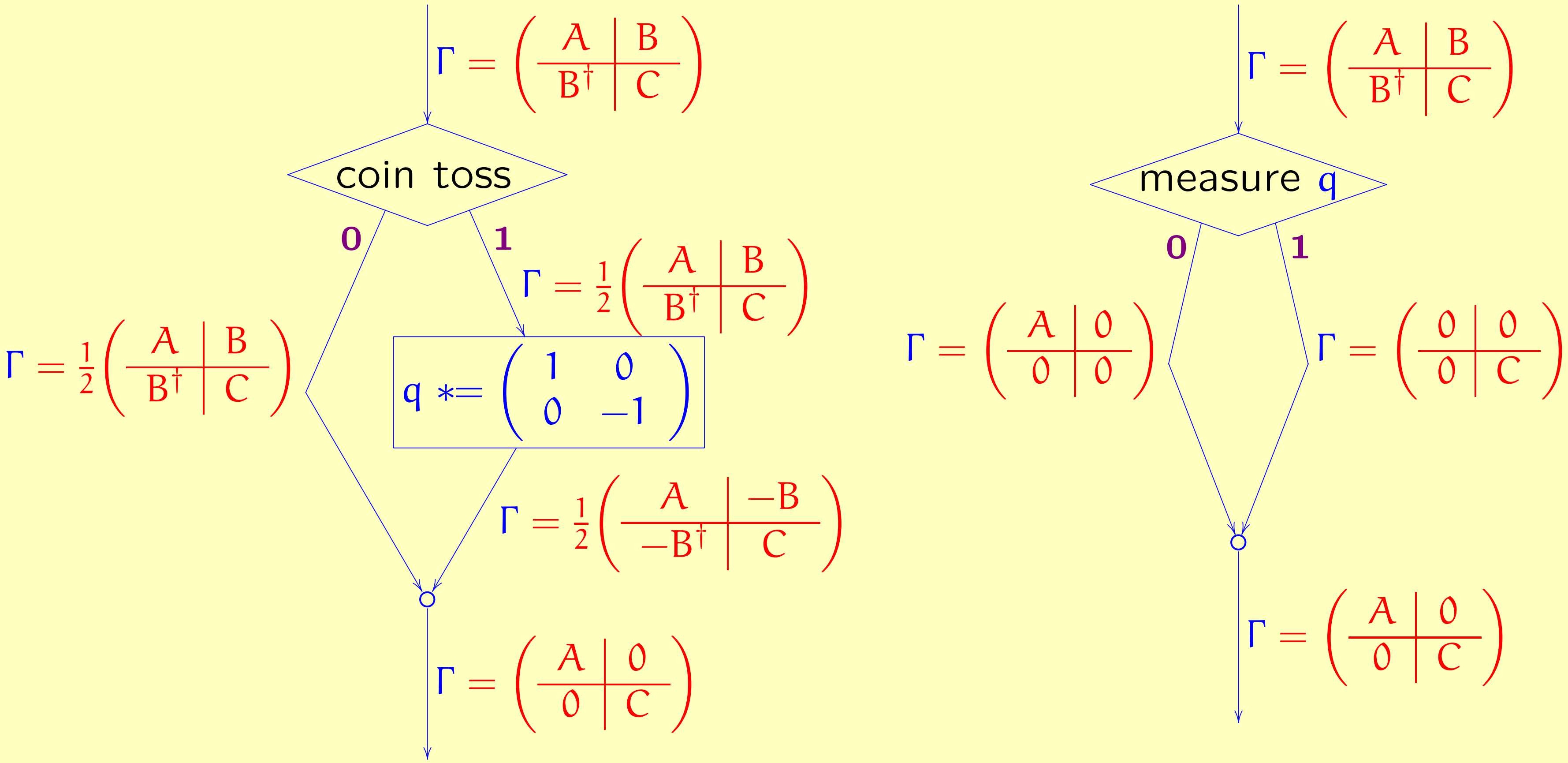
Example: coin toss



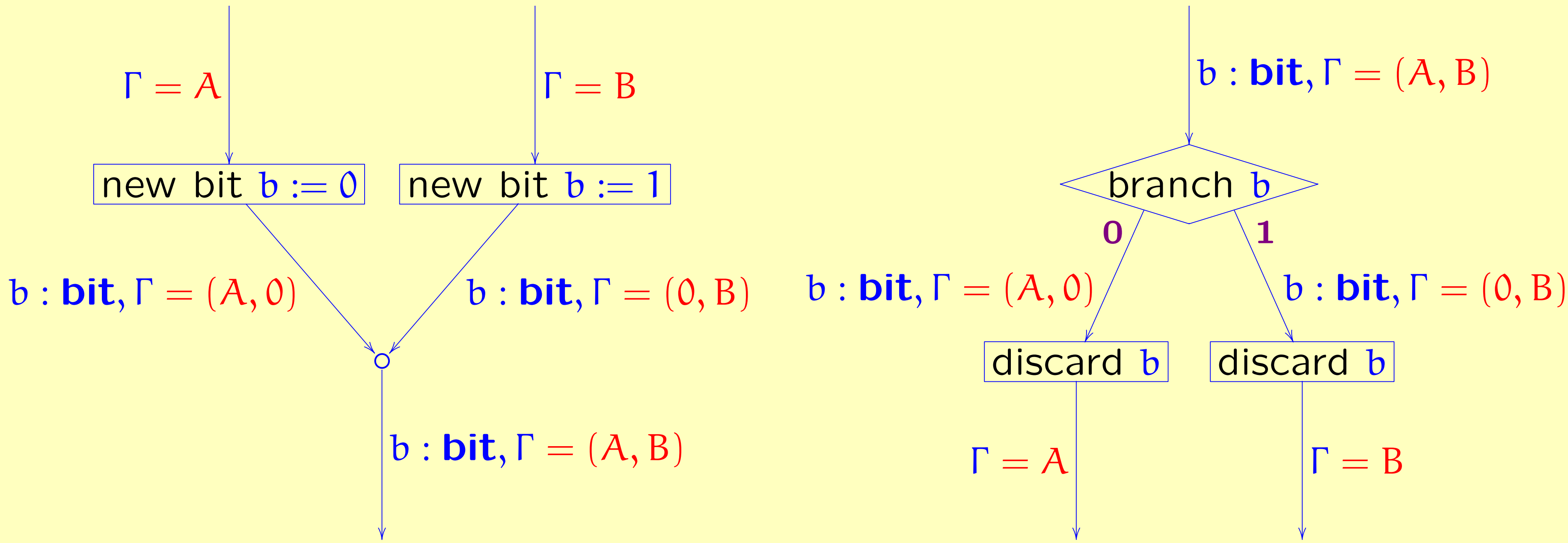
Example: a correct program transformation



Example: “collapse” a qubit without measuring it



Example: equivalence of **bit** = two parallel control edges

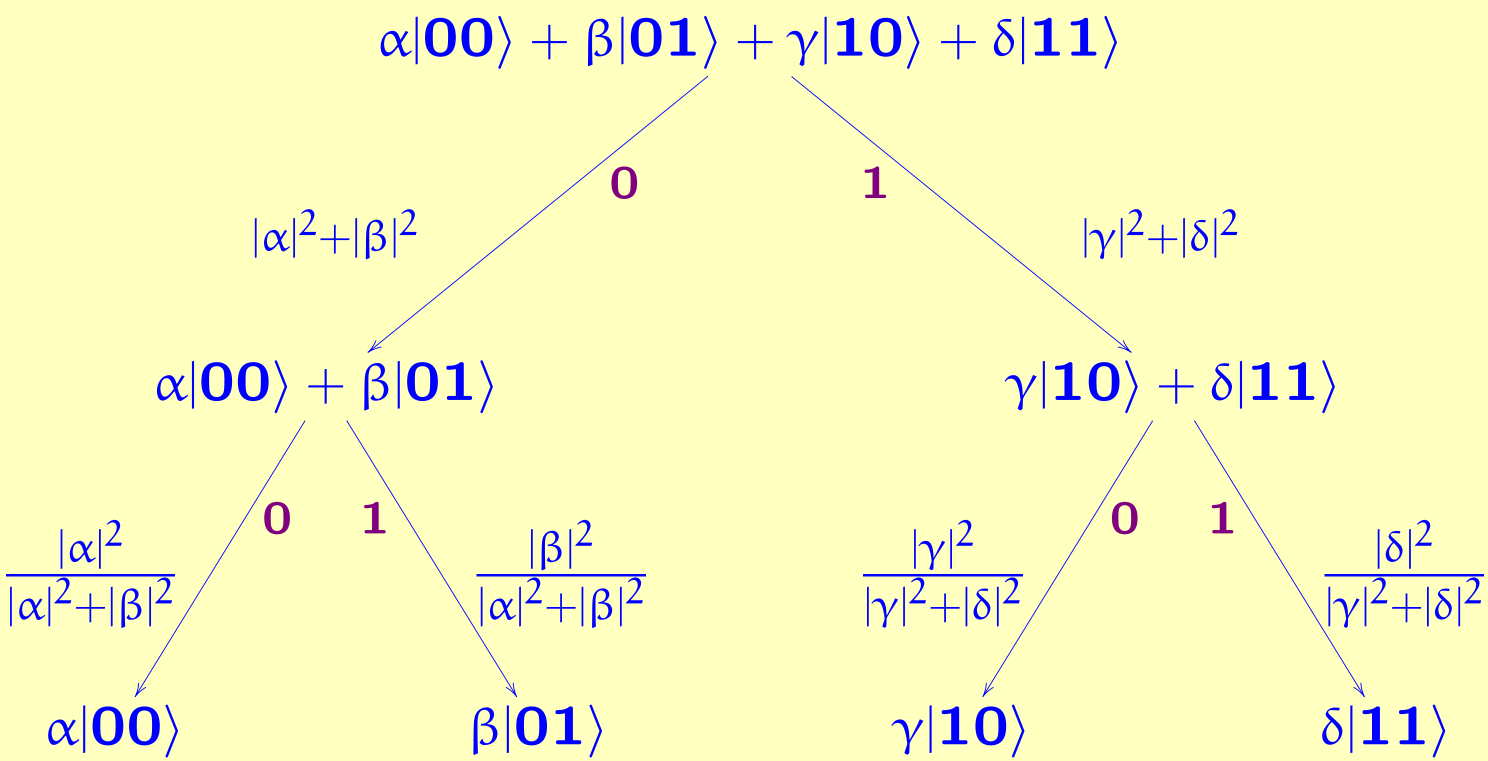


Detour: some experiments and thought experiments on entanglement

Einstein-Podolsky-Rosen “paradox”

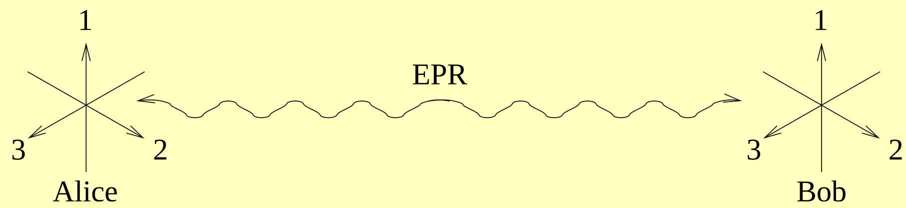
- Performing two measurements on an entangled state yields correlated results.
- This even happens “at a distance”, i.e., if the two qubits are spatially separated.
- Einstein regarded this as a paradox.

Recall: Two Measurements



Bell's experiment, usual description

Thought experiment: send an entangled pair of photons in state $\Phi = \frac{1}{\sqrt{2}}|\mathbf{00}\rangle + \frac{1}{\sqrt{2}}|\mathbf{11}\rangle$ in two different directions.



Alice and Bob will decide independently which *axis* 1, 2, 3 to measure in. The outcome of each measurement is "pass" or "fail". The probabilities that they observe the same value are:

	1	**2**	**3**
1	1	$\frac{1}{4}$	$\frac{1}{4}$
2	$\frac{1}{4}$	1	$\frac{1}{4}$
3	$\frac{1}{4}$	$\frac{1}{4}$	1

Note: measuring in an "axis" means to apply a unitary transformation before measuring.

Bell's experiment, continued

If the photons were carrying "predetermined" specified outcomes for different measurement angles, one would have to have

$$\mathrm{P}_{\mathbf{1},\mathbf{2}}(\text{equal}) + \mathrm{P}_{\mathbf{2},\mathbf{3}}(\text{equal}) + \mathrm{P}_{\mathbf{1},\mathbf{3}}(\text{equal}) \geq 1$$

However,

$$\mathrm{P}_{\mathbf{1},\mathbf{2}}(\text{equal}) + \mathrm{P}_{\mathbf{2},\mathbf{3}}(\text{equal}) + \mathrm{P}_{\mathbf{1},\mathbf{3}}(\text{equal}) = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}$$

So the predictions of quantum theory are *incompatible* with "local hidden variable theories".

Note: however, this does not yield a method for superluminal communication.

Example: PR boxes (Popescu and Rohrlich)

Consider the following problem:

- Alice and Bob are given the task of creating a pair of Boolean functions of one argument,

$$g, h : \textbf{bit} \to \textbf{bit}.$$

  Alice keeps g and Bob keeps h. They go to different rooms.

- Alice is given a random bit x and Bob is given a random bit y (x and y are independent and uniformly distributed).

- The functions g and h are supposed to satisfy:

$$g(x) \oplus h(y) = x \vee y,$$

  where $\oplus$ denotes "exclusive or", and $\vee$ denotes "or".

PR boxes, best probabilistic solution

$$g(0) \oplus h(0) = 0$$
$$g(0) \oplus h(1) = 1$$
$$g(1) \oplus h(0) = 1$$
$$g(1) \oplus h(1) = 1$$

What is Alice and Bob's probability of success?

It is easily seen that with classical (even probabilistic) functions, the best Alice and Bob can hope for is to win 75% of the time.

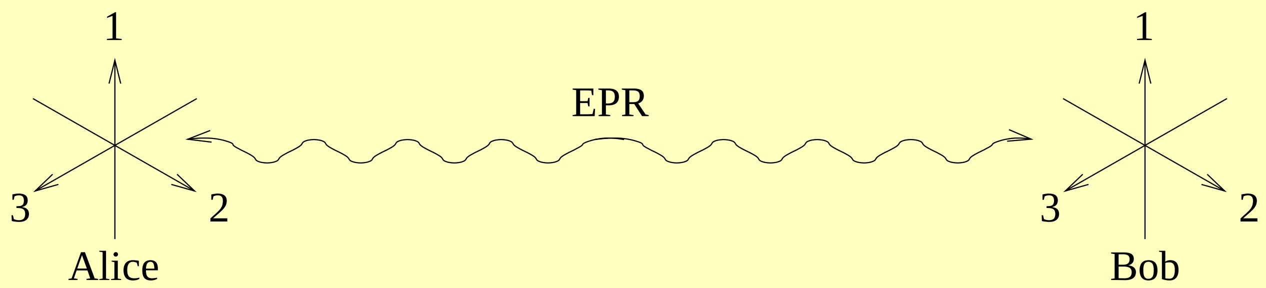
One possible solution is: let g and h be the constant 1 function. Or let g be the constant 0 function and h the identity function.

One cannot do better.

PR boxes, a better quantum solution

$$g(0) \oplus h(0) = 0$$
$$g(0) \oplus h(1) = 1$$
$$g(1) \oplus h(0) = 1$$
$$g(1) \oplus h(1) = 1$$

Using the same setup as in Bell's experiment, Bob and Alice can achieve a success rate of 81.25%. The functions g and h share an entangled EPR state.



If $x = 0$, Alice measures in basis 1, else in basis 2. If $y = 0$, Bob measures in basis 1, else in basis 3.

The probabilities of agreement are:

	1	**2**
1	1	$\frac{1}{4}$
3	$\frac{1}{4}$	$\frac{1}{4}$

In other words,

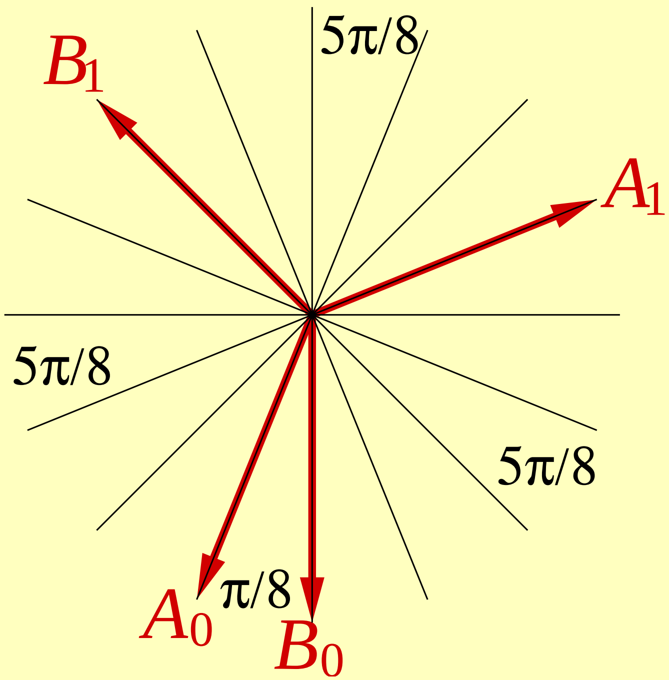
$$P\left(g(0) \oplus h(0) = 0\right) = 1$$
$$P\left(g(0) \oplus h(1) = 1\right) = \frac{3}{4}$$
$$P\left(g(1) \oplus h(0) = 1\right) = \frac{3}{4}$$
$$P\left(g(1) \oplus h(1) = 1\right) = \frac{3}{4}$$

Therefore, the combined chance of success (on uniformly distributed input) is $\frac{1+.75+.75+.75}{4} = 0.8125$.

PR boxes, best quantum solution

Actually, the optimal success rate Alice and Bob can achieve is $\cos^2(\pi/8) \approx 85.36\%$. It is done as follows:

If $x = 0$, Alice measures in basis A_0, else in basis A_1. If $y = 0$, Bob measures in basis B_0, else in basis B_1.



$$P\left(g(0) \oplus h(0) = 0\right) = \cos^2(\tfrac{\pi}{8}) = .8536$$
$$P\left(g(0) \oplus h(1) = 1\right) = \sin^2(\tfrac{5\pi}{8}) = .8536$$
$$P\left(g(1) \oplus h(0) = 1\right) = \sin^2(\tfrac{5\pi}{8}) = .8536$$
$$P\left(g(1) \oplus h(1) = 1\right) = \sin^2(\tfrac{5\pi}{8}) = .8536$$