MAT 5361, TOPICS IN QUANTUM COMPUTATION, WINTER 2004
Answers to Homework 1

Problem 1.1 First, we verify the density matrix formula in case of a pure state. This was already almost done in class: it is a simple matter of re-expressing the probability diagram with matrices:

$$\begin{pmatrix} \alpha\bar\alpha & \alpha\bar\beta & \alpha\bar\gamma & \alpha\bar\delta \\ \beta\bar\alpha & \beta\bar\beta & \beta\bar\gamma & \beta\bar\delta \\ \gamma\bar\alpha & \gamma\bar\beta & \gamma\bar\gamma & \gamma\bar\delta \\ \delta\bar\alpha & \delta\bar\beta & \delta\bar\gamma & \delta\bar\delta \end{pmatrix}$$

$$p_0=\alpha\bar\alpha+\beta\bar\beta \quad \swarrow\ \mathbf{0} \qquad\qquad \mathbf{1}\ \searrow \quad p_1=\gamma\bar\gamma+\delta\bar\delta$$

$$\begin{pmatrix} \alpha\bar\alpha & \alpha\bar\beta & 0 & 0 \\ \beta\bar\alpha & \beta\bar\beta & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad\qquad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \gamma\bar\gamma & \gamma\bar\delta \\ 0 & 0 & \delta\bar\gamma & \delta\bar\delta \end{pmatrix}$$

What needs to be shown now is that this extends to mixed states as expected, i.e., linearly. For simplicity, consider a mixture of two pure states (mixtures of n pure states can be treated similarly): Suppose the initial mixed state is $m = \lambda_0\{v_0\} + \lambda_1\{v_1\}$, where $v_0 = (\alpha,\beta,\gamma,\delta)^T$, $v_1 = (\alpha',\beta',\gamma',\delta')^T$, and $\lambda_0,\lambda_1 \geqslant 0$, $\lambda_0+\lambda_1 \leqslant 1$. There are four possible outcomes of the measurement, namely $w_{00} = (\alpha,\beta,0,0)$, $w_{01} = (0,0,\gamma,\delta)$, $w_{10} = (\alpha',\beta',0,0)$, $w_{11} = (0,0,\gamma',\delta')$.

To deal with conditional probabilities correctly, let us write I_i for the event "the experiment starts in state v_i", M_k for the event "the outcome of the measurement is $k \in \{\mathbf{0},\mathbf{1}\}$", and O_{ik} for "I_i and M_k"; this event corresponds to the outcome w_{ik}.

Recall that $P(A)$ denotes the probability of an event A, and $P(A|B)$ denotes the *conditional probability* of an event A, assuming the event B. Also recall Bayes' law of probabilities:

$$P(A|B) = \frac{P(A \text{ and } B)}{P(B)}$$

Note that $P(I_i) = \lambda_i$ is given, and that $P(M_k|I_i) = |w_{ik}|^2$ follows from out knowledge of the pure case.

We are interested in two questions: (1) what are $P(M_0)$ and $P(M_1)$, and (2) assuming M_k has occurred, then in which mixed state will the system be after the measurement?

The answer to the first question is an easy application of Bayes' law. Because I_0 and I_1 are disjoint events and $M_k \subseteq I_0 \cup I_1$, we have:

$$\begin{aligned} P(M_k) &= P(M_k \text{ and } I_0) + P(M_k \text{ and } I_1) \\ &= P(I_0)P(M_k|I_0) + P(I_1)P(M_k|I_1) \\ &= \lambda_0|w_{0k}|^2 + \lambda_1|w_{1k}|^2. \end{aligned}$$

For the second question, the density matrix of the outgoing state, assuming that $\mathbf{0}$ has been measured, is by definition the following (assuming here the ordinary normalization convention, by which density matrices have trace 1):

$$D_0 = \sum_{ik} P(O_{ik}|M_0)\,\frac{1}{|w_{ik}|^2}\,w_{ik}w_{ik}^*.$$

We can calculate:

$$P(O_{i0}|M_0) = P(I_i \text{ and } M_0|M_0) = \frac{P(I_i \text{ and } M_0)}{P(M_0)} = \frac{P(I_i)P(M_0|I_i)}{P(M_0)} = \frac{\lambda_i|w_{i0}|^2}{P(M_0)}$$

and

$$P((O_{i1}|M_0) = P(I_i \text{ and } M_1|M_0) = 0.$$

It follows that

$$D_0 = \frac{1}{P(M_0)}\sum_i \lambda_i w_{i0}w_{i0}^*.$$

By our advanced normalization convention, we multiply this probability by $P(M_0)$, so that the re-normalized density matrix in the measurement branch $\mathbf{0}$ is:

$$D_0' = \sum_i \lambda_i w_{i0}w_{i0}^*.$$

Finally, we note that if

$$\sum_i \lambda_i v_i v_i^* = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$$

was the density matrix of the initial mixed state of the system, then D_0' is just

$$D_0' = \sum_i \lambda_i w_{i0}w_{i0}^* = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right),$$

as was to be shown. The calculation for $k = \mathbf{1}$ is analogous. Note: in the above calculations, we have ignored the possibility of zero denominators. A careful analysis shows that zero denominators only occur where the corresponding numerator is also zero, and we can drop such terms without affecting the validity of the overall argument.

Problem 1.2 (a) In finite dimension, all norms are equivalent. More specifically, when $A \in \mathbb{C}^{n\times n}$ and $v \in \mathbb{C}^n$, we have

$$|Av|^2 = \sum_i(\sum_j a_{ij}v_j)^2 \leqslant \sum_i(\sum_j a_{ij}^2)(\sum_j v_j^2) = \|A\|_2|v|,$$

and thus $\|A\| \leqslant \|A\|_2$. It follows that if the theorem gives $\|B-\lambda B'\|_2 \leqslant \epsilon$, then $\|B-\lambda B'\| \leqslant \epsilon$ holds as well.

(b) For the first part, note that $|ABv| \leqslant \|A\||Bv| \leqslant \|A\|\|B\||v|$, by definition of $\|A\|$ and $\|B\|$. Thus, $|v| \leqslant 1$ implies that $|ABv| \leqslant \|A\|\|B\|$. Since $\|AB\|$ is the supremum of all such $|ABv|$, we have $\|AB\| \leqslant \|A\|\|B\|$.

For the second part, first note that if $A \in \mathbb{C}^{n' \times n}$ and $B \in \mathbb{C}^{m' \times m}$, and if $w \in \mathbb{C}^n$ and $u \in \mathbb{C}^m$, then $(A \otimes B)(w \otimes u) = Aw \otimes Bu$, and $|w \otimes u| = |w||u|$. Now, assume $|w| \leqslant 1$ and $|u| \leqslant 1$. Then $|Aw||Bu| = |Aw \otimes Bu| = |(A \otimes B)(w \otimes u)| \leqslant \|A \otimes B\||w \otimes u| = \|A \otimes B\||w||u| \leqslant \|A \otimes B\|$. By taking the supremum of the left-hand-side, we get $\|A\|\|B\| \leqslant \|A \otimes B\|$. Conversely, assume $v \in \mathbb{C}^{nm}$ with $|v| \leqslant 1$. Then we can write $v = \sum_i w_i \otimes u_i$ in such a way that $|v| = \sum_i |w_i||u_i|$ — indeed, this is possible by writing $v = (u_1, \ldots, u_n)$, and letting $w_i = e_i$. Then $(A \otimes B)v = (A \otimes B)(\sum_i w_i \otimes u_i) = \sum_i (A \otimes B)(w_i \otimes u_i) = \sum_i (Aw_i \otimes Bu_i)$, thus $|(A \otimes B)v| \leqslant \sum_i |Aw_i \otimes Bu_i| \leqslant \sum_i \|A\||w_i|\|B\||u_i| = \|A\|\|B\| \sum_i |w_i||u_i| = \|A\|\|B\||v|$. It follows that $\|A \otimes B\| \leqslant \|A\|\|B\|$.

(c) First, suppose that $\|B - \lambda B'\| \leqslant \epsilon$, and let $A = \mathrm{id}_n \otimes B$ and $A' = \mathrm{id}_n \otimes B'$. Then $\|A - \lambda A'\| = \|\mathrm{id}_n \otimes (B - \lambda B')\| = \|\mathrm{id}_n\|\|B - \lambda B'\| \leqslant 1\epsilon = \epsilon$. Thus, if a gate is approximated within a certain error, then the error does not change by adding additional perfect parallel wires.

Second, suppose B_1, B_2, B_1', B_2' are unitary gates and λ_1, λ_2 are unit scalars such that $\|B_1 - \lambda_1 B_1'\| \leqslant \epsilon_1$ and $\|B_2 - \lambda_2 B_2'\| \leqslant \epsilon_2$, and let $B = B_1 B_2$, $B' = B_1' B_2'$, and $\lambda = \lambda_1 \lambda_2$. Then

$$\begin{array}{rcl}
\|B - \lambda B'\| & = & \|B_1 B_2 - \lambda_1 \lambda_2 B_1' B_2'\| \\
& = & \|B_1 B_2 - \lambda_1 B_1' B_2 + \lambda_1 B_1' B_2 - \lambda_1 \lambda_2 B_1' B_2'\| \\
& \leqslant & \|B_1 B_2 - \lambda_1 B_1' B_2\| + \|\lambda_1 B_1' B_2 - \lambda_1 \lambda_2 B_1' B_2'\| \\
& = & \|B_1 - \lambda_1 B_1'\|\|B_2\| + \|\lambda_1 B_1'\|\|B_2 - \lambda_2 B_2'\| \\
& \leqslant & \epsilon_1 \|B_2\| + \epsilon_2 \|\lambda_1 B_1'\|
\end{array}$$

Since B_2 and B_1' are unitary, we have $\|B_2\| = \|\lambda_1 B_1'\| = 1$, and thus $\|B - \lambda B'\| \leqslant \epsilon_1 + \epsilon_2$. This shows that error propagation is additive. The case for n gates now follows by an easy induction.

(d) By part (c), we know that to approximate an n-gate circuit within ϵ, we must approximate each gate within ϵ/n. By the Kitaev-Solovay Theorem, each gate can be approximated within error ϵ/n by using at most $c \log^d(n/\epsilon)$ basic gates. Thus, the total number of gates required is at most $nc \log^d(n/\epsilon)$. As a function of n, this behaves like $n \log n$, which is certainly bounded by a polynomial in n (in fact, much less than $O(n^2)$). So the approximation given by the Kitaev-Solovay Theorem scales well to large quantum circuits.

Problem 1.3 (a) $A \in D_n$ is maximal iff $\mathrm{tr}\, A = 1$. Proof: suppose $\mathrm{tr}\, A = 1$ and $A \sqsubseteq B$. Then $B - A$ is positive, hence $\mathrm{tr}(B - A) \geqslant 0$. But also $\mathrm{tr}(B - A) = \mathrm{tr}\, B - \mathrm{tr}\, A \leqslant 1 - 1 = 0$, hence $\mathrm{tr}(B - A) = 0$; since $B - A$ is positive, it follows that $B - A = 0$, hence $A = B$, so A was maximal. Conversely, suppose $\mathrm{tr}\, A < 1$, and let $B = A + (1 - \mathrm{tr}\, A)I$, where I is the identity matrix. Then clearly $\mathrm{tr}\, B \in D_n$ and $A \sqsubseteq B$, but $A \neq B$, hence A is not maximal.

(b) This is tricky. We first consider the case where $n = 1$. In this case, a density matrix is just a scalar $0 \leqslant a \leqslant 1$. On scalars, define the relation $a <_0 b$ iff ($a = 0$ or $a < b$). Then we have $a \ll b$ iff $a <_0 b$. Proof: suppose $a \ll b$ and $a \neq 0$. Consider $a_i = (1 - \frac{1}{i})b$, then $b \leqslant \bigvee^{\uparrow}_i a_i$, therefore there is some i with $a \leqslant a_i$, therefore $a < b$. Conversely, suppose that $a <_0 b$ and $b \leqslant \bigvee^{\uparrow}_i a_i$. If $a = 0$, then $a \leqslant a_i$ trivially.

Otherwise $a < b$, and therefore $a < \bigvee^{\uparrow}_i a_i$. by leastness of the upper bound, it follows that $a < a_i$ for some a_i.

Now we can do the case for general n. For $A, B \in D_n$, we have $A \ll B$ iff for all $v \in \mathbb{C}^n$, $v^* A v <_0 v^* B v$. [Equivalently, all the eigenvalues of $B - A$ are non-negative, and any eigenvector of eigenvalue 0 of $B - A$ is already an eigenvector of eigenvalue 0 of A.]

For example:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \ll \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}, \qquad \begin{pmatrix} 0.2 & 0 \\ 0 & 0 \end{pmatrix} \ll \begin{pmatrix} 0.5 & 0 \\ 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0.2 & 0 \\ 0 & 0.3 \end{pmatrix} \ll \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}, \quad \begin{pmatrix} 0.2 & 0 \\ 0 & 0.5 \end{pmatrix} \not\ll \begin{pmatrix} 0.5 & 0 \\ 0 & 0.5 \end{pmatrix}.$$

Proof idea: The proof is mostly pointwise, but in the right-to-left direction, we need to use compactness to show that i can be chosen uniformly for all v.

Proof: "$\Rightarrow$": Suppose $A \ll B$, and take some $v \in \mathbb{C}^n$. If $v^* A v = 0$, then there is nothing to show. Else, we have $v^* A v > 0$. Let $A_i = (1 - \frac{1}{i})B$, so that $B = \bigvee^{\uparrow}_i A_i$. Therefore, $A \sqsubseteq A_i$ for some i. It follows that $v^* A v \leqslant v^* A_i v$, therefore $v^* A_i v \neq 0$. Then $v^* A_i v = (1 - \frac{1}{i}) v^* B v < v^* B v$, so finally, $v^* A v < v^* B v$, as desired.

"$\Leftarrow$": For any positive matrix A, define $\mathrm{null}(A) = \{v \in \mathbb{C}^n \mid Av = 0\}$ and $\mathrm{ran}(A) = \{Av \mid v \in \mathbb{C}^n\}$. Note that $\mathrm{null}(A)$ and $\mathrm{ran}(A)$ are orthogonal complements of each other; also $v \in \mathrm{null}(A)$ iff $v^* A v = 0$; these facts follow from diagonalization. Also note that $A \sqsubseteq B$ implies $\mathrm{null}(B) \subseteq \mathrm{null}(A)$.

Now assume that for all v, $v^* A v <_0 v^* B v$. Then, by definition, $A \sqsubseteq B$. To show that $A \ll B$, take a directed sequence (A_i) such that $B \sqsubseteq \bigvee^{\uparrow}_i A_i$. Let $B' = \bigvee^{\uparrow}_i A_i$, and let $S = \{v \in \mathrm{ran}(B') \mid |v| = 1\}$. As the unit ball of the finite dimensional space $\mathrm{ran}(B')$, the set S is thus a compact set.

Now for all i, let $S_i = \{v \in S \mid v^* A_i v \leqslant v^* A v\}$. As a closed subset of the compact set S, each S_i is compact. Moreover, since the quantity $v^* A_i v$ increases with i, we have $S_i \supseteq S_j$ for $i \leqslant j$, so $(S_i)_i$ is a decreasing sequence of compact sets. We claim that the intersection $\Cap_i S_i$ is empty: for take some $v \in S$, then $v^* A v <_0 v^* B v$ by assumption, therefore $v^* A v <_0 v^* B' v$, but $v^* B' v \neq 0$, hence $v^* A v < v^* B' v$. But as $i \to \infty$, we have $v^* A_i v \to v^* B' v$, therefore there exists some i with $v^* A_i v > v^* A v$, hence $v \notin S_i$. So $(S_i)_i$ is a decreasing sequence of compact sets with empty intersection. It follows that some S_i is already empty. Therefore, there exists some i such that for all $v \in S$, $v^* A_i v > v^* A v$. We now claim that $A \sqsubseteq A_i$. We already know that $v^* A v \leqslant v^* A_i v$ for all $v \in S$, and therefore for all $v \in \mathrm{ran}(B')$. Now take any $v \in \mathbb{C}^n$, then v can be written $v = u + w$, where $u \in \mathrm{null}(B')$, $w \in \mathrm{ran}(B')$. Since $A_i \sqsubseteq B'$, we have $u \in \mathrm{null}(A_i)$; also, since $A \sqsubseteq B \sqsubseteq B'$, we have $u \in \mathrm{null}(A)$. Therefore $v^* A v = (u + w)^* A (u + w) = w^* A w \leqslant w^* A_i w = (u + w)^* A_i (u + w) = v^* A_i v$. Since v was arbitrary, we have $A \sqsubseteq A_i$, as desired, and thus $A \ll B$.

Problem 1.4

(a) $F(A, B, C, D) = (A + C, B, D, 0)$.

(b)

$$F\left(\begin{array}{cc} A & B \\ \hline C & D \end{array}\right) = \left(\begin{array}{cc|cc} (a_{00}+x) & -x & (b_{00}+y) & -y \\ -x & x & -y & y \\ \hline (c_{00}+z) & -z & (d_{00}+w) & -w \\ -z & z & -w & w \end{array}\right),$$

where $A = (a_{ij})_{ij}$, $B = (b_{ij})_{ij}$, etc, and $x = a_{11} + b_{11} + c_{11} + d_{11}$, $y = a_{11} - b_{11} + c_{11} - d_{11}$, $z = a_{11} + b_{11} - c_{11} - d_{11}$, $w = a_{11} - b_{11} - c_{11} + d_{11}$.

(c) $F(A, B, C, D) = (0, B + D, A + C, 0)$.

(d) $F(A) = (\frac{1}{2}A, \frac{1}{2}A)$.

(e) $F\left(\begin{array}{cc} a & b \\ c & d \end{array}\right) = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right)$.

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

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

(h) $F\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) = (\left(\begin{array}{c|c} A & 0 \\ \hline 0 & 0 \end{array}\right), NDN)$.

(i) As in class, we write $\Phi(Y)$ for the superoperator obtained from this flow chart by "plugging" the recursive call with the superoperator Y. We let $F_0 = 0$ and $F_{i+1} = \Phi(F_i)$. Let $A = (a_{ij})_{ij}$. We calculate:

$$F_1(A) = \left(\begin{array}{cccc} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$F_2(A) = \left(\begin{array}{cccc} a_{00} & a_{01} & 0 & 0 \\ a_{10} & a_{11} & 0 & 0 \\ 0 & 0 & a_{22} & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$F_3(A) = F_2(A)$.

Thus, we reach a fixpoint where $F(A) = \bigvee^{\uparrow}_i F_i(A) = F_2(A)$. This is the denotation of the recursively defined flowchart X.

Problem 1.5 (a) This is a superoperator. A Kraus representation is $F(A) = UAU^*$, where $U = \frac{1}{\sqrt{2}}(\,1\ 1\,)$; note that $U^*U = 1$. A flow chart is: (input p; $p \mathrel{*}= H$; if (measure p)=0 then discard p else diverge).

(b) This problem is best analyzed in terms of its characteristic matrix, which we can easily write down:

$$\chi_F = \left(\begin{array}{cccc} \frac{1}{3} & 0 & \frac{1}{6} & \frac{1}{6} \\ 0 & \frac{1}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{3} & 0 \\ \frac{1}{6} & \frac{1}{6} & 0 & \frac{1}{3} \end{array}\right)$$

This matrix is seen to be writable as a sum of rank 1 positive matrices:

$$\left(\begin{array}{cccc} \frac{1}{6} & 0 & \frac{1}{6} & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{6} & 0 & \frac{1}{6} & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cccc} \frac{1}{6} & 0 & 0 & \frac{1}{6} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{6} & 0 & 0 & \frac{1}{6} \end{array}\right) + \left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{6} & \frac{1}{6} & 0 \\ 0 & \frac{1}{6} & \frac{1}{6} & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{6} & 0 & \frac{1}{6} \\ 0 & 0 & 0 & 0 \\ 0 & \frac{1}{6} & 0 & \frac{1}{6} \end{array}\right),$$

and thus χ_F is positive, which proves that F is completely positive. Moreover, the trace characteristic matrix is

$$\chi_F^{\mathrm{tr}} = \left(\begin{array}{cc} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{array}\right),$$

which is $\sqsubseteq I_2$. Therefore, F is a superoperator. A Kraus representation can be read off from the above decomposition of χ_F, namely: $F(A) = \sum_{i=1}^{4} U_i A U_i^*$, where

$$U_1 = \frac{1}{\sqrt{6}}\left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right), U_2 = \frac{1}{\sqrt{6}}\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), U_3 = \frac{1}{\sqrt{6}}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), U_4 = \frac{1}{\sqrt{6}}\left(\begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}\right).$$

Note that $\sum_i U_i U_i^* = \left(\begin{array}{cc} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{array}\right) \sqsubseteq I_2$. A flow chart can be obtained from the Kraus representation, as in the proof of Theorem 6.12 in [Selinger], but this requires implementing a 16×16 unitary matrix. Instead of following the general procedure, it is easier to guess a flow chart directly from the decomposition of χ_F. (input p; with probability $\frac{2}{3}$ do skip else (if (measure p)=0 then skip else diverge); if (coin) then $p \oplus= 1$ else skip).

(c) This is not positive, e.g. $F\left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right) = (1, -1)$.

(d) This is a superoperator. A Kraus representation is $F(A) = \sum_{i=1}^{3} U_i A U_i^*$, where

$$U_1 = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), U_2 = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), U_3 = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Note that $\sum_i U_i^* U_i = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. A possible flow chart is (input p; if (coin) then skip else if (measure p) then skip else skip).

(e) This is a superoperator. A Kraus representation is:

$$F(A, B) = (U_1 A U_1^*, U_2 A U_2^* + U_3 A U_3^* + V B V^*, U_4 A U_4^*),$$

where

$$U_1 = \frac{1}{\sqrt{2}}(\,1\ 0\,), U_2 = \frac{1}{2}\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), U_3 = \frac{1}{2}\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right), U_4 = (\,0\ 1\,), V = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -i \end{smallmatrix}\right).$$

Note that $\sum_i U_i^* U_i = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $V^* V = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. A flow chart is given by (input b, q; if ($b = 0$) then (if (measure q)$=0$ then (if (coin) then (discard q; exit 1) else $q \mathrel{*}= H$; exit 2) else (discard q; exit 3)) else $q \mathrel{*}= \left(\begin{smallmatrix} 1 & 0 \\ 0 & -i \end{smallmatrix}\right)$; exit 2).

Problem 1.6 Suppose $F : V_\sigma \to V'_\sigma$ and $G : V_\tau \to V'_\tau$ are superoperators. To prove that $F \oplus G : V_{\sigma\oplus\sigma'} \to V_{\tau\oplus\tau'}$ is a superoperator, note that for $A \in D_\sigma$ and $B \in D_\tau$, we have $(F \oplus G)(A, B) = (FA, GB)$, which is clearly positive and satisfies $\mathrm{tr}(FA, GB) = \mathrm{tr}\, FA + \mathrm{tr}\, GB \leqslant \mathrm{tr}\, A + \mathrm{tr}\, B$, by assumption on F and G. Moreover, for $A \in D_{\rho\otimes\sigma}$ and $B \in D_{\rho\otimes\tau}$, we have $\mathrm{id}_\rho \otimes (F \oplus G)(A, B) = ((\mathrm{id}_\rho \otimes F)(A), (\mathrm{id}_\rho \otimes G)(B))$, which is also still positive.

To show that $F \otimes G : V_{\sigma\otimes\sigma'} \to V_{\tau\otimes\tau'}$ is a superoperator, note that $F \otimes G = (\mathrm{id}_{\sigma'} \otimes G) \circ (F \otimes \mathrm{id}_\tau)$. The two component maps are completely positive by definition, and they clearly satisfy the trace condition, because e.g. $\mathrm{tr}_{\sigma'\otimes\tau'} \circ (\mathrm{id}_{\sigma'} \otimes G)(A) = (\mathrm{tr}_{\sigma'} \otimes (\mathrm{tr}_{\tau'} \circ G))(A) \leqslant (\mathrm{tr}_{\sigma'} \otimes \mathrm{tr}_\tau)(A) = \mathrm{tr}_{\sigma'\otimes\tau}\, A$.

Problem 1.7 (a) We have directly from the definition: $F \sqsubseteq G$ iff $\mathrm{id}_\tau \otimes (G - F)(A)$ is positive for all τ and A, iff $G - F$ is completely positive. This is the case iff χ_{G-F} is a positive matrix, by a theorem from class. But $\chi_{G-F} = \chi_G - \chi_F$, so this holds iff $\chi_G - \chi_F$ is positive, iff $\chi_F \sqsubseteq \chi_G$.

(b) Let $F : V_\sigma \to V_1$. Clearly, if F is completely positive, then it is positive by definition. Conversely, assume F is positive. Let $\chi_F = B = (b_{ij})$, then B is hermitian. By definition of χ_F, we have $F(E_{ij}) = b_{ij}$, where E_{ij} is the ij-unit matrix. By linearity, $F(A) = \mathrm{tr}(BA^T)$ for all A. Now suppose B were not positive, then B has some eigenvector v for a negative eigenvalue λ. Then let $A^T = vv^*$, and we have $F(A) = \mathrm{tr}(Bvv^*) = \mathrm{tr}(v^*Bv) < 0$, contradiction the positivity of F. Thus, $B = \chi_F$ is positive, hence F is completely positive by the characterization theorem from class.

(c) Let $F, G : V_\sigma \to V_1$, then $F \sqsubseteq G$ iff $G - F$ is completely positive iff $G - F$ is positive iff for all positive A, $F(A) \sqsubseteq G(A)$.