MASSACHUSETTS INSTITUE OF TECHNOLOGY

Media Laboratory

MAS.961 Quantum Information Science September 06, 2001

Entrance Quiz: Solutions

1. (a) $(1+i)/\sqrt{2}$

   (b) $(1-i)/\sqrt{2}$

   (c) -1

2. $$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \equiv |+\rangle$$

   has eigenvalue 1 and

   $$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \equiv |-\rangle$$

   has eigenvalue -1. The $\{|+\rangle, |-\rangle\}$ basis turns up often. For example, the hadamard matrix H converts back and forth between the $\{|0\rangle, |1\rangle\}$ basis and the $\{|+\rangle, |-\rangle\}$ basis.

3. (a) $2iZ$

   (b) $2iZ \otimes Z$

   To avoid the factor of 2 it is common to define $S_x = X/2$ and so forth.

4. $$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

5. $$\left| \langle 1| \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \right|^2 = 1/2$$

6. Let $M_0 = |0\rangle\langle 0| \otimes I$ and $M_1 = |1\rangle\langle 1| \otimes I$. The probability of measuring zero and one respectively is $|\langle\psi|M_0|\psi\rangle|^2$ and $|\langle\psi|M_1|\psi\rangle|^2$, i.e. 9/25 and 16/25. Obtaining a zero projects the state onto $M_0|\psi\rangle$ and obtaining a one projects the state onto $M_1|\psi\rangle$, i.e. $|00\rangle$ and $|11\rangle$, respectively, after normalizing. Thus, the desired probability is 9/25.

7. $\sin\theta$ because $\langle 0|X|0\rangle = 0$.

8. $$U = e^{\frac{-iHt}{\hbar}}$$

   is a valid solution and is unique, since the equation is first-order in time.

9. $$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} \bar{a} & \bar{b} \end{bmatrix} = \begin{bmatrix} a\bar{a} & \bar{a}b \\ a\bar{b} & b\bar{b} \end{bmatrix}$$

10.

$$\rho_A = \mathrm{tr}_B \rho = \frac{1}{2}\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix} \qquad \text{and} \qquad \rho_B = \mathrm{tr}_A \rho = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

11.

$$\begin{bmatrix} a_1 a_2 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{bmatrix}$$

12.

$$\begin{bmatrix} & & & -i \\ & & i & \\ & -i & & \\ i & & & \end{bmatrix}$$

13. (a) Note that $X_j|\psi\rangle = |\psi\rangle$ for $j = 1, 2, 3$. Thus $X_1 X_2 X_3|\psi\rangle = |\psi\rangle$ and $\langle\psi|X_1 X_2 X_3|\psi\rangle = 1$.
    (b) $\langle\psi|X_1 Y_2 Y_3|\psi\rangle = \langle\psi|i^2 Z_2 Z_3|\psi\rangle = -1$.
    (c) $X_1 X_2 Y_3|\psi\rangle = Z_3|\psi\rangle = (|000\rangle - |111\rangle)/\sqrt{2}$ which is orthogonal to $|\psi\rangle$. Thus $\langle\psi|X_1 X_2 Y_3|\psi\rangle = 0$.

14.

$$|\psi'\rangle = e^{i\alpha/2}\left[\cos\frac{\theta}{2}|0\rangle + e^{i(\phi-\alpha)}\sin\frac{\theta}{2}\right]$$

15. One possible choice is

$$|\psi\rangle = \frac{\sqrt{3}}{2}|00\rangle + \frac{1}{2}|11\rangle$$

16. Three qubits each start at $|0\rangle$ and you apply a Hadamard to each one to obtain

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

which gives the desired answer when expanded out.

17. (a) $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
    (b) $|11\rangle$
    (c) $|01\rangle$
    (d) $|+\rangle|+\rangle|\psi\rangle$

18. Let $\vec{\sigma}$ denote $\sigma_x\hat{x} + \sigma_y\hat{y} + \sigma_z\hat{z}$, so the expression we are trying to simplify is $e^{i\vec{n}\cdot\vec{\sigma}}$. One can verify that $(\vec{n}\cdot\vec{\sigma})^2 = n^2 I$ by writing it out. A more elegant proof of that claim is the following: for $U \in SU(2)$, let $R_U \in SO(3)$ denote the effects of conjugating elements of the form $\vec{x}\cdot\vec{\sigma}$ by U. So $U(\vec{n}\cdot\vec{\sigma})U^\dagger = (R_U\vec{n})\cdot\vec{\sigma}$. Since $|\vec{n}| = n$, we can choose U so that $(R_U\vec{n})\cdot\vec{\sigma} = n\sigma_z$, which clearly squares to $n^2 I$. So

$$n^2 I = (U(\vec{n}\cdot\vec{\sigma})U^\dagger)^2 = U(\vec{n}\cdot\vec{\sigma})^2 U^\dagger$$

and conjugating both sides by U gives the desired result. Now we expand

$$e^{i\vec{n}\cdot\vec{\sigma}} = \sum_k \frac{(i\vec{n}\cdot\vec{\sigma})^k}{k!} = 1 + i\vec{n}\cdot\vec{\sigma} - \frac{n^2}{2} - \frac{n^2}{3!}i\vec{n}\cdot\vec{\sigma} + \frac{n^4}{4!} + \cdots$$

and collect odd and even powers of k to obtain

$$e^{i\vec{n}\cdot\vec{\sigma}} = I\cos n + i\hat{n}\cdot\vec{\sigma}\sin n$$

Don't panic if you didn't follow the $SO(3)$ stuff: it's worth knowing, but not immediately necessary.

19. Using

$$H = -\sum_i p_i \log_2 p_i$$

and a little math, we see that a 50-50 chance of emitting 0 or 1 will achieve the maximal entropy, which is one bit. To avoid the math, we can note that entropy is concave, and left invariant by exchanging 0 and 1; thus any maximum must be achieved by a uniform distribution.

20. Shannon's theorem says that the channel capacity C is the supremum of the mutual information

$$I(X,Y) \equiv H(X) + H(Y) - H(X,Y)$$

maximized over all *single-shot* uses of the channel, where X and Y are the probability distributions for the source and receiver. (Similar expressions, by the way, are difficult to come up with in the quantum case.) This makes things way simpler, since instead of worrying about coding schemes for asymptotically large numbers of bits, we only need to optimize over a single parameter p: say we send 0 with probability p and 1 with probability $1-p$. Since I is unchanged if we replace p with $1-p$ (swapping the 0 and 1 symbols) and since it is concave in p, it follows that $p = 1/2$ must achieve the maximum value of I. Thus $H(X) = H(Y) = 1$. Let $Z = X \oplus Y$. This represents whether or not a bit flip occured, and X, Y carries the same information as X, Z, but X and Z are independent, unlike X and Y. Thus

$$H(X,Y) = H(X,Z) = H(X) + H(Z) = 1 + H_2(p),$$

where $H_2(p) = -p\log_2 p - (1-p)\log_2(1-p)$. Thus the capacity is $C = 1 - H_2(p)$.

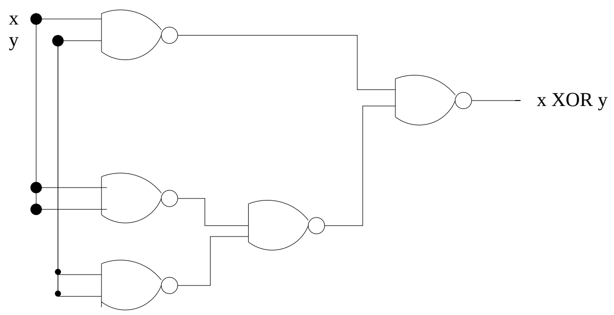
21. If there is one bit flip, then it can be corrected, but if there are two or three bit flips, then we will get the wrong answer. Thus $P(\text{error}) = 3p^2 + p^3 = O(p^2)$.

22. $-\sum_k p_k \log p_k = \frac{1}{4}\log_2 4 + \frac{1}{4}\log_2 4 + \frac{1}{2}\log_2 2 = \frac{4}{4} + \frac{1}{2} = 3/2$. To achieve this rate, encode 0 as 00, 1 as 01 and 2 as 1. The expected number of bits necessary per symbol is 3/2.

23. After we've opened three doors and failed to find the prize, there's no need to open the fourth, since we can deduce that the prize is behind that door. Hence the trick: we only need to find out where the prize is, not actually get it. The answer is $(1+2+3+3)/4 = 2.25$.

24. (a) AND: input $a, 0, b$ and output $a \wedge \neg b$, $a \wedge b$ and b.
    (b) OR: input $a, 1, b$ and output $a \vee b$, $a \vee \neg b$ and b.
    (c) NOT: input $0, 1, x$ and output x, $\neg x$, and x.

25. Here is the circuit:



Proving that NAND can't be made with just XOR gates is a little tricky, partly because we need to define the problem properly. Classical computation (sometimes) takes some primitives for granted, such as COPY, ERASE, and so on. Allowing all these still leaves one thing invariant: any circuit with only XOR (and COPY, ERASE, FANOUT, etc..) will have all outputs (and intermediate results) expressible as linear combinations (mod 2) of the inputs. This can be proved by induction, as the XOR of two linear combinations will produce another different linear combination. Finally, NAND cannot be expressed as a linear combination of its inputs.

26.

$$P\left(\sum X_i \leq \frac{n}{2}\right) = \sum_{k=0}^{n/2} \left(\frac{1}{2}-\epsilon\right)^k \left(\frac{1}{2}+\epsilon\right)^{n-k} \binom{n}{k} \leq 2^n \left(\frac{1}{2}-\epsilon\right)^{n/2} \left(\frac{1}{2}+\epsilon\right)^{n/2} = \left(1-4\epsilon^2\right)^{n/2} \leq e^{-2\epsilon^2 n}$$