UNM Physics 452/581: Introduction to Quantum Information, Solution Set 3, Fall 2007

3.1 Quantum Safecracker

- (a) Recall that $U(\hat{n},\theta) = \exp(-i\hat{n}\cdot\vec{\sigma}\theta/2) = I\cos\frac{\theta}{2} - i\hat{n}\cdot(X,Y,Z)\sin\frac{\theta}{2}$. Since gates are equivalent up to a global phase, we can immediately see that $U(\hat{x},\pi) = -iX \equiv X$, $U(\hat{y},\pi) = -iY \equiv Y$, $U(\hat{z},\pi) = -iZ \equiv Z$.

- (b) Recall the following Pauli properties: $XY = iZ$, $YZ = iX$, $ZX = iY$. Swapping the order of multiplication results in a negative sign.

  - (i) First rotate about $\hat{x}$, then about $\hat{y}$.

$$
\begin{aligned}
U(\hat{y},\frac{\pi}{2})U(\hat{x},\frac{\pi}{2}) &= (I\cos\frac{\pi}{4} - iY\sin\frac{\pi}{4})(I\cos\frac{\pi}{4} - iX\sin\frac{\pi}{4}) && (1)\\
&= I\cos^2\frac{\pi}{4} - iX\cos\frac{\pi}{4}\sin\frac{\pi}{4} - iY\sin\frac{\pi}{4}\cos\frac{\pi}{4} - YX\sin^2\frac{\pi}{4} && (2)\\
&= \frac{1}{2}(I - iX - iY + iZ) && (3)\\
&= \frac{1}{2}\begin{pmatrix} 1+i & -(1+i) \\ 1-i & 1-i \end{pmatrix} && (4)\\
&= \frac{1}{\sqrt{2}}\begin{pmatrix} e^{i\frac{\pi}{4}} & -e^{i\frac{\pi}{4}} \\ e^{i\frac{7\pi}{4}} & e^{i\frac{7\pi}{4}} \end{pmatrix} && (5)\\
&= \frac{e^{i\frac{\pi}{4}}}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -i & -i \end{pmatrix} && (6)
\end{aligned}
$$

  - (ii) Looking at Eq. (3), we notice it has a very similar form to the general decomposition of a rotation at the beginning of part (a), with $\vec{n} = (1,1,-1)$. Normalizing, we have $\hat{n} = \frac{1}{\sqrt{3}}(1,1,-1)$, implying $\theta = \frac{2\pi}{3}$ to give the desired result.

- (c) Since we are assuming ϵ is infinitesimal, we can do a Taylor expansion of the matrix exponential, keeping the first three terms:

$$
\exp\left(-i\hat{n}\cdot\vec{\sigma}\frac{\epsilon}{2}\right) \approx I - i\hat{n}\cdot\vec{\sigma}\frac{\epsilon}{2} - (\hat{n}\cdot\vec{\sigma})^2\frac{\epsilon^2}{8} = I - i\hat{n}\cdot\vec{\sigma}\frac{\epsilon}{2} - \frac{\epsilon^2}{8}I \qquad (7)
$$

  utilizing the fact that $(\hat{n}\cdot\vec{\sigma})^2 = 1$.

– (*i*) Overall, the rotation is (dropping terms of order ϵ^3 or higher):

$$U(\hat{y},-\epsilon)U(\hat{x},-\epsilon)U(\hat{y},\epsilon)U(\hat{x},\epsilon) = (I + \frac{i\epsilon}{2}Y - \frac{\epsilon^2}{8}I)(I + \frac{i\epsilon}{2}X - \frac{\epsilon^2}{8}I) \tag{8}$$

$$\times (I - \frac{i\epsilon}{2}Y - \frac{\epsilon^2}{8}I)(I - \frac{i\epsilon}{2}X - \frac{\epsilon^2}{8}I) \tag{9}$$

$$= \left(I + \frac{i\epsilon}{2}Y + \frac{i\epsilon}{2}X - \frac{\epsilon^2}{4}I - \frac{\epsilon^2}{4}YX\right) \tag{10}$$

$$\times \left(I - \frac{i\epsilon}{2}Y - \frac{i\epsilon}{2}X - \frac{\epsilon^2}{4}I - \frac{\epsilon^2}{4}YX\right) \tag{11}$$

$$= I + \frac{i\epsilon}{2}Y + \frac{i\epsilon}{2}X - \frac{i\epsilon}{2}Y - \frac{i\epsilon}{2}X - \frac{\epsilon^2}{2} - \frac{\epsilon^2}{2}YX \tag{12}$$

$$+ \frac{\epsilon^2}{4}(X^2 + Y^2) + \frac{\epsilon^2}{4}(XY + YX) \tag{13}$$

$$= I - \frac{\epsilon^2}{2}YX \tag{14}$$

$$= I + i\frac{\epsilon^2}{2}Z \tag{15}$$

– (*iii*) Comparing to the general taylor series expansion, this is $U(-\hat{z},\epsilon^2)$.

- (*d*)

– (*i*) We have:

$$U(\frac{1}{\sqrt{3}}(\hat{x}+\hat{y}+\hat{z}),\frac{2\pi}{3}) = I\cos\frac{\pi}{3} - i\sin\frac{\pi}{3}\frac{1}{\sqrt{3}}(X+Y+Z) \tag{16}$$

$$= \frac{1}{2}(I - iX - iY - iZ) \tag{17}$$

$$= \frac{1}{2}\begin{pmatrix} 1-i & -(1+i) \\ 1-i & 1+i \end{pmatrix} \tag{18}$$

$$\tag{19}$$

– (*ii*) The spin up vectors are given by the +1 eigenvectors of the corresponding Pauli matrices.

1. Spin up along X

$$\frac{1}{2}\begin{pmatrix} 1-i & -(1+i) \\ 1-i & 1+i \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} -i \\ 1 \end{pmatrix} = \frac{-i}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \tag{20}$$

Up to a phase, this is spin up along Y.

2. Spin up along Y

$$\frac{1}{2}\begin{pmatrix} 1-i & -(1+i) \\ 1-i & 1+i \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1-i \\ 0 \end{pmatrix} = e^{-i\frac{\pi}{4}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{21}$$

Up to a phase, this is spin up along Z.

3. Spin up along Z

$$\frac{1}{2}\begin{pmatrix}1-i & -(1+i)\\ 1-i & 1+i\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1-i\\1-i\end{pmatrix}=\frac{e^{-i\frac{\pi}{4}}}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \tag{22}$$

Up to a phase, this is spin up along X.

– (c) Comparing Eq. (3) and Eq. (17), we see that the only difference is the sign of the Z term, which came from simplifying the YX term. Knowing that reversing the order of multiplication of two Pauli matrices results in an overall minus sign, we should try first rotating about $\hat{y}$ then about $\hat{x}$:

$$U(\hat{x},\frac{\pi}{2})U(\hat{y},\frac{\pi}{2}) = (I\cos\frac{\pi}{4}-iX\sin\frac{\pi}{4})(I\cos\frac{\pi}{4}-iY\sin\frac{\pi}{4}) \tag{23}$$

$$= I\cos^2\frac{\pi}{4}-iX\cos\frac{\pi}{4}\sin\frac{\pi}{4}-iY\sin\frac{\pi}{4}\cos\frac{\pi}{4}-XY\sin^2\frac{\pi}{4} \tag{24}$$

$$= \frac{1}{2}(I-iX-iY-iZ) \tag{25}$$

$$= \frac{1}{2}(I-i(1,1,1)\cdot(X,Y,Z)) \tag{26}$$

$$= I\cos\frac{\pi}{3}-\frac{i}{\sqrt{3}}(1,1,1)\cdot(X,Y,Z)\sin\frac{\pi}{3} \tag{27}$$

So rotate by $\frac{\pi}{2}$ about $\hat{y}$, then $\frac{\pi}{2}$ about $\hat{x}$ to open the safe.

3.2 Bloch sphere

- (a) Recall from class that any qubit state say can be written as $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$. Taking the explicit outer product:

$$\begin{pmatrix}\cos\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2}\end{pmatrix}\begin{pmatrix}\cos\frac{\theta}{2} & e^{-i\phi}\sin\frac{\theta}{2}\end{pmatrix} \tag{28}$$

$$= \begin{pmatrix}\cos^2\frac{\theta}{2} & e^{-i\phi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2}\cos\frac{\theta}{2} & \sin^2\frac{\theta}{2}\end{pmatrix} \tag{29}$$

$$= \frac{1}{2}\begin{pmatrix}1+\cos\theta & \cos\phi\sin\theta-i\sin\phi\sin\theta\\ \cos\phi\sin\theta+i\sin\phi\sin\theta & 1-\cos\theta\end{pmatrix} \tag{30}$$

$$= \frac{1}{2}\left[\begin{pmatrix}1&0\\0&1\end{pmatrix}+\cos\phi\sin\theta\begin{pmatrix}0&1\\1&0\end{pmatrix}+\sin\phi\sin\theta\begin{pmatrix}0&-i\\i&0\end{pmatrix}+\cos\theta\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right] \tag{31}$$

$$= \frac{1}{2}\left[I+(\cos\phi\sin\theta,\sin\phi\sin\theta,\cos\theta)\cdot(X,Y,Z)\right] \tag{32}$$

So $\vec{\mathbf{p}} = (\cos\phi\sin\theta,\sin\phi\sin\theta,\cos\theta)$ and $|\vec{\mathbf{p}}| = \cos^2\phi\sin^2\theta+\sin^2\phi\sin^2\theta+\cos^2\theta = \sin^2\theta+\cos^2\theta = 1$.

- (b) Since $U(\hat{n},\theta)$ takes $|\psi\rangle$ to $|\psi'\rangle$, we have

$$\frac{1}{2}(I+\vec{\mathbf{p}}'\cdot\vec{\sigma}) = U(\hat{n},\theta)\frac{1}{2}(I+\vec{\mathbf{p}}\cdot\vec{\sigma})U^\dagger(\hat{n},\theta) = \frac{1}{2}(I+U(\hat{n},\theta)(\vec{\mathbf{p}}\cdot\vec{\sigma})U^\dagger(\hat{n},\theta)) \tag{33}$$

Before continuing, we make note of the following identity (using Einstein summation convention):

$$(\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = a_i b_j \sigma_i \sigma_j = a_i b_j (I\delta_{ij} + i\epsilon_{ijk}\sigma_k) = (\vec{a}\cdot\vec{b}) + i(\vec{a}\times\vec{b})\cdot\vec{\sigma} \tag{34}$$

If you are unaccustomed to this notation, you can verify the identity by explicitly calculating the left and right hand sides.

$$U(\hat{n},\theta)(\vec{\mathbf{p}}\cdot\vec{\sigma})U^\dagger(\hat{n},\theta) \tag{35}$$
$$= \left[I\cos\frac{\theta}{2} - i\sin\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})\right](\vec{\mathbf{p}}\cdot\vec{\sigma})\left[I\cos\frac{\theta}{2} + i\sin\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})\right] \tag{36}$$
$$= \left[I\cos\frac{\theta}{2} - i\sin\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})\right]\left[\cos\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma}) + i\sin\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma})(\hat{n}\cdot\vec{\sigma})\right] \tag{37}$$
$$= \left[I\cos\frac{\theta}{2} - i\sin\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})\right]\left[\cos\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma}) + i\sin\frac{\theta}{2}\left((\vec{\mathbf{p}}\cdot\hat{n})I + i(\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma}\right)\right] \tag{38}$$
$$= \cos^2\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma}) + i\sin\frac{\theta}{2}\cos\frac{\theta}{2}\left((\vec{\mathbf{p}}\cdot\hat{n})I + i(\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma}\right) \tag{39}$$
$$- i\sin\frac{\theta}{2}\cos\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})(\vec{\mathbf{p}}\cdot\vec{\sigma}) + \sin^2\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})\left((\vec{\mathbf{p}}\cdot\hat{n})I + i(\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma}\right) \tag{40}$$
$$= \cos^2\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma}) + \frac{i}{2}\sin\theta\left((\vec{\mathbf{p}}\cdot\hat{n})I + i(\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma}\right) - \frac{i}{2}\sin\theta\left((\vec{\mathbf{p}}\cdot\hat{n})I - i(\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma}\right)$$
$$+ \sin^2\frac{\theta}{2}\left[((\vec{\mathbf{p}}\cdot\hat{n})\hat{n}\cdot\vec{\sigma}) + i(\hat{n}\cdot\vec{\sigma})((\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma})\right] \tag{41}$$
$$= \cos^2\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma}) - \sin\theta(\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma} + \sin^2\frac{\theta}{2}((\vec{\mathbf{p}}\cdot\hat{n})\hat{n}\cdot\vec{\sigma}) \tag{42}$$
$$+ i\sin^2\frac{\theta}{2}\left(\underbrace{\hat{n}\cdot(\vec{\mathbf{p}}\times\hat{n})}_{=0\text{ since }(\vec{\mathbf{p}}\times\hat{n})\perp\hat{n}} + i(\hat{n}\times(\vec{\mathbf{p}}\times\hat{n}))\cdot\vec{\sigma}\right) \tag{43}$$
$$= \cos^2\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma}) - \sin\theta(\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma} + \sin^2\frac{\theta}{2}((\vec{\mathbf{p}}\cdot\hat{n})\hat{n}\cdot\vec{\sigma}) \tag{44}$$
$$- \sin^2\frac{\theta}{2}\left(\vec{\mathbf{p}}\underbrace{(\hat{n}\cdot\hat{n})}_{=1\text{ since }|\hat{n}|^2=1} - \hat{n}(\vec{\mathbf{p}}\cdot\hat{n})\right)\cdot\vec{\sigma} \tag{45}$$
$$= \cos^2\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma}) - \sin\theta(\vec{\mathbf{p}}\times\hat{n})\cdot\vec{\sigma} - \sin^2\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\vec{\sigma}) + 2\sin^2\frac{\theta}{2}(\vec{\mathbf{p}}\cdot\hat{n})(\hat{n}\cdot\vec{\sigma}) \tag{46}$$
$$= \cos\theta(\vec{\mathbf{p}}\cdot\vec{\sigma}) + \sin\theta(\vec{\hat{n}}\times\vec{\mathbf{p}})\cdot\vec{\sigma} + (1-\cos\theta)(\vec{\mathbf{p}}\cdot\hat{n})(\hat{n}\cdot\vec{\sigma}) \tag{47}$$

Since we are looking for something of the form $\vec{\mathbf{p}}'\cdot\vec{\sigma}$ we directly read off $\vec{\mathbf{p}}' = \cos\theta\vec{\mathbf{p}} + \sin\theta(\hat{n}\times\vec{\mathbf{p}}) + (1-\cos\theta)(\vec{\mathbf{p}}\cdot\hat{n})\hat{n}$, which corresponds to rotating the vector $\tilde{\mathbf{p}}$ by an angle θ around the unit vector $\hat{n}$. This has been written in the form of Rodrigues' rotation formula.

- (c) We will work in the z-basis, so that $|\pm x\rangle = \frac{1}{\sqrt{2}}(|+z\rangle \pm |-z\rangle)$ and $|\pm y\rangle =$

$\frac{1}{\sqrt{2}}\left(|+z\rangle \pm i|-z\rangle\right)$. Given the problem statement, we have that

$$U|\pm z\rangle = e^{i\theta_z^{(\pm)}}|\mp z\rangle \tag{48}$$

Using this in the definitions for the other two directions, we find

$$U|\pm x\rangle = e^{i\theta_x^{(\pm)}}|\pm x\rangle \tag{49}$$

$$= \frac{1}{\sqrt{2}}\left[e^{i\theta_x^{(\pm)}}|+z\rangle \pm e^{i\theta_x^{(\pm)}}|-z\rangle\right] \tag{50}$$

$$\tag{51}$$

But we also have

$$U|\pm x\rangle = U\frac{1}{\sqrt{2}}\left[|+z\rangle \pm |-z\rangle\right] \tag{52}$$

$$= \frac{1}{\sqrt{2}}\left[e^{i\theta_z^{(+)}}|-z\rangle \pm e^{i\theta_z^{(-)}}|+z\rangle\right] \tag{53}$$

$$= \frac{1}{\sqrt{2}}\left[\pm e^{i\theta_z^{(-)}}|+z\rangle + e^{i\theta_z^{(+)}}|-z\rangle\right] \tag{54}$$

Comparing coefficients we find

$$e^{i\theta_x^{(\pm)}} = \pm e^{i\theta_z^{(-)}} \tag{55}$$

$$e^{i\theta_x^{(\pm)}} = \pm e^{i\theta_z^{(+)}} \tag{56}$$

$$\Rightarrow\ e^{i\theta_z^{(-)}} = e^{i\theta_z^{(+)}} \tag{57}$$

For the y basis, we have

$$U|\pm z\rangle = e^{i\theta_y^{(\pm)}}|\pm y\rangle \tag{58}$$

$$= \frac{1}{\sqrt{2}}\left[e^{i\theta_y^{(\pm)}}|+z\rangle \pm ie^{i\theta_y^{(\pm)}}|-z\rangle\right] \tag{59}$$

$$\tag{60}$$

But we also have

$$U|\pm y\rangle = U\frac{1}{\sqrt{2}}\left[|+z\rangle \pm i|-z\rangle\right] \tag{61}$$

$$= \frac{1}{\sqrt{2}}\left[e^{i\theta_z^{(+)}}|-z\rangle \pm ie^{i\theta_z^{(-)}}|+z\rangle\right] \tag{62}$$

$$= \frac{1}{\sqrt{2}}\left[\pm ie^{i\theta_z^{(-)}}|+z\rangle + e^{i\theta_z^{(+)}}|-z\rangle\right] \tag{63}$$

Comparing coefficients we find

$$e^{i\theta_y^{(\pm)}} = \pm ie^{-\theta_z^{(-)}} \tag{64}$$

$$e^{i\theta_y^{(\pm)}} = \mp ie^{-\theta_z^{(+)}} \tag{65}$$

$$\Rightarrow\ e^{-\theta_z^{(-)}} = -e^{-\theta_z^{(+)}} \tag{66}$$

There is no way to satisfy both Eq. (57) and Eq. (66) simultaneously.

3.3 Simon Says

- (a) The Walsh-Hadamard transform is given by

$$U_{WH} = \frac{1}{2^{n/2}} \sum_{j,k=0}^{2^n-1} (-1)^{j \cdot k} |j\rangle\langle k| \tag{67}$$

Applying this to an initial state of the form $|0\rangle^{\otimes n}$ gives

$$\frac{1}{2^{n/2}} \sum_{j,k=0}^{2^n-1} (-1)^{j \cdot k} |j\rangle\langle k|0\rangle = \frac{1}{2^{n/2}} \sum_{j,k=0}^{2^n-1} (-1)^{j \cdot k} |j\rangle \delta_{k0} \tag{68}$$

$$= \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} (-1)^{j \cdot 0} |j\rangle \tag{69}$$

$$= \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle \tag{70}$$

which is a uniform superposition over all states.

- (b) Define the linear map $Q := |i\rangle|j\rangle \mapsto |i\rangle|j \oplus x_o\rangle$. Then

$$Q\left[\left(\frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} |i\rangle\right) \otimes |0\rangle^{\otimes n}\right] = Q\left[\frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} \left(|i\rangle \otimes |0\rangle^{\otimes n}\right)\right] \tag{71}$$

$$= \left[\frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} Q\left(|i\rangle \otimes |0\rangle^{\otimes n}\right)\right] \tag{72}$$

$$= \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} |i\rangle \otimes |x_i\rangle \tag{73}$$

- (c) We now measure using the projectors $\Pi_j = I^{\otimes n} \otimes |j\rangle\langle j|$, for $j = 0, \ldots, N-1$. Consider the case where $s = 0^n$. We have $x_i = x_j$ if and only if $i = j \oplus 0$, which implies that each x_i is distinct. Since we are free to order this list in any way, let $x_i = i$ for $i = 0, \ldots, N-1$. Our state at the end of part (a) is then

$$\frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} |i\rangle \otimes |i\rangle \tag{74}$$

The probability of outcome j is given by

$$\text{prob}(j) = \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} \langle i| \otimes \langle i| \Pi_j \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |k\rangle \tag{75}$$

$$= \frac{1}{2^n} \sum_{i,k=0}^{2^n-1} \langle i| \otimes \langle i| (I^{\otimes n} \otimes |j\rangle\langle j|) |k\rangle \otimes |k\rangle \tag{76}$$

$$= \frac{1}{2^n} \sum_{i,k=0}^{2^n-1} \langle i|k\rangle \langle i|j\rangle \langle j|k\rangle \tag{77}$$

$$= \frac{1}{2^n} \sum_{i,k=0}^{2^n-1} \delta_{ijk} \tag{78}$$

$$= \frac{1}{2^n} \tag{79}$$

where in the last step we used the fact that exactly one term in the sum has $i = j$ and $k = j$.

The post-measurement state is given by

$$\psi' = \sqrt{2^n} \Pi_j \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} |i\rangle \otimes |i\rangle \tag{80}$$

$$= \sum_{i=0}^{2^n-1} |i\rangle \otimes (|j\rangle\langle j|i\rangle) \tag{81}$$

$$= |j\rangle|j\rangle \tag{82}$$

$$= |j\rangle|x_j\rangle \tag{83}$$

where in the last step we have generalized from our assumed definition that $x_j = j$.

Now consider the case when $s \neq 0^n$. We now have that $x_i = x_j$ if and only if $i = j \oplus s$ which implies $x_i = x_{i \oplus s}$. Then exactly two $|x_i\rangle$ terms are equal. The probability of measuring outcome j for this case is

$$\mathrm{prob}(j) = \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} \langle i| \otimes \langle x_i| \Pi_j \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |x_k\rangle \tag{84}$$

$$= \frac{1}{2^n} \sum_{i,k=0}^{2^n-1} (\langle i| \otimes \langle x_i|)(I^{\otimes n} \otimes |j\rangle\langle j|)(|k\rangle \otimes |x_k\rangle) \tag{85}$$

$$= \frac{1}{2^n} \sum_{i,k=0}^{2^n-1} \langle i|k\rangle \otimes (\langle x_i|j\rangle\langle j|x_k\rangle) \tag{86}$$

$$= \frac{1}{2^n} \sum_{i,k=0}^{2^n-1} \delta_{ik}(\langle x_i|j\rangle\langle j|x_k\rangle) \tag{87}$$

$$= \frac{1}{2^n} \sum_{i}^{2^n-1} (\langle x_i|j\rangle\langle j|x_i\rangle) \tag{88}$$

$$= \frac{1}{2^{n-1}} \tag{89}$$

where in the last step we have used the fact that $\langle x_i|j\rangle$ is equal to one for exactly two terms in the sum.

The post-measurement state is given by

$$\psi' = \sqrt{2^{n-1}} \Pi_j \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} |i\rangle \otimes |x_i\rangle \tag{90}$$

$$= \frac{1}{\sqrt{2}} \sum_{i=0}^{2^n-1} |i\rangle \otimes (|j\rangle\langle j|x_i\rangle) \tag{91}$$

$$= \frac{1}{\sqrt{2}} \sum_{i=0}^{2^n-1} |i\rangle \otimes |j\rangle \delta_{j,x_i} \tag{92}$$

$$= \frac{1}{\sqrt{2}} (|j\rangle + |j \oplus s\rangle) \otimes |x_j\rangle \tag{93}$$

where in the last step we have used the fact that $x_j = x_{j\oplus s}$.

- (d) First consider the case when $s = 0^n$. Applying another Walsh-Hadamard transform gives

$$U_{WH}|j\rangle|x_j\rangle = \left[\frac{1}{2^{n/2}} \sum_{i,k=0}^{2^n-1} (-1)^{i\cdot k} |i\rangle\langle k|j\rangle \right] \otimes x_j \tag{94}$$

$$= \left[\frac{1}{2^{n/2}} \sum_{i,k=0}^{2^n-1} (-1)^{i\cdot k} |i\rangle \delta_{kj} \right] \otimes x_j \tag{95}$$

$$= \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} (-1)^{i\cdot j} |i\rangle \otimes |x_j\rangle \tag{96}$$

Now consider the case when $s \neq 0^n$.

$$\begin{aligned}
& U_{WH}\left[\frac{1}{\sqrt{2}}\left(|j\rangle + |j \oplus s\rangle\right)\right] \otimes |x_j\rangle && (97)\\
&= \frac{1}{\sqrt{2}}\left[U_{WH}|j\rangle \otimes |x_j\rangle + U_{WH}|j \oplus s\rangle \otimes |x_j\rangle\right] && (98)\\
&= \frac{1}{2^{n/2+1/2}}\left[\sum_{i=0}^{2^n-1}(-1)^{i\cdot j}|i\rangle \otimes |x_j\rangle + \sum_{i,k=0}^{2^n-1}(-1)^{i\cdot k}|i\rangle\langle k|j \oplus s\rangle \otimes |x_j\rangle\right] && (99)\\
&= \frac{1}{2^{n/2+1/2}}\left[\sum_{i=0}^{2^n-1}(-1)^{i\cdot j}|i\rangle \otimes |x_j\rangle + \sum_{i,k=0}^{2^n-1}(-1)^{i\cdot k}|i\rangle\delta_{k,j\oplus s} \otimes |x_j\rangle\right] && (100)\\
&= \frac{1}{2^{n/2+1/2}}\left[\sum_{i=0}^{2^n-1}(-1)^{i\cdot j}|i\rangle \otimes |x_j\rangle + \sum_{i=0}^{2^n-1}(-1)^{i\cdot(j\oplus s)}|i\rangle \otimes |x_j\rangle\right] && (101)\\
&= \frac{1}{2^{n/2+1/2}}\sum_{i=0}^{2^n-1}\left[(-1)^{i\cdot j} + (-1)^{i\cdot j}(-1)^{i\cdot s}\right]|i\rangle \otimes |x_j\rangle && (102)\\
&= \frac{1}{2^{n/2+1/2}}\sum_{i=0}^{2^n-1}(-1)^{i\cdot j}\underbrace{\left[1 + (-1)^{i\cdot s}\right]}_{\text{is 2 if } i\cdot s=0,\text{ else }=0}|i\rangle \otimes |x_j\rangle && (103)\\
&= \frac{1}{2^{(n-1)/2}}\sum_{i\cdot s=0}(-1)^{i\cdot j}|i\rangle \otimes |x_j\rangle && (104)
\end{aligned}$$

where the sum in the last line is over i that satisfy $i \cdot s = 0$.

- (e) Looking at our worst case results in part (d), we notice that there is a uniform (equal) probability of recovering a given index i. Clearly the first measurement will yield an i_0 that is linearly independent, since it is the only index we have so far. Using this i_0, we start to form a basis $\mathbf{B}$, which is the span of $\{i_0\}$, where we treat i_0 as a length n vector with entries 0 and 1. Measuring again, we get result i_1. This will be linearly independent of $\mathbf{B}$ if it is not equal to i_0. The probability of this is the probability of not measuring i_0, which is just $1 - \frac{1}{2^n}$.

  Generalizing, we see that at step $m+1$, the probability that we measure an index that is linearly independent from the span of the m previous independent vectors is $\frac{2^n - 2^m}{2^n} = 1 - \frac{1}{2^{m-n}}$. To understand this expression, realize that from a linear algebra perspective, we can interpret our basis of m vectors as spanning the first m entries of an arbitrary vector. The only place a linearly independent vector can differ is in the remaining m locations, indicating that of all the 2^n possible bit strings, only $2^n - 2^m$ are linearly independent from those we have already seen. The probability that the n

equations are linearly independent is then

$$P_{\text{independent}} = \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{4}\right) \times \cdots \times \left(1 - \frac{1}{2^{n-1}}\right) \times \left(1 - \frac{1}{2^n}\right) \tag{105}$$

$$> \prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) \tag{106}$$

$$> \frac{1}{4} \tag{107}$$

where we have acheived a lower bound by adding terms. Since $1 - \frac{1}{2^n} < 1$ for all n, we are guaranteed that the final expression is smaller than the actual form.