TEST VII (TOETS VII) 3B

1.

$$\begin{aligned}
|s(\theta,\phi)\rangle &= P\left(\frac{\pi}{4}-\frac{\phi}{2}\right)U_H P\left(\frac{\theta}{2}\right)U_H|0\rangle \\
&= P\left(\frac{\pi}{4}-\frac{\phi}{2}\right)U_H P\left(\frac{\theta}{2}\right)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \\
&= P\left(\frac{\pi}{4}-\frac{\phi}{2}\right)U_H \frac{1}{\sqrt{2}}(e^{i\theta/2}|0\rangle+e^{-i\theta/2}|1\rangle) \\
&= P\left(\frac{\pi}{4}-\frac{\phi}{2}\right)\frac{1}{2}\left(e^{i\theta/2}(|0\rangle+|1\rangle)+e^{-i\theta/2}(|0\rangle-|1\rangle)\right) \\
&= P\left(\frac{\pi}{4}-\frac{\phi}{2}\right)\left(\cos\frac{\theta}{2}|0\rangle+i\sin\frac{\theta}{2}|1\rangle\right) \\
&= e^{i\frac{\pi}{4}}\left(e^{-i\frac{\phi}{2}}\cos\frac{\theta}{2}|0\rangle+e^{i\frac{\phi}{2}}\sin\frac{\theta}{2}|1\rangle\right) \\
&= e^{i\frac{\pi}{4}-\frac{\phi}{2}}\left(\cos\frac{\theta}{2}|0\rangle+e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)
\end{aligned}$$

The most general state of a single qubit is described by three real parameters $\theta, \phi, \sigma \in \mathbf{R}$:

$$e^{i\sigma}\left(\cos\frac{\theta}{2}|0\rangle+e^{i\phi}\sin\frac{\theta}{2}|1\rangle)\right).$$

The parameter σ represents the global phase, and can be ignored since it cannot be detected in our measurement model. The same applies to the global phase $\exp(i\pi/4-\phi/2)$ in our derivation. Thus θ and ϕ can be used to define any single qubit $|s(\theta,\phi)\rangle$. For the probabilities we have

$$\begin{aligned}
|\langle 0|s(\theta,\phi)\rangle|^2 &= \cos^2\frac{\theta}{2} \\
|\langle 1|s(\theta,\phi)\rangle|^2 &= \sin^2\frac{\theta}{2}
\end{aligned}$$

$$
\begin{aligned}
|\langle s(\theta',\phi')|s(\theta,\phi)\rangle|^2 &= \left| e^{-i\frac{\pi}{4}}\left(e^{i\frac{\phi'}{2}}\cos\frac{\theta'}{2}\langle 0| + e^{-i\frac{\phi'}{2}}\sin\frac{\theta'}{2}\langle 1|\right)\cdot \right. \\
&\quad \left. e^{i\frac{\pi}{4}}\left(e^{-i\frac{\phi}{2}}\cos\frac{\theta}{2}|0\rangle + e^{i\frac{\phi}{2}}\sin\frac{\theta}{2}|1\rangle\right)\right|^2 \\
&= \left|\cos\frac{\theta}{2}\cos\frac{\theta'}{2}e^{\frac{i}{2}(\phi'-\phi)} + \sin\frac{\theta}{2}\sin\frac{\theta'}{2}e^{\frac{i}{2}(\phi-\phi')}\right|^2 \\
&= \left|\cos\frac{1}{2}(\phi'-\phi)\cos\frac{1}{2}(\theta'-\theta) + i\sin\frac{1}{2}(\phi'-\phi)\sin\frac{1}{2}(\theta'+\theta)\right|^2 \\
&= \cos^2\frac{1}{2}(\phi'-\phi)\cos^2\frac{1}{2}(\theta'-\theta) + \sin^2\frac{1}{2}(\phi'-\phi)\sin^2\frac{1}{2}(\theta'+\theta)
\end{aligned}
$$

2.

$$(x_A, x_B, x_C) \in \{\,(0,0,1),(0,1,0),(1,0,0),(1,1,1)\,\}.$$

Note the symmetry in the state $|\psi\rangle$. A qubit can be exchanged with any other without our being able to determine any difference. Thus we need only calculate the transform for $(0,0,1)$ and $(1,1,1)$. For $(1,1,1)$ we have $f_3(1,1,1)|\psi\rangle = I \otimes I \otimes I|\psi\rangle = |\psi\rangle$. Measuring the qubits yields

$$(s_A, s_B, s_C) \in \{\,(0,0,1),(0,1,0),(1,0,0),(1,1,1)\,\}$$

with equal probability. In each case we find $s_A + s_B + s_C = 1 \ mod\ 2$. For $(0,0,1)$ we have $f_3(0,0,1) = U_H \otimes U_H \otimes I$. Note that

$$|\psi\rangle = \frac{1}{2}(|01\rangle + |10\rangle) \otimes |0\rangle + \frac{1}{2}(|00\rangle - |11\rangle) \otimes |1\rangle.$$

Thus

$$f_3(0,0,1)|\psi\rangle = \frac{1}{2}(|00\rangle - |11\rangle) \otimes |0\rangle + \frac{1}{2}(|01\rangle + |10\rangle) \otimes |1\rangle.$$

We find that measuring the qubits yields

$$(s_A, s_B, s_C) \in \{\,(0,0,0),(0,1,1),(1,0,1),(1,1,0)\,\}$$

with equal probability. In each case we find $s_A + s_B + s_C = 0 \ mod\ 2$.

(x_A, x_B, x_C)	$x_A \cdot x_B \cdot x_C$	$s_A + s_B + s_C$ *mod* 2
(0,0,1)	0	0
(0,1,0)	0	0
(1,0,0)	0	0
(1,1,1)	1	1

We find that $s_A + s_B + s_C = x_A \cdot x_B \cdot x_C \ mod\ 2$.
Suppose Alice, Bob and Carol each have a bit string $(x_{A,1}, \ldots, x_{A,n})$, $(x_{B,1}, \ldots, x_{B,n})$ and $(x_{C,1}, \ldots, x_{C,n})$, respectively. They want to calculate

$$f(\mathbf{x}_A, \mathbf{x}_B, \mathbf{x}_C) = \sum_{j=1}^{n} x_{A,j} \cdot x_{B,j} \cdot x_{C,j} \ mod\ 2$$

sharing (communicating) as little information as possible. If Alice, Bob and Carol share n triplets of qubits in the state $|\psi\rangle$ they can calculate $s_{A,1}, \ldots, s_{A,n}$, $s_{B,1}, \ldots, s_{B,n}$ and $s_{C,1}, \ldots, s_{C,n}$ respectively as above. Thus

$$f(\mathbf{x}_A, \mathbf{x}_B, \mathbf{x}_C) = \sum_{j=1}^{n} s_{A,j} + s_{B,j} + s_{C,j} \ mod\ 2.$$

If Alice, Bob and Carol calculate

$$S_{A|B|C} = \sum_{j=1}^{n} S_{A|B|C,j} \ mod\ 2,$$

Bob and Carol need only to send one bit each (S_B and S_C) to Alice for Alice to compute $f(\mathbf{x}_A, \mathbf{x}_B, \mathbf{x}_C) = S_A + S_B + S_C$, for any n. Classically, for $n >= 3$, 3 bits of communication is required.