A. Here are two short, closely related problems.

1. Prove that any permutation matrix is unitary.
2. If a permutation matrix is its own inverse, then what special property must the permutation matrix have?

B. In class we've proved that $F \cdot (|\alpha\rangle \otimes |-\rangle) = (-1)^{f(\alpha)} |\alpha\rangle \otimes |-\rangle$ for any n-qbit classical state $|\alpha\rangle$. One way to interpret this theorem is that we're demonstrating 2^n eigenvectors for F, with each eigenvalue being ± 1 depending on exactly which f underlies F. But F is unitary $2^{n+1} \times 2^{n+1}$, so it should have 2^{n+1} eigenvectors.

So here's my question: Where are the other 2^n eigenvectors for F? (Hint: Make an educated guess, and then check it.)

C. Here is a classical seven-bit operation:

$$\begin{aligned} & |\alpha\beta\gamma\delta\zeta\eta\theta\rangle \\ \mapsto\ & |\alpha\beta\gamma\delta\rangle\, |\zeta \oplus (\alpha \odot \gamma) \oplus (\alpha \odot \beta \odot \delta) \oplus (\gamma \odot \beta \odot \delta)\rangle\, |\eta \oplus \alpha \oplus \gamma \oplus (\beta \odot \delta)\rangle\, |\theta \oplus \beta \oplus \delta\rangle\,. \end{aligned}$$

What does it do, in English? (Hint: Recognize it as the invertible version of a non-invertible f. Analyze f from right to left. The answer is short and simple, eventually.)

D. With so many similar toy problems flying around, maybe it's useful to consider how they relate to each other. The Bernstein-Vazirani problem is not a special case of the Simon problem, and the Simon problem is not a special case of the Bernstein-Vazirani problem. (You might want to take a moment to convince yourself of those facts, but don't hand in your musings.)

So here's my question: What is the intersection of the Bernstein-Vazirani and Simon problems? In other words, what is the largest problem that can be viewed as a special case of both? Be thorough, precise, and specific. For example, Bernstein-Vazirani has 2^n possible answers, and Simon has $2^n - 1$ possible answers. How many possible answers does the intersection problem have?

E. (This is an optional study problem. Don't hand it in.) In the analysis of Simon's algorithm, rigorously show that the first partial measurement collapses the state to some $\frac{1}{\sqrt{2}}(|\beta\rangle + |\delta \oplus \beta\rangle) \otimes |f(\beta)\rangle$, with all β being equally probable. (You will need to get down and dirty with the concept of partial measurement of the last m qbits of an $(n+m)$-qbit state.)

E. (This is another optional study problem.) What happens if we remove the first partial measurement from Simon's core algorithm? Does the algorithm still work? (Warning: This also takes a while.)