A. The key concept is that, if F is invertible (and takes classical states to classical states), then it is a permutation of the classical states, so it is a permutation matrix, so it is a unitary matrix, so it is a valid gate.

1. This F is its own inverse and hence a valid gate by the reasoning above. It is symmetric to — and equally as good as — our usual convention.

2. This construction does not generally work. For example, if f is the identity function ($f(\alpha) = \alpha$), then $F \cdot |\alpha\rangle|\beta\rangle = |0 \cdots 0\rangle|\beta\rangle$, so F is not invertible and not unitary.

3. Define G by $G \cdot |\alpha\rangle|\beta\rangle = |\mathrm{rev}(\alpha)\rangle|\beta \oplus f(\mathrm{rev}(\alpha))\rangle$. Then

$$G \cdot F \cdot |\alpha\rangle|\beta\rangle = G \cdot |\mathrm{rev}(\alpha)\rangle|\beta \oplus f(\alpha)\rangle = |\alpha\rangle|\beta \oplus f(\alpha) \oplus f(\alpha)\rangle = |\alpha\rangle|\beta\rangle$$

and

$$F \cdot G \cdot |\alpha\rangle|\beta\rangle = F \cdot |\mathrm{rev}(\alpha)\rangle|\beta \oplus f(\mathrm{rev}(\alpha))\rangle = |\alpha\rangle|\beta \oplus f(\mathrm{rev}(\alpha)) \oplus f(\mathrm{rev}(\alpha))\rangle = |\alpha\rangle|\beta\rangle.$$

So $G = F^{-1}$, and F is a valid gate by the reasoning above.

B. The intersection problem concerns a function $f : \{0,1\}^n \to \{0,1\}$ containing a hidden δ such that $f(\alpha) = \delta \odot \alpha$. The function is either constant, which happens only when $\delta = 0 \cdots 0$, or fair, which happens for all other δ. So the intersection problem is: Determine whether $\delta = 0 \cdots 0$.

C. In Shor's algorithm, we are trying to find c/d such that

$$\left| \frac{b}{2^n} - \frac{c}{d} \right| \leq \frac{1}{2^{n+1}}.$$

If there were two such c/d — call them c/d and c'/d' — then they would satisfy

$$\left| \frac{c}{d} - \frac{c'}{d'} \right| \leq \left| \frac{b}{2^n} - \frac{c}{d} \right| + \left| \frac{b}{2^n} - \frac{c'}{d'} \right| \leq \frac{2}{2^{n+1}} = \frac{1}{2^n}.$$

But in Homework 15 Problem C we proved that, because $d, d' < m$,

$$\left| \frac{c}{d} - \frac{c'}{d'} \right| > \frac{1}{2^n}.$$

This contradiction implies that there cannot be two such c/d.

D. First, the assumption that $2^n \geq m^2$ justifies the assumption that the superposition coming out of F is approximately uniform (although there might be other ways to justify that assumption). Second, it lets us replace the sine of a certain angle with the angle itself. Third, it tells us that $qp/2^n \approx 1$ (just after the second reason). Those three reasons should have appeared in your Homework 15. The fourth reason, which we learned after Homework 15, is that the $c/d \neq c'/d'$ exercise used in problem C above depends on $\frac{1}{m^2} \geq \frac{1}{2^n}$.