CSEP 590tv In Class Problems, July 27, 2005

Dave Bacon

1. Suppose we are working on the n bit Bernstein-Varizani problem and the hidden strings are $a = 01$ and $b = 0$. The two bit function is then $f(x_1, x_2) = (a \cdot x) \oplus b = (0 \cdot x_1 \oplus 1 \cdot x_2) \oplus 0 = x_2$. The unitary used to evaluate this function is

$$U = \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \sum_{y=0}^{1} |x_1, x_2, y \oplus f(x_1, x_2)\rangle\langle x_1, x_2, y|$$

Write this unitary as a sum of outer products of computational basis states for this choice of function.

Solution: The unitary is

$$U = \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \sum_{y=0}^{1} |x_1, x_2, y \oplus f(x_1, x_2)\rangle\langle x_1, x_2, y|$$

Now we expand these sum, one by one. First do the sum over y

$$\begin{aligned} U &= \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} (|x_1, x_2, 0 \oplus f(x_1, x_2)\rangle\langle x_1, x_2, 0| + |x_1, x_2, 1 \oplus f(x_1, x_2)\rangle\langle x_1, x_2, 1|) \\ &= \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \left(|x_1, x_2, f(x_1, x_2)\rangle\langle x_1, x_2, 0| + |x_1, x_2, \bar{f}(x_1, x_2)\rangle\langle x_1, x_2, 1|\right) \end{aligned}$$

where we have used the fact that $0 \oplus a = a$ and $1 \oplus a = \bar{a}$ where $\bar{a}$ is "not a". Now expand the sums over x_2:

$$U = \sum_{x_1=0}^{1} \left(|x_1, 0, f(x_1, 0)\rangle\langle x_1, 0, 0| + |x_1, 0, \bar{f}(x_1, 0)\rangle\langle x_1, 0, 1| + |x_1, 1, f(x_1, 1)\rangle\langle x_1, 1, 0| + |x_1, 1, \bar{f}(x_1, 1)\rangle\langle x_1, 1, 1|\right)$$

At this point we can use the fact that f does not depend on x_1 but only on x_2. Thus $f(x_1, 0) = 0$, $\bar{f}(x_1, 0) = 1$, $f(x_1, 1) = 1$, and $\bar{f}(x_1, 1) = 0$. Substituting this in we find

$$U = \sum_{x_1=0}^{1} (|x_1, 0, 0\rangle\langle x_1, 0, 0| + |x_1, 0, 1\rangle\langle x_1, 0, 1| + |x_1, 1, 1\rangle\langle x_1, 1, 0| + |x_1, 1, 0\rangle\langle x_1, 1, 1|)$$

Finally we can expand the sum over x_1:

$$\begin{aligned} U = {} & |0, 0, 0\rangle\langle 0, 0, 0| + |0, 0, 1\rangle\langle 0, 0, 1| + |0, 1, 1\rangle\langle 0, 1, 0| + |0, 1, 0\rangle\langle 0, 1, 1| \\ & + |1, 0, 0\rangle\langle 1, 0, 0| + |1, 0, 1\rangle\langle 1, 0, 1| + |1, 1, 1\rangle\langle 1, 1, 0| + |1, 1, 0\rangle\langle 1, 1, 1| \end{aligned}$$

Wow, what a big messy looking thing. Good thing we usually don't do this expansion but try to manipulate things symbolically.

Now apply this unitary to the three qubit wave function $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Express you answer as a sum over computational basis kets.

Solution: We need to calculate

$$U \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

To do this, first note that this is the same as

$$U \frac{1}{2\sqrt{2}} (|00\rangle \otimes (|0\rangle - |1\rangle) + |01\rangle \otimes (|0\rangle - |1\rangle) + |10\rangle \otimes (|0\rangle - |1\rangle) + |11\rangle \otimes (|0\rangle - |1\rangle))$$

So now we need to calculate things like

$$U\frac{1}{2\sqrt{2}}|00\rangle \otimes (|0\rangle - |1\rangle)$$

which is equal to

$$U\frac{1}{2\sqrt{2}}|00\rangle \otimes (|0\rangle - |1\rangle) = \frac{1}{2\sqrt{2}}(U|0,0,0\rangle + U|0,0,1\rangle)$$

We can use the expansion in the first part of this problem to calculate $U|0,0,0\rangle$. Or we can recall that $U|x_1,x_2,y\rangle = |x_1,x_2,y \oplus f(x_1,x_2)\rangle$. Thus $U|0,0,0\rangle = |0,0,0 \oplus f(0,0)\rangle = |0,0,0\rangle$. Similarly $U|0,0,1\rangle = |0,0,1 \oplus f(0,0)\rangle = |0,0,1\rangle$. Putting these together we find that

$$U\frac{1}{2\sqrt{2}}|00\rangle \otimes (|0\rangle - |1\rangle) = \frac{1}{2\sqrt{2}}\left(|0,0,0\rangle - |0,0,1\rangle\right) = |00\rangle \otimes (|0\rangle - |1\rangle)$$

Next we do the same thing, but for

$$U\frac{1}{2\sqrt{2}}|01\rangle \otimes (|0\rangle - |1\rangle)$$

Now we need to calculate the terms $U|0,1,0\rangle$ and $U|0,1,1\rangle$. We do this: $U|0,1,0\rangle = |0,1,0 \oplus f(0,1)\rangle = |0,1,1\rangle$ and $U|0,1,1\rangle = |0,1,1 \oplus f(0,1)\rangle = |0,1,0\rangle$, using the definition of f. So we obtain

$$U\frac{1}{2\sqrt{2}}|01\rangle \otimes (|0\rangle - |1\rangle) = \frac{1}{2\sqrt{2}}(|0,1,1\rangle - |0,1,0\rangle) = -\frac{1}{2\sqrt{2}}|01\rangle \otimes (|0\rangle - |1\rangle)$$

Continuing in a similar fashion, we can do the other two terms. If we do this we obtain

$$\begin{aligned} U\frac{1}{2\sqrt{2}}|10\rangle \otimes (|0\rangle - |1\rangle) &= \frac{1}{2\sqrt{2}}|10\rangle \otimes (|0\rangle - |1\rangle) \\ U\frac{1}{2\sqrt{2}}|11\rangle \otimes (|0\rangle - |1\rangle) &= -\frac{1}{2\sqrt{2}}|11\rangle \otimes (|0\rangle - |1\rangle) \end{aligned}$$

Back to what we were originally trying to calculate:

$$U\frac{1}{2\sqrt{2}}\left(|00\rangle \otimes (|0\rangle - |1\rangle) + |01\rangle \otimes (|0\rangle - |1\rangle) + |10\rangle \otimes (|0\rangle - |1\rangle) + |11\rangle \otimes (|0\rangle - |1\rangle)\right)$$

We've calculated the action of U on all of these terms:

$$\begin{aligned} &U\frac{1}{2\sqrt{2}}\left(|00\rangle \otimes (|0\rangle - |1\rangle) + |01\rangle \otimes (|0\rangle - |1\rangle) + |10\rangle \otimes (|0\rangle - |1\rangle) + |11\rangle \otimes (|0\rangle - |1\rangle)\right) \\ &= \frac{1}{2\sqrt{2}}\left(|00\rangle \otimes (|0\rangle - |1\rangle) - |01\rangle \otimes (|0\rangle - |1\rangle) + |10\rangle \otimes (|0\rangle - |1\rangle) - |11\rangle \otimes (|0\rangle - |1\rangle)\right) \end{aligned}$$

Notice the new minus signs. Since the last qubit in our sum is always in the same state, we can write this answer as

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

which is our nice beautiful answer. We could have gotten this faster by using the phase kickback trick:

$$\begin{aligned} &U\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}((-1)^{f(0,0)}|00\rangle + (-1)^{f(0,1)}|01\rangle + (-1)^{f(1,0)}|10\rangle + (-1)^{f(1,1)}|11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}((-1)^{0}|00\rangle + (-1)^{1}|01\rangle + (-1)^{0}|10\rangle + (-1)^{1}|11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

Finally, apply two Hadamards to the first two qubits of this resulting state. What is the resulting computational basis state for these first two qubits?

Solution: The first two qubits are, before we apply the Hadamards, have the wave function

$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

So we want to calculate

$$H \otimes H \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

The easy way to do this is to note that

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

Thus

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

But $H \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |0\rangle$ and $H \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |1\rangle$. Thus

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

Which, as claimed in class is exactly $a = (0, 1)$!

2. Suppose that we run Simon's algorithm for a 5 bit function. We obtain the four bitstrings, 01100, 11010, 00111, and 0001. Remember that these all satisfy $y \cdot s = 0 \bmod 2$. What is the hidden xor mask s?

Solution: We are trying to find $s = (s_1, s_2, s_3, s_4, s_5)$. The four equations are

$$\begin{aligned}
(0,1,1,0,0) \cdot (s_1, s_2, s_3, s_4, s_5) &= 0 \bmod 2 \\
(1,1,0,1,0) \cdot (s_1, s_2, s_3, s_4, s_5) &= 0 \bmod 2 \\
(0,0,1,1,1) \cdot (s_1, s_2, s_3, s_4, s_5) &= 0 \bmod 2 \\
(0,0,0,0,1) \cdot (s_1, s_2, s_3, s_4, s_5) &= 0 \bmod 2
\end{aligned}$$

or, calculating these products:

$$\begin{aligned}
s_2 + s_3 &= 0 \bmod 2 \\
s_1 + s_2 + s_4 &= 0 \bmod 2 \\
s_3 + s_4 + s_5 &= 0 \bmod 2 \\
s_5 &= 0 \bmod 2
\end{aligned}$$

So we already know, write off the bat, that $s_5 = 0$. Substituting this into the remaining equations reduces them to

$$\begin{aligned}
s_2 + s_3 &= 0 \bmod 2 \\
s_1 + s_2 + s_4 &= 0 \bmod 2 \\
s_3 + s_4 &= 0 \bmod 2
\end{aligned}$$

Now suppose that $s_4 = 0$. Then the last of the above equations implies $s_3 = 0$. But $s_3 = 0$ implies, via the first equation, that $s_2 = 0$. Finally the second equation then implies that $s_1 = 0$. So if $s_4 = 0$ we get the $s = 0$ solution, which is not what we are looking for. So try $s_4 = 1$. The last equation $s_3 + s_4 = 0 \bmod 2$, now implies that $s_3 = 1$. Similarly the first equation $s_2 + s_3 = 0 \bmod 2$ now implies that $s_2 = 1$. Finally the second equation now implies that $s_1 = 0$. Thus we have found that $s_1 = s_2 = s_3 = s_4 = 1$ and $s_5 = 0$. So our xor mask is $s = (0, 1, 1, 1, 0)$.