Homework 28

Joe Baker, Brett Schreiber, Brian Knotten

March 30, 2018

51

Let f be the function passed as input to Simon's algorithm. When Simon's algorithm returns $a = 0$ it is claiming that the function from $\{0,1\}^n \to \{0,1\}^n$ is a permutation. During the measurement of the first n bits in Simon's algorithm, you get a uniformly distributed y at random such that $y * a = 0$. Since $a = 0$ in this case, you get a uniformly distributed measurement of y. If f is a permutation, then there is a uniform distribution that y in the range of f is chosen from input x, so Simon's algorithm correctly handles the case where $a = 0$.

52

a

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

b

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

c

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

d

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} a+b+c+d \\ a-b+c-d \\ a+b-c-d \\ a-b-c+d \end{bmatrix}$$

e

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \sqrt{a^2+b^2} \\ \sqrt{c^2+d^2} \end{bmatrix} = \begin{bmatrix} \sqrt{a^2+b^2} + \sqrt{c^2+d^2} \\ \sqrt{a^2+b^2} - \sqrt{c^2+d^2} \end{bmatrix}$$

f

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \sqrt{a^2+b^2} \\ \sqrt{c^2+d^2} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \sqrt{a^2+c^2} \\ \sqrt{b^2+d^2} \end{bmatrix} = \begin{bmatrix} \sqrt{a^2+b^2} + \sqrt{c^2+d^2} \\ \sqrt{a^2+b^2} - \sqrt{c^2+d^2} \end{bmatrix} \begin{bmatrix} \sqrt{a^2+c^2} + \sqrt{b^2+d^2} \\ \sqrt{a^2+c^2} - \sqrt{b^2+d^2} \end{bmatrix} = \begin{bmatrix} a+b+c+d \\ a-b+c-d \\ a+b-c-d \\ a-b-c+d \end{bmatrix}$$