1 The Chernoff bound

1.1

Define the random variable X_i to represent the i-th coin toss. Let $X_i = 1$ when the coin is heads, and $X_i = 0$ when the coin is tails. Then for n coin flips, the sum $\langle X\rangle = \sum \langle X_i\rangle = 2n/3$.

If less than half of the flips come out heads, then $X < n/2$. We can use the Chernoff bound to estimate the probability of such an event. We will use

$$Pr(X \leq (1-\epsilon)\mu) \leq \exp(-\epsilon^2\mu/2)$$

We need to find ϵ. We set $n/2 = (1-\epsilon)\mu = (1-\epsilon)2n/3$, and find $\epsilon = 1/4$. Then

$$\begin{aligned} Pr(X \leq n/2) &\leq \exp(-\frac{2n}{2 \cdot 16 \cdot 3}) \\ &= \exp(-n/48) \\ n &= -48 \ln(Pr(X \leq n/2)) \end{aligned}$$

Setting $Pr(X \leq n/2) = 10^{-4}$, we estimate $n \approx 442$.

1.2

We can also solve the problem exactly. The probability of a *particular* length n sequence of flips containing exactly k heads is just $(2/3)^k(1/3)^{n-k}$. There are, however, $\binom{n}{k}$ such sequences all containing k heads, so the total probability of finding exactly k heads in n flips is

$$P(k) = \binom{n}{k}\left(\frac{2}{3}\right)^k\left(\frac{1}{3}\right)^{n-k}$$

and then

$$P(X < n/2) = \sum_{k=0}^{n/2-1}\binom{n}{k}\left(\frac{2}{3}\right)^k\left(\frac{1}{3}\right)^{n-k}$$

Plugging this sum into Mathematica to evaluate numerically gives $n \approx 110$ for $P(X < n/2) = 10^{-4}$.

2 The quantum half-adder

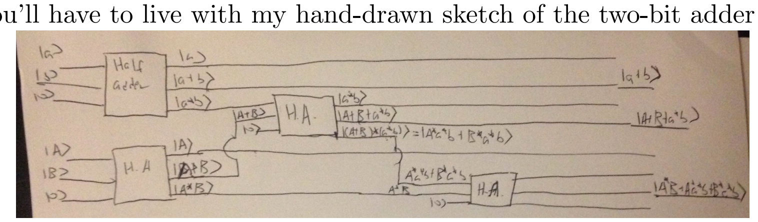
2.1

Adding modulo-two works more or less like adding in base 10. If I add two one-bit numbers a and b, I need to carry a bit only if both a and b are 1. Another way of saying this is that the carry bit is $a * b$ which equals 1 only if both a and b are 0.

If I want to add two two bit numbers, Aa and Bb, the first bit from the addition just gives $a+b$. The carry is $a*b$, so the second bit in the addition is $a*b+A+B$. You can tell by inspection that I will need a carry bit if any two of $(a*b)$, B, and A are 1. A way of writing this is that the carry bit is $(A*B+A*a*b+B*a*b)$.

2.2

LaTeX-ing quantum circuits (or any circuits for that matter) can be a pain, so you'll have to live with my hand-drawn sketch of the two-bit adder circuit.



2.3

We need 8 total qubits. 4 for representing the input, and 4 ancillary qubits.

2.4

The tracking is basically done on the figure.

2.5

If one adds 10 to 11, the output of the circuit is, in descending order vis-a-vis the figure:

$$|0\rangle|1\rangle|0\rangle|0\rangle|1\rangle|0\rangle|1\rangle|0\rangle$$

3 Universality

3.1

We can do this with just a simple Taylor expansion to second order in ϵ.

$$\begin{aligned} U_X &= \exp i\epsilon X \approx 1 + i\epsilon X - (\epsilon^2/2)X^2 \\ U_Y &= \exp i\epsilon Y \approx 1 + i\epsilon Y - (\epsilon^2/2)Y^2 \end{aligned}$$

Note that $X^2 = Y^2 = I$. Now get ready for a bunch of algebra. To simplify things, I will drop everything higher order than ϵ^2 as soon as possible. Let's do this piece by piece.

$$\begin{aligned}
U_Y U_X &\approx (1 + i\epsilon Y - \epsilon^2/2)(1 + i\epsilon X - \epsilon^2/2) \\
&\approx (1 + i\epsilon(X+Y) - \epsilon^2 YX - \epsilon^2) \\
U_X^\dagger U_Y U_X &\approx (1 - i\epsilon X - \epsilon^2/2)(1 + i\epsilon(X+Y) - \epsilon^2 YX - \epsilon^2) \\
&\approx 1 + i\epsilon(X+Y) - \epsilon^2 YX - \epsilon^2 - i\epsilon X + \epsilon^2 X(X+Y) - \epsilon^2/2 \\
&= 1 + i\epsilon Y + \epsilon^2 [X, Y] - \epsilon^2/2 \\
&= 1 + i\epsilon Y + 2i\epsilon^2 Z - \epsilon^2/2 \\
U_Y^\dagger U_X^\dagger U_Y U_X &\approx (1 - i\epsilon Y - \epsilon^2/2)(1 + i\epsilon Y + 2i\epsilon^2 Z - \epsilon^2/2) \\
&\approx 1 + i\epsilon Y + 2i\epsilon^2 Z - \epsilon^2/2 - i\epsilon Y + \epsilon^2 Y^2 - \epsilon^2/2 \\
&= 1 + 2i\epsilon^2 Z \\
&\approx \exp(2i\epsilon^2 Z)
\end{aligned}$$

3.2

4 Measurement

4.1

In general, the measurement operators for some observable are projectors onto the eigenvectors of the observable. In our case, our observable is

$$\begin{aligned}
\hat{n} \cdot \vec{\sigma} &= \begin{pmatrix} n_z & n_x - i n_y \\ n_x + i n_y & -n_z \end{pmatrix} = \begin{pmatrix} \cos(\theta) & \sin(\theta)(\cos(\phi) - i\sin(\phi)) \\ \sin(\theta)(\cos(\phi) + i\sin(\phi)) & -\cos(\theta) \end{pmatrix} \\
&= \begin{pmatrix} \cos(\theta) & e^{-i\phi}\sin(\theta) \\ e^{i\phi}\sin(\theta) & -\cos(\theta) \end{pmatrix}
\end{aligned}$$

with the constraint that $\hat{n}$ is a unit vector with real coefficients. Since a later part of this problem wants us to use spherical coordinates, I will go ahead and write $\hat{n}$ in polar coordinates from the start.

Diagonalizing this matrix isn't hard, but I'm not good at algebra so we'll just plug it into Mathematica to save us the heartbreak. There are two eigenvectors. One has eigenvalue +1, which I denote $|n+\rangle$, and one has eigenvalue −1, which I'll call $|n-\rangle$. The answers are:

$$\begin{aligned}
|n+\rangle &= \frac{1}{\sqrt{\cot^2(\theta/2) + 1}} \begin{pmatrix} e^{-i\phi}\cot(\theta/2) \\ 1 \end{pmatrix} \\
|n-\rangle &= \frac{1}{\sqrt{\tan^2(\theta/2) + 1}} \begin{pmatrix} -e^{-i\phi}\tan(\theta/2) \\ 1 \end{pmatrix}
\end{aligned}$$

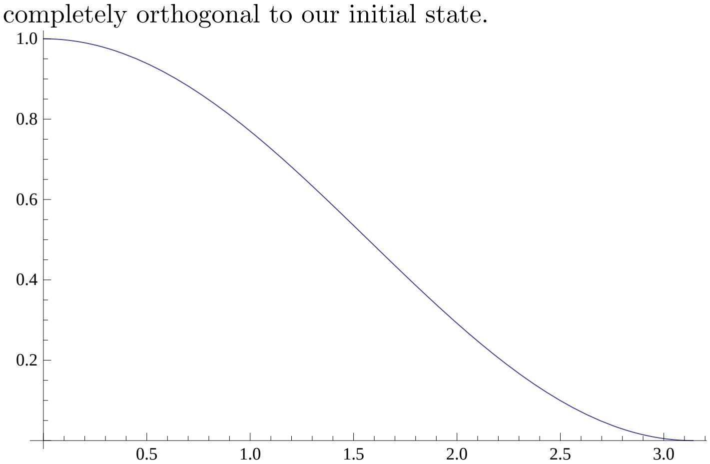
The measurement operators are $|n+\rangle\langle n+|$ and $|n-\rangle\langle n-|$.

4.2

For this part, we need to know $|\langle 0|n+\rangle|^2$. This is just

$$|\langle 0|n+\rangle|^2 = \frac{\cot^2(\theta/2)}{\cot^2(\theta/2)+1}$$

I've plotted this probability as a function of θ from 0 to π. This has the behavior we should expect: if $\theta = 0$, $|n+\rangle = |0\rangle$ up to a phase. If $\theta = \pi$, $|n+\rangle = |1\rangle$, and is completely orthogonal to our initial state.



4.3

After the measurement, the state is either $|n+\rangle$, or $|n-\rangle$, depending on the measurement result.