Homework #4

Due: March 5, 2021 **Points:** 100

Questions

1. (*25 points*) Suppose composite machine catdog (see Section 9.4.1) receives no HIGH inputs. Does it emit the same value from the left and the right? If so, prove it; if not, give a counterexample.

2. (*25 points*) Consider again the algorithm in Figure 9–7. The power used is another side channel for most instantiations of this algorithm. Explain how this side channel works. How might you add sufficient noise to it to render it unusable?

3. (*15 points*) Prove that for $n = 2$, $H(X)$ is maximal when $p_1 = p_2 = \frac{1}{2}$.

4. (*15 points*) Consider the statement

   if $(x = 1)$ **and** $(y = 1)$ **then** $z := 1$

   where x and y can each be 0 or 1, with both equally likely and z is initially 0. Compute the conditional probabilities $H(x|z')$ and $H(y|z')$.

5. (*20 points*) Let $L = (S_L, \leq_L)$ be a lattice. Define:

   (a) $S_{IL} = \{[a,b] \mid a,b \in S_L \wedge a \leq_L b\}$

   (b) $\leq_{IL} = ([a_1,b_1],[a_2,b_2]) \mid a_1 \leq_L a_2 \wedge b_1 \leq_L b_2$

   (c) $lub_{IL}([a_1,b_1],[a_2,b_2]) = (lub_L(a_1,a_2), lub_L(b_1,b_2))$

   (d) $glb_{IL}([a_1,b_1],[a_2,b_2]) = (glb_L(a_1,a_2), glb_L(b_1,b_2))$

   Prove that the structure $IL = (S_{IL}, \leq_{IL})$ is a lattice.