1 Practice Problems

1. Create an arithmetic circuit that takes signals x_1, x_2, …, x_n and is satisfied if *at least* one signal is 0.

   we note that this is effectively the same as saying $\sum_{i=1}^{n} x_i \leq n-1$

   we construct the circuit:

   $$\sum_{i=1}^{n} 2^i * x_i = \sum_{i=1}^{n} x_i$$

   note this assumes divisibility by 2.

2. Create an arithmetic circuit that takes signals x_1, x_2, …, x_n and is satisfied if all signals are 1.

   $$\sum_{i=1}^{n} x_i - n = 0$$

3. A bipartite graph is a graph that can be colored with two colors such that no two neighboring nodes share the same color. Devise an arithmetic circuit scheme to show you have a valid witness of a 2-coloring of a graph. Hint: the scheme in this tutorial needs to be adjusted before it will work with a 2-coloring. TODO

4. Create an arithmetic circuit that constrains k to be the maximum of x, y, or z. That is, k should be equal to x if x is the maximum value, and same for y and z.

5. Create an arithmetic circuit that takes signals x_1, x_2, …, x_n, constrains them to be binary, and outputs 1 if *at least* one of the signals is 1. Hint: this is trickier than it looks. Consider combining what you learned in the first two problems and using the NOT gate.

6. Create an arithmetic circuit to determine if a signal v is a power of two (1, 2, 4, 8, etc). Hint: create an arithmetic circuit that constrains another set of signals to encode the binary representation of v, then place additional restrictions on those signals.

7. Create an arithmetic circuit that models the Subset sum problem (link). Given a set of integers (assume they are all non-negative), determine if there is a subset that sums to a given value k. For example, given the set $\{3, 5, 17, 21\}$ and $k = 22$, there is a subset $\{5, 17\}$ that sums to 22. Of course, a subset sum problem does not necessarily have a solution. Use a "switch" that is 0 or 1 if a number is part of the subset or not.

8. The covering set problem starts with a set $S = \{1, 2, \ldots, 10\}$ and several well-defined subsets of S, for example: $\{1, 2, 3\}$, $\{3, 5, 7, 9\}$, $\{8, 10\}$, $\{5, 6, 7, 8\}$, $\{2, 4, 6, 8\}$, and asks if we can take at most k subsets of S such that their union is S. In the example problem above, the answer for $k = 4$ is true because we can use $\{1, 2, 3\}$, $\{3, 5, 7, 9\}$, $\{8, 10\}$, $\{2, 4, 6, 8\}$. Note that for each problem, the subsets we can work with are determined at the beginning. We cannot construct the subsets ourselves. If we had been given the subsets $\{1, 2, 3\}$, $\{4, 5\}$ $\{7, 8, 9, 10\}$ then there would be no solution because the number 6 is not in the subsets. On the other hand, if we had been given $S = \{1, 2, 3, 4, 5\}$ and the subsets $\{1\}$, $\{1, 2\}$, $\{3, 4\}$, $\{1, 4, 5\}$ and asked can it be covered with $k = 2$ subsets, then there would be no solution. However, if $k = 3$ then a valid solution would be $\{1, 2\}$, $\{3, 4\}$, $\{1, 4, 5\}$. Our goal is to prove for a given set S and a defined list of subsets of S, if we can pick a set of subsets such that their union is S. Specifically, the question is if we can do it with k or fewer subsets. We wish to prove we know which k (or fewer) subsets to use by encoding the problem as an arithmetic circuit.