Exercise 6: Containment

Task 1: Containing Choice

The goal in this exercise is to prove Lemma 6.5.

a) Show the equivalence stated in the lemma.

b) Construct a k-bit MUX_M implementation out of two $(k-1)$-bit MUX_M implementations and a CMUX. (Hint: To show correctness, make a case distinction on the k^{th} control bit, which is fed to the CMUX.)

c) What is the size of the resulting MUX_M implementation when applying the construction from b) recursively?

Task 2: Copy and Conquer

Masking registers are registers that have somewhat predictable behavior when storing a metastable bit. A *mask*-0 register R has the following behavior. Like an ordinary register, if R stores a bit $b \in \{0,1\}$, then every time the value of R is read, it will return b. If the bit stored in R is M, then every sequence of accesses to R will return a sequence of values of the form $00\cdots0M11\cdots1$. In particular, every sequence of accesses to R will return a sequence of values containing at most a single M.

a) Let $f\colon \{0,1\}^n \to \{0,1\}$ be a function, and suppose $x \in \{0,1,M\}^n$ satisfies $f_\text{M}(x) \neq M$. Let C be an arbitrary (not necessarily metastability containing!) circuit implementing f. Suppose the individual bits of x are stored in mask-0 registers, and let $x^{(1)}, x^{(2)}, \ldots, x^{(2n+1)}$ denote the values of x read by a sequence of accesses to the registers storing x. Finally, for each $i \in \{1,2,\ldots,2n+1\}$, define $y_i = C(x^{(i)})$. Show that the value $f_\text{M}(x)$ can be inferred from $y_1, y_2, \ldots, y_{2n+1}$.

b) Come up with a small circuit that sorts its n inputs according to the total order $0 \leq \text{M} \leq 1$. That is, devise a circuit C with n inputs and n outputs such that if $y = C(x)$ then we have $y_1 \leq y_2 \leq \cdots \leq y_n$, where y has the same number of 0s, 1s, and Ms as x. (Hint: Figure out a solution sorting two values and then plug it into a binary sorting network to get the general circuit. You don't have to (re)invent sorting networks, you may just point to a reference.)

c) Combine a) and b) to derive a circuit implementing f_M from any (non-containing) circuit implementing f! Your solution should only be by a factor of $n^{\mathcal{O}(1)}$ larger than to the non-containing solution.

Task 3*: Clocked Circuits

a) How would a model for clocked circuits based on the same worst-case assumptions look like? (Hint: Reading up on it is fine.)

b) Standard registers, when being read, will output M if they're internally metastable and 0 or 1, respectively, when they're stable. Show that they add no power in terms of the functions that can be computed! (Hint: Unroll the circuit, i.e., perform the multi-round computation in a single round with a larger circuit.)

c) In Task 2, you saw that masking registers allow for more efficient metastability-containing circuits. Show that they are also computationally more powerful, i.e., they can compute functions that cannot be computed with masking registers! (Hint: You already used this in Task 2!)