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 allow to mask internal metastability, resulting in, e.g., the sequence $0\ldots0\text{M}1\ldots1$ when reading sequentially from a mask-0 register. The key property for this exercise is that there is only a single M read from the register. We consider a function $f\colon\{0,1\}^n\to\{0,1\}$ in this exercise.

a) Suppose inputs are stored in masking registers, which we read $2n+1$ times, each time making a separate copy $x^{(i)}$, $i\in\{1,\ldots,2n+1\}$, of the input x. If $f_\text{M}(x)\neq\text{M}$, what can you say about the collection of $2n+1$ outputs generated from feeding each $x^{(i)}$ to a copy of a (non-containing) circuit implementing f?

b) Come up with a small circuit that sorts its n inputs according to the total order $0\leq\text{M}\leq1$. (Hint: Figure out a solution sorting two values and then plug it into a 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!)