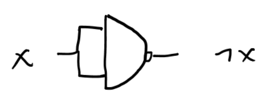
2.111/8.370/18.435 Problem Set 1 Solutions

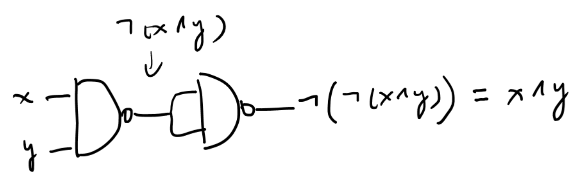
Due: September 24, 2015

Notations: $\wedge$ = AND; $\vee$ = OR; $\neg$ = NOT; Algebra is over $GF(2)$ (Boolean algebra).

1. **Show that NAND and COPY suffice to generate AND, OR, NOT and COPY (possibly with extra inputs).**



Notice that $x \wedge y = \neg(\neg(x \wedge y))$:



Notice that $x \vee y = \neg(\neg x \wedge \neg y)$ (De Morgan's law), OR can be constructed using NOT and AND given above.

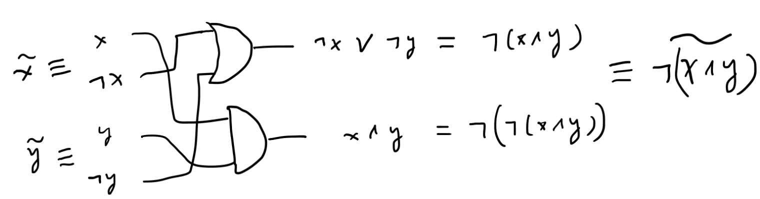
So {NAND, COPY} is universal.

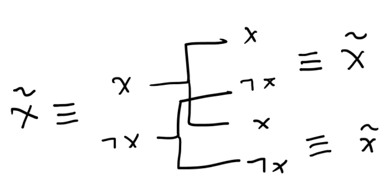
2. **Show that AND, OR and COPY don't suffice to produce NOT.**

Notice that AND, OR and COPY gates are monotone increasing: the output of $x = 1$ is never smaller than that of $x = 0$, where x is some input variable. This property holds for any circuit composed of AND, OR and COPY. Thus any such circuit cannot produce non-monotone gates, including NOT.

3. **Show that with *dual-rail encoding*, using {AND, OR, COPY} on the physical (original) bits, one can perform any logical function on the logical bits.**

As shown in Problem 1, {NAND, COPY} is universal. Logical NAND and COPY can be constructed as follows:



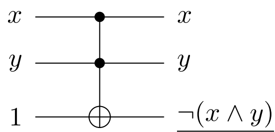


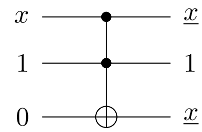
4. **Can one perform universal circuit computation using CNOTs and additional inputs? If yes, give construction. If no, why not?**

   No. One simple argument is that CNOT is a linear map while AND, OR are not. More explicitly, notice that e.g. $x \wedge y = xy$ (non-linear) while $\mathrm{CNOT}(x, y) = (x, x + y)$ (bilinear). The non-linear xy term in AND can never be achieved by wiring up CNOTs and add extra inputs because all these operations are linear. Similar argument follows for OR.

5. **Show that CCNOTs (Toffoli gates) are universal on their own.**

   As shown in Problem 1, {NAND, COPY} is universal. We can use CCNOTs to construct NAND and COPY as follows:





6. **Show that Fredkin gate (C-SWAP) + wire + extra bits is universal.**

   We can use Fredkin gates to construct AND, OR, NOT and COPY using the following circuits: