Reading and Exercises:

This is the last problem set before the take-home final. Read the “Advanced” lectures through A7.

(1) Show that for any fixed prime $p$, ACC$^0[p]$ can simulate a mod-$p^2$ gate. *Hint:* What can you say about the congruence of $n$-choose-$m$ modulo $p$? How about when $m = p$ and $n = pk$ for some integer $k$?

Then show this for circuits of Boolean and mod-$p^e$ gates, for $e \geq 3$. For non-prime $m$ and $e \geq 2$, can ACC$^0[m]$ circuits simulate a mod-$m^e$ gate? (18 + 18 + 18 = 54 pts.)

(2) Finish the details of proving that mSO[$\leq$] represents exactly the class REG of regular languages. It suffices to do the forward direction, as lecture showed the main point of the converse where unrestricted Kleene star introduces a second-order existential quantifier. Use marked words in the “layered” style of lectures, and prove by induction on standard regular expressions a lemma showing that chopping off the bottom layer always simulates an existential quantifier on the corresponding variable. Note that this induction needs no case for $\cap$ or $\sim$ (i.e., complements), but the regular languages are closed under both operations—so why isn’t this lemma violated by the counterexample for $\cap$ shown in lecture. (24 pts. Possible open-ended extra credit if you explore other possible ways to circumvent the $\cap$ problem, and/or whether there are cases of small FO[$\leq$] formulas that require large SF expressions.)

(3) Advanced lecture A4, exercises on page 13, 3 and 4: write formulas in FO($+,\ast$) that represent the numeric predicates “$y$ is a power of 2” and “$y$ is a power of 2 and when $x$ is written as a sum of powers of 2, $y$ appears in that sum.” (6+12 = 18 pts.)

(4) Suppose that $R$ is a *-free regular expression over the “tandem alphabet” $\Sigma \times \Sigma$. Suppose that for all $x \in \Sigma^*$ there is a unique $y \in \Sigma^*$, $|y| = |x|$, such that $[y]$ matches $R$. (Recall that $[y] = (x_1,y_1)(x_2,y_2)\cdots(x_n,y_n)$ over $\Sigma \times \Sigma$.) Show that the function $f_R(x) = y$ is computable by DLOGTIME-uniform AC$^0$ circuits. (18 pts.)

(5) Same problem as (4), except that now the basis includes “dominoes” $(c,\epsilon)$ where $c \in \Sigma$ but $\epsilon$ is the empty string, and you are to classify $f_R$ into TC$^0$. Thus $R$ becomes a true “2D regular expression” over $\Sigma^* \times \Sigma^*$, and $y$ need no longer have the same length as $x$. (12 pts., for 126 regular-credit points on the set. For 12 pts. extra credit, can you find an $R$ for which $f_R$ is complete for TC$^0$ under AC$^0$ reductions?)

(X) Same problem as (4), except that the basis also includes $(\epsilon,c)$. Now what? (I don’t know the answer, and wonder if $f_R$ is even guaranteed to be computable now... Points ad-lib.)