Problem Set 1 Due Mon. 2/13

Reading and Exercises:

For next week, please read lectures B01–B09. Looking ahead to the following week, from the Allender-Loui-Regan notes, please begin the section 29.4 on representing languages via formal systems of logic. this material, in tandem with lecture A01, will go more slowly.

1. Suppose you are given access to a big unknown directed acyclic graph \( G \), with nodes labeled \( 1 \ldots N \). Suppose your only means of getting information about \( G \) is to make a query \( P(i, j) \), which returns \text{true} if and only if there is a path from node \( i \) to node \( j \) in \( G \). Note that \( P(i, i) \) is always true since zero steps counts as a path, and you are of course allowed to test \( i \neq j \).

   (a) Can you define an algorithm by looping from 1 to \( N \) that will decide \( E(u, v) \), i.e. whether there is an edge from node \( u \) to node \( v \)? If \( P(u, v) = 0 \) of course \( E(u, v) = 0 \), but what do you do if \( P(u, v) = 1 \)?

   (b) Now suppose the graph is \textit{leveled}, meaning the set \( V \) of nodes is partitioned into disjoint subsets \( V_0 \cup V_1 \cup \ldots \cup V_d \) so that each edge goes from \( V_{i-1} \) to \( V_i \) for some \( i \). Now can you define such an algorithm?

   (c) Assuming leveled-ness, write a logical formula involving \( P(\cdot, \cdot) \) that defines \( E(u, v) \). You may use \( = \) and \( \neq \) but may not assume an ordering of the nodes by their labels.

   (d) Do you think you can write down a formula involving \( E(\cdot, \cdot) \) that defines \( P(i, j) \)? Just try out some reasoning. \( (6+6+6+3 = 21 \text{ pts.}) \)

2. Show that there are \( O(n) \)-size \( \text{NC}^1 \) circuits that compute the addition of two length-\( n \) binary numbers. This is Exercise 7 in lecture B02, and for a hint it embodies exercise 3 on the same page. You may reference results proved in class, but it is helpful to include the reference as part of a sketch of the circuits, not just in prose. \( (18 \text{ pts.}) \)

3. The \textit{subset-sum} problem is, given a set \( S \) of \( n \)-many positive integers and a target integer \( t \), is there a subset \( T \) of \( S \) whose members sum to \( t \)? The integers are in standard binary notation, and sometimes (not now) one restricts them to have \( O(\log n) \) size. Show that this problem belongs to \( \text{NP} \), indeed to \textit{“nondeterministic AC}^1\textit{”} in the sense that its witness predicate belongs to \( \text{AC}^1 \) (which is a deterministic class). Later we will improve this, using machinery in lectures A01–A06. \( (18 \text{ pts.}) \)

4. Show that the language of undirected graphs that contain a triangle belongs to \( \text{AC}^0 \). You may use either an adjacency-matrix or edge-list representation for the graph, and showing \( \text{P-uniformity} \) of the circuits is enough. \( (12 \text{ pts.}) \)

5. (Open-ended question, meaning: the professor has not had time to solve it before assigning it.) Let \( C \) be a circuit of NAND gates of depth \( d \) and size \( s \) (in wires). Show how to create an equivalent circuit \( C' \) of NAND gates that is \textit{leveled}, as in question 1(c). You are allowed to make \( C' \) a \textit{“double-rail”} circuit, meaning the negations \( \bar{x}_i \) of the variables are also input gates. Can you do so without multiplying the depth by a factor of 2 or more, i.e. so that there is a fixed constant \( k \) (independent of \( C \)) such that the depth \( d' \) of \( C' \) always satisfies \( d' \leq d + k \)? Also say what the size increase is. \( (21 \text{ base points for a linear depth expansion, making 90 regular-credit points on the set, plus unknown extra-credit if you can see what I'm not seeing, if any.}) \)