Assignment 1.

Due: 5pm on 16th Feb 2026

1

Exercise 1.2 — Quantifiers. Use the logical quantifiers $\forall$ (for all), $\exists$ (there exists), as well as $\wedge, \vee, \neg$ and the arithmetic operations $+, \times, =, >, <$ to write the following:

a. An expression $\varphi(n, k)$ such that for every natural number n, k, $\varphi(n, k)$ is true if and only if k divides n.

b. An expression $\varphi(n)$ such that for every natural number n, $\varphi(n)$ is true if and only if n is a power of three.

[2]

2

Exercise 1.3 Describe the following statement in English words: $\forall_{n \in \mathbb{N}} \exists_{p>n} \forall a, b \in \mathbb{N} (a \times b \neq p) \vee (a = 1)$.

[1]

3

Exercise 1.13 Give an example of a pair of functions $F, G : \mathbb{N} \to \mathbb{N}$ such that neither $F = O(G)$ nor $G = O(F)$ holds.

[2]

4

Exercise 2.7 Suppose that $R : \mathbb{N} \to \{0,1\}^*$ corresponds to representing a number x as a string of x 1's, (e.g., $R(4) = 1111$, $R(7) = 1111111$, etc.). If x, y are numbers between 0 and $10^n - 1$, can we still multiply x and y using $O(n^2)$ operations if we are given them in the representation $R(\cdot)$? What is the best upper bound you can show?

[4]

5

Exercise 3.5 — XOR is not universal. Prove that for every n-bit input circuit C that contains only XOR gates, as well as gates that compute the constant functions 0 and 1, C is *affine or linear modulo two*, in the sense that there exists some $a \in \{0,1\}^n$ and $b \in \{0,1\}$ such that for every $x \in \{0,1\}^n$, $C(x) = \sum_{i=0}^{n-1} a_i x_i + b \mod 2$.

Conclude that the set $\{XOR, 0, 1\}$ is *not* universal.

[6]

6

Exercise 4.14 — Circuits for threshold. Prove that there is some constant c such that for every $n > 1$, and integers $a_0, \ldots, a_{n-1}, b \in \{-2^n, -2^n + 1, \ldots, -1, 0, +1, \ldots, 2^n\}$, there is a NAND circuit with at most n^c gates that computes the *threshold* function $f_{a_0,\ldots,a_{n-1},b} : \{0,1\}^n \to \{0,1\}$ that on input $x \in \{0,1\}^n$ outputs 1 if and only if $\sum_{i=0}^{n-1} a_i x_i > b$.

[5]

7 a)

Exercise 5.4 — Counting lower bound for multibit functions. Prove that there exists a number $\delta > 0$ such that for every sufficiently large n and every m there exists a function $f : \{0,1\}^n \to \{0,1\}^m$ that requires at least $\delta m \cdot 2^n/n$ gates to compute it.

b) Use part (a) to show the following:

Exercise 5.5 — Size hierarchy theorem for multibit functions. Prove that there exists a number C such that for every n, m and $n+m < s < m \cdot 2^n/(Cn)$ there exists a function $f \in SIZE_{n,m}(C \cdot s) \setminus SIZE_{n,m}(s)$.

[6 + 4]

8

Exercise 5.8 — Random functions are hard. Suppose $n > 1000$ and that we choose a function $F : \{0,1\}^n \to \{0,1\}$ at random, choosing for every $x \in \{0,1\}^n$ the value $F(x)$ to be the result of tossing an independent unbiased coin. Prove that the probability that there is a $2^n/(1000n)$ sized ckt. that computes F is at most 2^{-100}.[14]

[5]

[14] **Hint:** An equivalent way to say this is that you need to prove that the set of functions that can be computed using at most $2^n/(1000n)$ ~~lines~~ gates has fewer than $2^{-100}2^{2^n}$ elements. Can you see why?

9 a)

Exercise 8.5 — Longest Path. Let $LONGPATH : \{0,1\}^* \to \{0,1\}^*$ be the function that on input a string encoding a triple (G, u, v) outputs a string encoding ∞ if u and v are disconnected in G or a string encoding the length k of the *longest simple path* from u to v. Prove that $LONGPATH$ is computable by a Turing machine.

b) Which well known algorithm would you use if I instead asked for the length of the shortest path?

[4+1]

10

Exercise 9.4 — Computable compositions. Suppose that $F : \{0,1\}^* \to \{0,1\}$ and $G : \{0,1\}^* \to \{0,1\}$ are computable functions. For each one of the following functions H, either prove that H is *necessarily computable* or give an example of a pair F and G of computable functions such that H will not be computable. Prove your assertions.

a). $H(x) = 1$ iff $F(x) = 1$ OR $G(x) = 1$.

b). $H(x) = 1$ iff there exist two non-empty strings $u, v \in \{0,1\}^*$ such that $x = uv$ (i.e., x is the concatenation of u and v), $F(u) = 1$ and $G(v) = 1$.

[2+3]

11

Exercise 9.7 — TM Equivalence. Let $EQ : \{0,1\}^* :\to \{0,1\}$ be the function defined as follows: given a string representing a pair (M, M') of Turing machines, $EQ(M, M') = 1$ iff M and M' are functionally equivalent as per Definition 9.14. Prove that EQ is uncomputable.

[5]

Definition 9.14 — Semantic properties. A pair of Turing machines M and M' are *functionally equivalent* if for every $x \in \{0,1\}^*$, $M(x) = M'(x)$. (In particular, $M(x) = \perp$ iff $M'(x) = \perp$ for all x.)