Advanced Algorithms & Complexity (CS G526) Comprehensive Exam, 2023

There are 5 questions in all and total marks are $7+7+7+7+(1+1+5) = 35$. This is an open book exam. You can use any printed or handwritten material. Please show all steps of your solution and give full derivation of your results.

1. Let `LINEQ` denote the set of satisfiable rational linear equations. That is, `LINEQ` consists of the set of all pairs (A,b), where A is an $m \times n$ rational matrix and b is an m-dimensional rational vector, such that $Ax = b$ for some n-dimensional vector x. Prove that `LINEQ` is in **NP**.

2. By making use of efficient algorithms, find the last three digits in the decimal expansion of

$$3^{2023}.$$

3. Let $f : \{0,1\}^* \to \mathbb{N}$ and $\alpha < 1$. An algorithm A is an α-approximation for f if for every x,

$$\alpha f(x) \leq A(x) \leq \frac{f(x)}{\alpha}.$$

   Prove that if there is a polynomial-time algorithm that approximates `#CYCLE` within a factor $1/2$, then $\mathbf{P} = \mathbf{NP}$.

4. Prove that a *Strongly-2-Universal* family of hash functions is also *2-Universal*.

5. Let $\phi(x,y,z) = (\bar{x} \vee y \vee z) \wedge (x \vee \bar{y} \vee z) \wedge (x \vee y \vee \bar{z})$.

   (a) Using arithmetization, find the equivalent polynomial $P_\phi(x,y,z)$ for ϕ.

   (b) Compute

$$K = \sum_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \sum_{b_3 \in \{0,1\}} P_\phi(b_1, b_2, b_3)$$

   (c) Given (ϕ, K) as input, taking the prime $p = 17$, show the complete working of the sum-check protocol.