Name:

COL202: Quiz-1

Maximum marks: 40 Kerberos id:

Instructions.

1. For each problem, you will receive 10% marks for leaving it blank. However, there will be penalty for submitting bogus proofs.

2. Please write your proofs clearly (marks will be deducted for skipping steps, not mentioning which PMI you are using, etc). In case you need make any assumptions, explicitly state what you are assuming.

Notations. The set of natural numbers is denoted by $\mathbb{N}$,[1] rational numbers by $\mathbb{Q}$ and real numbers by $\mathbb{R}$. For any $d \in \mathbb{N}$, let $[d]$ denote the set $\{1, 2, \ldots, d\}$.

Question 1: Fun with Polynomials (15 marks). Let $\mathbb{Q}[x]$ denote the set of all polynomials with rational coefficients (that is, any polynomial of the form $p(x) = p_0 + p_1 \cdot x + p_2 \cdot x^2 + \ldots + p_d \cdot x^d$, where each $p_i \in \mathbb{Q}$). For any non-zero polynomial $p(x) = \sum_{i=0}^{d} p_i \cdot x^i$, $p_d \neq 0$, the degree of the polynomial is d. [2]

Polynomials can be added, subtracted and multiplied. Given two polynomials $g(x), h(x) \in \mathbb{Q}[x]$ with degrees d and ℓ respectively, the degree of $g(x) + h(x)$ and $g(x) - h(x)$ is at most $\max(d, \ell)$. and the degree of $g(x) \cdot h(x)$ is $d + \ell$.

An element $\alpha \in \mathbb{Q}$ is a *rational root* of $p(x)$ if $p(\alpha) = 0$. Finally, we say that a polynomial $h(x)$ divides polynomial $g(x)$ if there exists a polynomial $q(x) \in \mathbb{Q}[x]$ such that $g(x) = h(x) \cdot q(x)$.

1. (10 marks) For any two polynomials $g(x), h(x)$ with degrees d and ℓ respectively such that $\ell > 0$ and $h(x)$ does not divide $g(x)$, show that there exist polynomials $q(x)$ and $r(x)$ such that $g(x) = h(x) \cdot q(x) + r(x)$ and degree of $r(x)$ is less than ℓ. (The polynomials $q(x)$ and $r(x)$ are also unique, but you don't need to prove this part). Use PMI/Strong PMI/WOP to prove this.

2. (5 marks) Use (1) to prove that for any non-zero $f(x) \in \mathbb{Q}[x]$ and $\alpha \in \mathbb{Q}$, α is a rational root of $f(x)$ if and only if $(x - \alpha)$ divides $f(x)$.

   (This can be used to conclude that for any degree d non-zero polynomial, there exist at most d distinct rational roots of f, although you don't need to prove this).

---

[1] $\mathbb{N} = \{1, 2, 3, \ldots\}$

[2] The degree of any non-zero rational constant is 0, and the degree of 0 is defined to be $-\infty$.

Question 2: 'Proving' Some Axioms of Predicate Logic (10 marks). In this problem, we will prove the following statement of predicate logic, using axioms of propositional logic:

Claim 1. *For any $n \in \mathbb{N}$, any **finite** set $\mathcal{D}$ of size n, and any predicate $P : \mathcal{D} \to \{T, F\}$,*

$$\neg\Big(\forall x \in \mathcal{D}.\ P(x)\Big) \equiv \exists x \in \mathcal{D}.\ \neg P(x)$$

You are **only allowed** to use the following axioms (and there should be no 'verbal reasoning').

1. for any $n \in \mathbb{N}$, any finite set $\mathcal{D} = \{d_1, d_2, \ldots, d_n\}$,

$$\Big(\forall x \in \mathcal{D}.\ P(x)\Big) \equiv \Big(P(d_1) \wedge P(d_2) \wedge \ldots \wedge P(d_n)\Big)$$

2. for any $n \in \mathbb{N}$, any finite set $\mathcal{D} = \{d_1, d_2, \ldots, d_n\}$,

$$\Big(\exists x \in \mathcal{D}.\ P(x)\Big) \equiv \Big(P(d_1) \vee P(d_2) \vee \ldots \vee P(d_n)\Big)$$

3. $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$

4. $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$

5. for all $n \in \mathbb{N}$,

$$\Big(A_1 \wedge A_2 \wedge \ldots \wedge A_n \wedge A_{n+1}\Big) \equiv \Big(A_1 \wedge A_2 \wedge \ldots \wedge A_n\Big) \wedge A_{n+1}$$

6. for all $n \in \mathbb{N}$,

$$\Big(A_1 \vee A_2 \vee \ldots \vee A_n \vee A_{n+1}\Big) \equiv \Big(A_1 \vee A_2 \vee \ldots \vee A_n\Big) \vee A_{n+1}$$

7. $Q_1 \equiv Q_2$ if and only if $\neg Q_1 \equiv \neg Q_2$

Prove Claim 1 using induction. Clearly state whether you are using regular/strong induction, followed by the induction predicate, followed by the base case(s) and finally the induction step. In your induction step, you will need to use the axioms stated above. Clearly mention which axiom is used in each step.

Question 3: Les Countables (15 marks). An infinite set $\mathcal{S}$ is countable if there exists a bijection between $\mathbb{N}$ and $\mathcal{S}$. If there exists an injective function $f : \mathbb{N} \to \mathcal{S}$ but there does not exist an injective function $g : \mathcal{S} \to \mathbb{N}$, then we say that the set is uncountable.
In class/tutorials, we proved that the following sets are countable: $\mathbb{Z}$, $\mathbb{N} \times \mathbb{N}$, $\bigcup_{i=1}^{\infty} \mathbb{N}^i$, $\mathcal{T}$ = set of infinite strings with finitely many ones, $\mathcal{F} = \{f : \{0,1\} \to \mathbb{N}\}$.
We also showed that the following sets are uncountable: $\mathbb{R}$, $\mathcal{S}$ = set of all infinite bit strings, $\mathcal{W}$ = set of all infinite bit strings with infinitely many occurrences of 11, $\mathcal{G} = \{f : \mathbb{N} \to \{0,1\}\}$.

Given any function $f : \mathbb{N} \to \mathbb{N}$, we say that f is non-increasing if for all $i, j \in \mathbb{N}$ such that $i < j$, $f(i) \geq f(j)$. Similarly, we say that f is non-decreasing if for all $i, j \in \mathbb{N}$ such that $i < j$, $f(i) \leq f(j)$. Consider the following two sets:

$$\mathcal{S}_1 = \{f : \mathbb{N} \to \mathbb{N} \text{ such that } f \text{ is non-increasing}\}$$

$$\mathcal{S}_2 = \{f : \mathbb{N} \to \mathbb{N} \text{ such that } f \text{ is non-decreasing}\}$$

Is $\mathcal{S}_1$ countably infinite? Is $\mathcal{S}_2$ countably infinite? You must have two claims, one for $\mathcal{S}_1$ and another for $\mathcal{S}_2$. Prove your claims by showing a bijection to one of the sets listed above.