CMSC 250H - Quantifier Review, Proofs, Testing Primes

February 25, 2026

CMSC250H

Quantifiers

Recall the two types of quantification over sets:

1. Existential ($\exists$): "There exists" an element in the set
2. Universal ($\forall$): "For all" of the elements in the set

Remember that these two are inverses of one another

$$\neg\exists \equiv \forall \qquad \neg\forall \equiv \exists$$

Existential quantifiers are a lot weaker than universal quantifiers

Nesting quantifiers

We can nest quantifiers as well:

- Nesting quantifiers of the same type can be joined together:

$$(\exists x \in S)(\exists y \in S) \longrightarrow \exists x, y \in S \quad (\forall x \in S)(\forall y \in S) \longrightarrow \forall x, y \in S$$

- Nesting quantifiers of different types:

$$\exists x \in S(\forall y \in S) \qquad \forall x \in S(\exists x \in S)$$

Nesting Quantifiers of Different Types

The order of existential and universal quantifiers change the meaning of the statement:

1. $\exists x \in S(\forall y \in S) \longrightarrow$ There exists a specific x for all y, i.e its the same x for every single y. Remember y can even be x itself! If we need to differentiate between x and y we can establish that $x \neq y$.
2. $\forall x \in S(\exists y \in S) \longrightarrow$ For each x we have **SOME** y, i.e it can be a different y for each x (it can also be the same one, we don't know). All this says is that for each $x \in S$, some y satisfies a given property (it can even be that $y = x$)

The first statement is a lot stronger, since it establishes a specific x for all elements in the set.

Example

[

Statement] Every real number has a cubed root

Example

Statement

Every real number has a cubed root

$$\forall x \in \mathbb{R}(\exists y \in \mathbb{R})[y^3 = x \wedge y^3 \in \mathbb{R}]$$

Example

What would this statement mean?

Statement

$\exists x \in \mathbb{R}(\forall y \in \mathbb{R})[x = y^3 \wedge y^3 \in \mathbb{R}]$

Example

What would this statement mean?

Statement

$\exists x \in \mathbb{R}(\forall y \in \mathbb{R})[x = y^3 \wedge y^3 \in \mathbb{R}]$

This would mean that there is a real number x such that all the real numbers cubed is equal to that x! Which is clearly not true

What is this statement in English?

Statement

$\forall m \in \mathbb{Z}(\exists n \in \mathbb{Z})[m = n + 5]$

What is this statement in English?

Statement

$\forall m \in \mathbb{Z}(\exists n \in \mathbb{Z})[m = n + 5]$

For any integer m, there is some integer n such that $m = n + 5$

What if we flip the existential and universal quantifier?

Homework 2 Questions

Goal: Quantify a domain, $\mathbb{D}$ so that $\mathbb{D}$ is infinite and has both a least and greatest element.

Homework 2 Questions

Goal: Quantify a domain, $\mathbb{D}$ so that $\mathbb{D}$ is infinite and has both a least and greatest element.

Least Element in $\mathbb{D}$: we want a specific $x \in \mathbb{D}$ so that all other elements of $\mathbb{D}$ are greater than **OR EQUAL** to it, since it could be the case that $y = x$

$$\exists x \in \mathbb{D}(\forall y \in \mathbb{D})[x \leq y]$$

Homework 2 Question 2

Goal: Quantify a domain, $\mathbb{D}$ so that $\mathbb{D}$ is infinite and has both a least and greatest element.

Greatest Element in $\mathbb{D}$: we want a specific $z \in \mathbb{D}$ so that all other elements of $\mathbb{D}$ are less than **OR EQUAL** to it, since it could be the case that $y = x$

$$\exists z \in \mathbb{D}(\forall y \in \mathbb{D})[z \geq y]$$

Homework 2 Questions

Goal: Quantify a domain, $\mathbb{D}$ so that $\mathbb{D}$ is infinite and has both a least and greatest element.

Infinite: There are more than one ways to quantify infinity. Intuitively, infinity means that given any few elements, we can find one that is isn't in those given ones. Some common ways:

$$(\forall x, y \in \mathbb{D})(\exists z \in \mathbb{D})[x < y \implies x < z < y]$$

$$(\forall n \in \mathbb{N})(\exists x_1, x_2, \ldots, x_n \in \mathbb{D})[x_i \neq x_j \text{ for } i < j]$$

Homework 2 Question 3

What do we know about $\mathbb{Z}$ and $\mathbb{Q}$?

Homework 2 Question 3

What do we know about $\mathbb{Z}$ and $\mathbb{Q}$?

The integers are evenly spaced out, with each being ± 1 away from its ”successor/predecessor”.

On the real number line, the rationals are **dense**, meaning you can always find another one in between two of them.

Homework 2 Question 3

How about the real interval $(0, 1)$?

$(0, 1)$ does not include 0 or 1, so we cannot use those in our quantification, since we have to quanitify over elements in the set.

It is also infinite, and we can get arbitrarily close to 0 and 1 without ever reaching them.

Hard to differentiate it from $\mathbb{Q}$ in this case, given the quantification symbols we were allowed to use

CMSC 250H - Quantifier Review, Proofs, Testing Primes

February 25, 2026

CMSC250H

Homework 2 Question

How many cubes are needed to write a number?

What is known:

- Every number is the sum of ≤ 9 cubes
- For sufficiently large numbers we only need ≤ 7 cubes (large meaning > 454)

Unknown:

- It is thought that the number is between 4-7 for sufficiently large numbers, conjectured to be 4.

Proving We Need at Least 4

Can we prove that we need at least 4 cubes to write any number?

Proving We Need at Least 4

Can we prove that we need at least 4 cubes to write any number?

Work in your tables!

Hint: Try computing cubes modulo 9

Proof

Proof.

Consider cubes mod 9

$$1^3 \equiv 1 \mod 9$$
$$2^3 \equiv 8 \mod 9 \equiv -1 \mod 9$$
$$3^3 \equiv 0 \mod 9$$
$$4^3 \equiv 64 \mod 9 \equiv 1 \mod 9$$
$$5^3 \equiv 125 \mod 9 \equiv -1 \mod 9$$
$$6^3 \equiv 0 \mod 9$$
$$7^3 \equiv 343 \mod 9 \equiv 1 \mod 9$$
$$8^3 \equiv 512 \mod 9 \equiv -1 \mod 9$$

Proof

Proof.

Consider cubes mod 9

$$1^3 \equiv 1 \mod 9$$
$$2^3 \equiv 8 \mod 9 \equiv -1 \mod 9$$
$$3^3 \equiv 0 \mod 9$$
$$4^3 \equiv 64 \mod 9 \equiv 1 \mod 9$$
$$5^3 \equiv 125 \mod 9 \equiv -1 \mod 9$$
$$6^3 \equiv 0 \mod 9$$
$$7^3 \equiv 343 \mod 9 \equiv 1 \mod 9$$
$$8^3 \equiv 512 \mod 9 \equiv -1 \mod 9$$

Since every integer is congruent to $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ modulo 9, then all integers cubes are congruent to $\{-1, 0, 1\}$ mod 9 □

Proof

Proof.

We now consider combinations of these 3 residues

$$1+1+1 \equiv 3$$
$$-1+-1+-1 \equiv -3 \equiv 6$$
$$0+0+0 \equiv 0$$
$$-1+-1+1 \equiv -1 \equiv 8$$
$$1+1-1 \equiv 2$$
$$1+-1+0 \equiv 0$$
$$0+0+1 \equiv 1$$
$$0+0+-1 \equiv 8$$
$$0+-1+-1 \equiv -2 \equiv 7$$

Proof

Proof.

So the sum of any 3 cubes is congruent to $\{0, 1, 2, 3, 6, 7, 8\}$ modulo 9.

So we can't write any number that is 4 mod 9 or 5 mod 9 as a sum of three cubes! □

For example, take 41 which is $\equiv 5 \mod 9$. We need to express 41 as

$$2^3 + 2^3 + 2^3 + 2^3 + 2^3 + 1 = 41$$

CMSC 250H - Quantifier Review, Proofs, Testing Primes

February 25, 2026

CMSC250H

Sieve of Eratosthenes