CMSC 250H - Practice Exam and General Review

March 30, 2026

MIDTERM!

ANNOUNCEMENT

MIDTERM TOMORROW 3/31 IN CLASS AT 9:30am

Any questions on HW 6?

Problem 1 – Quantifiers & Domains

Setup

All symbols have their usual meaning. A *domain* is a subset of $\mathbb{R}$.

Consider sentence **(A)**:

$$(\forall x)(\exists y)[x + y = 0]$$

- (a) Give an **infinite** domain where A is **TRUE**, or prove none exists.
- (b) Give an **infinite** domain where A is **FALSE**, or prove none exists.
- (c) Give a **finite** domain (≥ 3 elements) where A is **TRUE**, or prove none exists.
- (d) Give a **finite** domain (≥ 3 elements) where A is **FALSE**, or prove none exists.

Problem 1 – Vote

Sentence (A): $(\forall x)(\exists y)[x + y = 0]$

If this problem appeared on the exam, would you be ready for it?

A	**B**	**C**
Yes, I’ve got it	Mostly, need review	No, need more practice

Solution – Problem 1 (Part A)

Sentence (A): $(\forall x)(\exists y)[x + y = 0]$

Key idea: For any x, we need its additive inverse $-x$ to exist in the domain.

Infinite domain where TRUE

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}$ (all contain additive inverses)

Infinite domain where FALSE

$\mathbb{N}$ (e.g. $x = 1$: there is no $y \in \mathbb{N}$ with $1 + y = 0$)

Solution – Problem 1 (Parts c & d)

Sentence (A): $(\forall x)(\exists y)[x + y = 0]$

Finite domain ($\geq$ 3 elements) where TRUE

$D = \{-1, 0, 1\}$

- $x = -1$: take $y = 1$ ✓
- $x = 0$: take $y = 0$ ✓
- $x = 1$: take $y = -1$ ✓

Finite domain ($\geq$ 3 elements) where FALSE

$D = \{0, 1, 2\}$

- $x = 1$: need $y = -1$, but $-1 \notin D$ $\quad\Rightarrow$ FALSE

Problem 1 (cont.) – Quantifiers & Domains

Consider sentence **(B)**:

$$(\forall x)(\exists y)[xy = 1]$$

- ⓐ Give an **infinite** domain where B is **TRUE**, or prove none exists.
- ⓑ Give an **infinite** domain where B is **FALSE**, or prove none exists.
- ⓒ Give a **finite** domain ($\geq$ 3 elements) where B is **TRUE**, or prove none exists.
- ⓓ Give a **finite** domain ($\geq$ 3 elements) where B is **FALSE**, or prove none exists.

Problem 1B – Vote

Sentence (B): $(\forall x)(\exists y)[xy = 1]$

If this problem appeared on the exam, would you be ready for it?

A	B	C
Yes, I've got it	Mostly, need review	No, need more practice

Solution – Problem 1B

Sentence (B): $(\forall x)(\exists y)[xy = 1]$

Key idea: Every element needs a multiplicative inverse in the domain.

Infinite domain where TRUE

$\mathbb{Q} \setminus \{0\}, \quad \mathbb{R} \setminus \{0\}$

Infinite domain where FALSE

$\mathbb{Z} \quad (x = 2\text{: need } y = \frac{1}{2} \notin \mathbb{Z})$

Finite domain (≥ 3) where TRUE

$D = \{\frac{1}{2}, 1, 2\}$ (each element's inverse is also in D)

Finite domain (≥ 3) where FALSE

$D = \{1, 2, 3\} \quad (x = 2\text{: need } y = \frac{1}{2} \notin D)$

Problem 2 – Boolean Functions

Consider the boolean function:

$$f(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = \begin{cases} T & \text{if exactly ONE input is } T \\ F & \text{otherwise} \end{cases}$$

- (a) How many rows are in the truth table for *f*?
- (b) How many rows evaluate to TRUE?
- (c) Write down all rows that make *f* evaluate to TRUE.
- (d) Write a formula for *f*. (Do *not* use a truth table.)
- (e) Let f_n be the generalization to n inputs. Name a function g such that the formula for f_n has length $O(g(n))$.

Problem 2 – Vote

Boolean function: exactly one input is TRUE

If this problem appeared on the exam,
would you be ready for it?

A	**B**	**C**
Yes, I've got it	Mostly, need review	No, need more practice

Solution – Problem 2 (a–c)

(a) Number of rows

$2^7 = \mathbf{128}$

(b) Rows evaluating to TRUE

Exactly **7** (one for each input being the single TRUE)

(c) All TRUE rows (using 0/1)

$$(1,0,0,0,0,0,0),\quad (0,1,0,0,0,0,0),\quad (0,0,1,0,0,0,0),$$
$$(0,0,0,1,0,0,0),\quad (0,0,0,0,1,0,0),\quad (0,0,0,0,0,1,0),\quad (0,0,0,0,0,0,1)$$

Solution – Problem 2 (d–e)

(d) Formula for f

$$(x_1 \wedge \neg x_2 \wedge \cdots \wedge \neg x_7) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3 \wedge \cdots \wedge \neg x_7) \vee \cdots \vee (\neg x_1 \wedge \cdots \wedge \neg x_6 \wedge x_7)$$

There are $n = 7$ clauses, each of length $n = 7$.

(e) Length of formula for f_n

Each of the n clauses has n literals, so the total length is n^2.

$$g(n) = n^2$$

The formula for f_n has length $O(n^2)$.

Problem 3 – “Cool” Numbers

Domain: natural numbers. Language includes standard logic and arithmetic.

A number is **cool** if it can be written as a sum of $\leq$ 3 cubes. Let $\mathrm{COOL}(x)$ mean x is cool.

- (a) Write a formula for $\mathrm{COOL}(x)$.
- (b) Write a sentence expressing: *There exist infinitely many numbers that are NOT cool.*
- (c) Give 2 examples of cool numbers and prove they are cool.
- (d) Give 2 examples of numbers that are *not* cool and prove it.

Problem 3 – Vote

First-order logic formulas and “cool” numbers

If this problem appeared on the exam,
would you be ready for it?

A	B	C
Yes, I’ve got it	Mostly, need review	No, need more practice

Solution – Problem 3 (a & b)

(a) Formula for COOL(x)

$$\mathrm{COOL}(x) \;\equiv\; (\exists y_1, y_2, y_3)\big[x = y_1^3 + y_2^3 + y_3^3\big]$$

Note: allowing $y_i = 0$ handles sums of 0, 1, or 2 cubes as well.

(b) Infinitely many non-cool numbers

$$(\forall x)(\exists y)\big[y > x \;\wedge\; \neg\,\mathrm{COOL}(y)\big]$$

Solution – Problem 3 (c & d)

(c) Two cool numbers

- $1 = 1^3$
- $2 = 1^3 + 1^3$

(d) Two numbers that are NOT cool

Claim: 4 and 5 are not cool.

Proof for 4: Suppose $4 = x^3 + y^3 + z^3$. Since $2^3 = 8 > 4$, each of $x, y, z \in \{0, 1\}$. So $x^3 + y^3 + z^3 \leq 1 + 1 + 1 = 3 < 4$. Contradiction.

The same argument works for 5: we still need $x, y, z \leq 1$, giving at most $3 < 5$.

Problem 4 – Fourth Powers mod 16

(a) Compute $0^4, 1^4, 2^4, \ldots, 15^4 \pmod{16}$.
Hint: $(16 - a)^4 \equiv a^4 \pmod{16}$.

(b) Use part (a) to find N and an infinite set X such that:

$$x \in X \implies x \text{ cannot be written as a sum of } N \text{ fourth powers.}$$

Make X as large as possible.

Problem 4 – Vote

Fourth powers modulo 16

If this problem appeared on the exam,
would you be ready for it?

A	**B**	**C**
Yes, I've got it	Mostly, need review	No, need more practice

Solution – Problem 4 (a)

All computations are mod 16.

Key observation: all even numbers raised to the 4th power give 0 mod 16.

a	$a^4 \bmod 16$	a	$a^4 \bmod 16$
0	0	8	0
1	1	9	1
2	0	10	0
3	1	11	1
4	0	12	0
5	1	13	1
6	0	14	0
7	1	15	1

Conclusion: Every fourth power mod 16 is in $\{0, 1\}$.

Solution – Problem 4 (b)

Consequence

A sum of k fourth powers is $\equiv 0, 1, 2, \ldots, k \pmod{16}$.

- If $n \equiv 14 \pmod{16}$: any sum of **13** fourth powers cannot equal n (max achievable is 13).
- If $n \equiv 15 \pmod{16}$: any sum of **14** fourth powers cannot equal n (max achievable is 14).

Best result

Take $N = 14$ and

$$X = \{n \in \mathbb{N} : n \equiv 15 \pmod{16}\} = \{15, 31, 47, 63, \ldots\}$$

X is infinite, and no element of X is a sum of 14 fourth powers.

Problem 5 – Constructive Induction

Let $T(n)$ be defined by:

$$T(1) = 0, \qquad T(n) = T\left(\left\lfloor \frac{n}{11} \right\rfloor\right) + T\left(\left\lfloor \frac{2n}{11} \right\rfloor\right) + T\left(\left\lfloor \frac{3n}{11} \right\rfloor\right) + 2n \quad (\forall n \geq 1)$$

Use **constructive induction** to find a constant $A \in \mathbb{N}$ such that:

$$(\forall n \geq 0)\ [T(n) \leq An]$$

Problem 5 – Vote

Constructive Induction to bound a recurrence

If this problem appeared on the exam,
would you be ready for it?

A	**B**	**C**
Yes, I've got it	Mostly, need review	No, need more practice

Solution – Problem 5

Proof that $T(n) \le An$; find conditions on A.

Base Case: $T(1) = 0 \le A \cdot 1$. No constraint needed.

IH: For all $n' < n$, $T(n') \le An'$.

IS: By definition and the IH:

$$\begin{aligned} T(n) &= T(\lfloor n/11 \rfloor) + T(\lfloor 2n/11 \rfloor) + T(\lfloor 3n/11 \rfloor) + 2n \\ &\le \frac{An}{11} + \frac{2An}{11} + \frac{3An}{11} + 2n = \frac{6An}{11} + 2n \end{aligned}$$

We **want** this $\le An$:

$$\frac{6A}{11} + 2 \le A \implies 2 \le \frac{5A}{11} \implies A \ge \frac{22}{5}$$

Since $A \in \mathbb{N}$, take $\boxed{A = 5}$.

Problem 6 – Powers of 2 mod 7

ⓐ Compute $2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6 \pmod 7$.

ⓑ State a true conjecture: the value of $2^n \pmod 7$ depends only on $n \pmod 3$.

ⓒ Prove your conjecture by induction.

Problem 6 – Vote

Powers of 2 modulo 7, proved by induction

If this problem appeared on the exam,
would you be ready for it?

A	**B**	**C**
Yes, I've got it	Mostly, need review	No, need more practice

Solution – Problem 6 (a & b)

(a) Computing powers

$$2^0 \equiv 1, \quad 2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 1, \quad 2^4 \equiv 2, \quad 2^5 \equiv 4, \quad 2^6 \equiv 1 \quad (\mathrm{mod}$$

(b) Conjecture

$$2^n \bmod 7 = \begin{cases} 1 & \text{if } n \equiv 0 \pmod 3 \\ 2 & \text{if } n \equiv 1 \pmod 3 \\ 4 & \text{if } n \equiv 2 \pmod 3 \end{cases}$$

Solution – Problem 6 (c) Proof by Induction

Base cases: $n = 0, 1, 2$ verified in part (a).

IH: The conjecture holds for n.

IS: Consider $2^{n+1} = 2 \cdot 2^n$. There are three cases:

- $n + 1 \equiv 0$, so $n \equiv 2$: by IH, $2^n \equiv 4$. Then $2^{n+1} \equiv 8 \equiv 1$ ✓
- $n + 1 \equiv 1$, so $n \equiv 0$: by IH, $2^n \equiv 1$. Then $2^{n+1} \equiv 2$ ✓
- $n + 1 \equiv 2$, so $n \equiv 1$: by IH, $2^n \equiv 2$. Then $2^{n+1} \equiv 4$ ✓

In each case the conjecture holds for $n + 1$. ■

CMSC 250H - Practice Exam and General Review

March 30, 2026

Weak Induction

Outline for Weak Induction:

1. Prove that the first statement S_1 is true.
2. Given any integer $k \geq 1$, prove that $S_k \implies S_{k+1}$ is true
3. It follows that S_n is true for all n

Strong Induction

Outline for Strong Induction:

1. Prove that the statements $S_1, \ldots, S_m$ are true
2. Given any integer $k \geq m$, prove that $S_1 \wedge S_2 \wedge S_3 \wedge \ldots \wedge S_k \implies S_{k+1}$ is true
3. It follows that S_n is true for all n

The only difference is the number of base cases you need to prove.

This allows for more flexibility when doing things that involve subcases of difference sizes (like Fibonacci).

Normally, we use the umbrella term induction and don't differentiate between the two.

Induction Proofs

Typically, there are three things you need to highlight in your proof:

1. The Base Case
2. The Inductive Hypothesis (your indcutive assumption)
3. The Inductive Step (your use of the assumption)

Example

Sequence

$$a_n = \begin{cases} 1 & n = 1 \\ 2 & n = 2 \\ \displaystyle\sum_{i=1}^{n-1} (i-1)\, a_i & n \geq 3 \end{cases}$$

Statement

Prove that $a_n = (n-1)!$ for all integers $n \geq 3$.

Base Case & Hypothesis

Base Case: $n = 3$

$$a_3 = (1-1)(1) + (2-1)(2) = 0 + 2 = 2 = (3-1)! \checkmark$$

Inductive Hypothesis

Assume for some $k \geq 3$: $a_k = (k-1)!$

Problem 4 — Inductive Step

Inductive Step: $n = k + 1$

$$a_{k+1} = \sum_{i=1}^{k} (i-1)a_i = \sum_{i=1}^{k-1} (i-1)a_i + (k-1)a_k$$

Note that $\sum_{i=1}^{k-1} (i-1)a_i = a_k$. So:

$$a_{k+1} = a_k + (k-1)a_k = (k-1)! + (k-1)(k-1)!$$

$$= (k-1)!\,(1 + k - 1) = (k-1)! \cdot k = k!$$

By PMI, the statement holds. ■

Constructive Induction

Key elements of Constructive Induction:

1. Guess the form your solution takes
2. Solve as if you have an inductive proof
3. During the proof, establish conditions on your unknown variables such that the relevant step holds
4. Solve for unknowns

Example

Statement

Use Constructive Induction to find constants A, B, C such that

$$\sum_{i=1}^{n}(4i-3) = An^2 + Bn + C.$$

Finding the Constants

Base Case: $n = 1$

$\sum_{i=1}^{1}(4i - 3) = 1$, so $A + B + C = 1$.

Inductive Step

Assuming $\sum_{i=1}^{n}(4i - 3) = An^2 + Bn + C$, for $n + 1$:

$$An^2 + Bn + C + 4(n+1) - 3 = A(n+1)^2 + B(n+1) + C$$

$$4n + 1 = 2An + A + B$$

Matching coefficients: $4 = 2A \Rightarrow A = 2, \quad 1 = A + B \Rightarrow B = -1$.
From base case: $C = 1 - A - B = 0$.

Result

Result

$$\sum_{i=1}^{n}(4i-3) = 2n^2 - n \blacksquare$$

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.

Contradiction Proofs

We have some proposition P we want to prove.

We assume it is false, and show that this assumption leads to nonsense (a contradiction)

Outline of Contradiction Proof

Proposition. P

- Assume ¬ P

$\vdots$

-
- Arrive at a conclusion C

$\vdots$

-
- Arrive at a conclusion $\neg C$
- Therefore $C \wedge \neg C$

$10^{1/3}$ is irrational

Proof.

Assume to the contrary that $10^{1/3}$ is rational. Then for $a, b \in$ we have that

$$10^{1/3} = \frac{a}{b}$$

with a, b sharing no common factors, for if they did, we could simply remove those to obtain new a and b. Cubing both sides we obtain:

$$10 = \frac{a^3}{b^3} \implies 10b^3 = a^3$$

□

$10^{1/3}$ is irrational

Proof.

So 10 divides a, and $a = 10k$ for some $k \in$. Plugging back in for a, we obtain

$$10b^3 = (10k)^3 \implies 10b^3 = 10^3k^3 \implies b^3 = 10^2k$$

So 10 divides b. However, we assumed that a and b shared no common factors, a contradiction. Thus, $10^{1/3}$ must be irrational □

$101^{1/4}$ is irrational

Proof.

Assume by way of contradiction that $101^{1/4}$ is rational. Then, there exists $a, b \in$, uniquely factored, such that

$$101^{1/4} = \frac{a}{b} \implies 101b^4 = a^4$$

Let $p_1 p_2 \dots p_k$ denote the prime factors of either a or b, and let the unique prime factorizations of a, b be

$$a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$
$$b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$$

□

$101^{1/4}$ is irrational

Proof.

Thus, substituting in, we obtain

$$101 \cdot p_1^{4b_1} p_2^{4b_2} \dots p_k^{4b_k} = p_1^{4a_1} p_2^{4a_2} \dots p_k^{4a_k}$$

Since 101, is prime, it must be that the exponent for $p_i = 101$ is odd on the left hand side, and even on the right. This contradicts unique prime factorization, thus $10^{1/4}$ must be irrational. □

Diffie Hellman