Midterm Review Session

**Comic Strip:**

- **Top Left Panel:**
  - A person says, "Excuse me? Should we use pens on the midterm, or pencils?"
  - Another person responds, "Use whatever you feel like."

- **Bottom Right Panel:**
  - A person holds a large crayon and says, "Sweet."
Predicate Logic
Circuits

Write boolean Algebra expression for:

1) Sum of products form

\[ p \bar{q} \bar{r} + p \bar{q} r + p q \bar{r} + p q r + p q r \]

\[ p \bar{r} + p \bar{r} \]

\[ p \bar{r} + p r = r \]

\[ r + p q \bar{r} = r + p q \]

\[ \overline{p r (q + q')} \]

\[ (p \implies q) \implies r \]

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>r</th>
<th>( p \implies q )</th>
<th>( (p \implies q) \implies r )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Logic/Predicate Logic

Likes (p, f) Person P likes to eat food f.
Serve (r, f) Restaurant r serves the food f.

(i) Every restaurant serves a food that no one likes.
\[ \forall r \exists f \left( \text{Serve}(r, f) \land \forall p \neg \text{Likes}(p, f) \right) \]

(ii) Every restaurant that serves TOFU also serves a food which RANDY does not like.
\[ \forall r \left( \text{Serve}(r, \text{TOFU}) \rightarrow \exists f \left( \text{Serve}(r, f) \land \neg \text{Likes}(\text{RANDY}, f) \right) \right) \]
$P(n)$ be " $\sum_{i=0}^{n} x_i = \frac{1 - x^{n+1}}{1 - x}$ for all $x \neq 1"$.  

True
Proofs

\[ \text{Rational}(x) = \exists p \exists q \ x = \frac{p}{q} \land \text{int}(p) \land \text{int}(q) \land q \neq 0 \]

\( \pi \) is not rational

Disprove: if \( x, y \) are irrational then \( x + y \) is irrational.

\( \pi + (-\pi) = 0 \)

\( \pi \) is irrational

\(-\pi\) is irrational: we prove by contradiction

Suppose \(-\pi\) is rational. \(-\pi = \frac{p}{q}\) for int \( p, q \) when \( q \neq 0 \).

\( \Rightarrow \pi = \frac{-p}{q} \). \(-p, q\) are int, \( q \neq 0 \) \( \Rightarrow \) \( \pi \) is rational which

is a contradiction. Therefore \(-\pi\) is irrational.

\( \pi + (-\pi) = 0 \) disproves the claim.

\( \pi + 1 - \pi = 1 \)
Proofs

Given: \( p \) \( \therefore q \rightarrow p \land q \)

1. \( p \) \[Given\]

2.1. \( q \) \[Assumption\]

2.2. \( p \land q \) \[Intro of \( \land \) 1, 2.1\]

2. \( q \rightarrow p \land q \) \[Direct proof rule\]


Proofs
Modular Equations

\[ \text{Mod: } a = b \Rightarrow ac \equiv bd \]
\[ c = d \Rightarrow a + c \equiv b + d \]

\[ a \equiv a \mod m \quad (\mod m) \]
\[ b \equiv b \mod m \quad (\mod m) \]
\[ a + b \equiv a \mod m + b \mod m \quad (\mod m) \]
\[ (a + b) \mod m = (a \mod m + b \mod m) \mod m \]

Euclidean Algorithm: Part (c):
Which integers in \{1, \ldots, 83\} have multiplicative inverses modulo 7.

There are numbers \( x \) s.t. \( \gcd(x, 7) = 1 \)

- if \( \gcd(x, 7) = 1 \) then Extend Euclidean Alg gives it.
- Otherwise if \( \gcd(x, 7) \neq 1 \) \( ax \equiv 1 \mod 7 \)

1, 2, 4, 5, 7, 8

\[ \Rightarrow 7 | ax - 1 \]
\[ \Rightarrow 7k = ax - 1 \Rightarrow 7k + ax = -1 \]
\[ \gcd(7k + ax, 7) = \text{but gcd}(x, 7) \neq 1 \]
Modular Exponentiation
Induction

1. Let $P(n)$ be "$T(n) = 2^n n!$". We prove $P(n)$ for all $n \geq 0$.

2. Base Case. Goal: $T(0) = 2^0 \cdot 0!$.
   
   \[ T(0) = 1 = 2^0 \cdot 0! \quad \checkmark \quad P(0) \text{ holds.} \]

3. IH. Assume $P(k)$ holds for some arbitrary $k \geq 0$.

4. IS. Goal $P(k+1)$ holds. $T(k+1) = 2^{k+1} (k+1)!$.

   \[ T(k+1) = 2(k+1) T(k) \quad (\text{since } k+1 \geq 1) \]

   \[ = 2(k+1) 2^k k! \quad (\text{by IH}) \]

   \[ = 2^{k+1} (k+1)! \quad \text{Implies } P(k+1) \]

5. Conclusion $P(n)$ holds for all $n \geq 0$. 


Induction

Part (c)

Suppose \( x_1, \ldots, x_n \) are odd. Prove \( x_1 x_2 \cdots x_n \) is odd.

Let \( P(n) \) be "if \( x_1, \ldots, x_n \) are odd, then \( x_1 \cdots x_n \) is odd."

Base Case. Goal "\( x_1 \) is odd." By assumption \( x_1 \) is odd.

\( P(1) \) holds.

IH. Assume \( P(k) \) holds for some \( k \in \mathbb{Z}^+ \).

TS. Goal \( P(k+1) \) holds, i.e., \( x_1 \cdots x_{k+1} \) is odd.

By IH \( x_1 \cdots x_k \) is odd.

So \( x_1 \cdots x_k = 2q + 1 \) for some int \( q \).

\( x_{k+1} \) by problem assumption, so \( x_{k+1} = 2r + 1 \) for some int \( r \).

\( x_1 \cdots x_{k+1} = (2q+1)(2r+1) = 2(2qr + r + q) + 1 \)

Since \( 2qr + r + q \) is int, \( x_1 \cdots x_{k+1} \) is odd.

This implies \( P(k+1) \).

Conclusion. \( x_1 \cdots x_n \) is odd for all \( n \).
Induction
Formal Proof

Suppose $\forall x \ P(x) \rightarrow Q(x)$, $\forall x \ Q(x) \rightarrow R(x)$, $\neg R(i)$

Proof: $\neg P(i)$.

1. $\forall x \ P(x) \rightarrow Q(x)$ [Given]
2. $\forall x \ Q(x) \rightarrow R(x)$ [Given]
3. $P(i) \rightarrow Q(i)$ [elim $\forall$ step 1]
4. $Q(i) \rightarrow R(i)$ [elim $\forall$ step 2]
5. $\neg R(i)$ [Given]
6. $\neg R(i) \rightarrow \neg Q(i)$ [contrapositive of 4.]
7. $\neg Q(i)$ [MP 5, 6]
8. $\neg Q(i) \rightarrow \neg P(i)$ [contrapositive of 3]
9. $\neg R(i)$ [MP 7, 8].
**# 4 Practice Midterm Part (a)**

The function takes input \((x_1, x_0)_2\) and outputs 1 if \(3 \mid (x_1, x_0)_2\).

Draw truth table:

<table>
<thead>
<tr>
<th>(x_1)</th>
<th>(x_0)</th>
<th>(3 \mid (x_1, x_0)_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Q: $A \subseteq B \iff \overline{B} \subseteq \overline{A}$

Assum $A \subseteq B$. Let $x \in \overline{B}$ be arbitrary. So $x \not\in B$

$A \subseteq B \iff (\forall x \ x \in A \rightarrow x \in B)$

$(\forall x \ x \not\in B \rightarrow x \not\in A)$

So $x \not\in A$. And $x \in \overline{A}$

Assum $\overline{B} \subseteq \overline{A}$. Let $C = \overline{B}$, $D = \overline{A}$.

$C \subseteq D \rightarrow \overline{D} \subseteq \overline{C}$

$\overline{B} \subseteq \overline{A}$ So $B \subseteq A$.

$A \subseteq B \iff \forall x \ x \in A \rightarrow x \in B$. def of $\subseteq$

$\forall x \ x \not\in B \rightarrow x \not\in A$ contrapos.

$\forall x \ x \in \overline{B} \rightarrow x \in \overline{A}$ def of $\overline{B}, \overline{A}$

$\overline{B} \subseteq \overline{A}$. def of $\subseteq$
6 Practice Exam

Prove if \( x, y \) are rational and then \( \frac{y^2}{x-7} \) is rational.

First we show \( \frac{1}{x-7} \) is rational.

Since \( x \) is rational \( x = \frac{p}{q} \) for int \( p, q \) and \( q \neq 0 \)

\( 0 \neq x-7 = \frac{p}{q} - 7 = \frac{p-7q}{q} \neq 0 \) So \( p-7q \neq 0 \)

\( \frac{1}{x-7} = \frac{q}{p-7q} \). Since \( q \) is int, \( p-7q \) int

and \( p-7q \neq 0 \), \( \frac{1}{x-7} \) is rational.

\( \frac{y^2}{x-7} = y \cdot \frac{1}{x-7} \) product of two rationals is a rational. So \( \frac{y^2}{x-7} \) is a rational.
Say \( k \) is a square modulo \( m \) if and only if \( \exists j \) s.t. \( k \equiv j^2 \pmod{m} \).

Let \( T = \{ m : m = n^2 + 1 \text{ for some int } n \} \).

(a) Prove if \( m \in T \), then \(-1\) is a square mod \( m \).

Since \( m \in T \), \( m = n^2 + 1 \) for some int \( n \).

Goal: \(-1 \equiv j^2 \pmod{m} \) for some int \( j \).

\[ m = n^2 + 1 \implies m = n^2 - (-1) \implies m \mid n^2 - (-1) \]

\[ n^2 \equiv -1 \pmod{m} \]

(b) If \( m, k \) if \( m \in T \) and \( k \) is a square mod \( m \), then \( -k \) is also a square mod \( m \).

Part (a):

\( m \in T \implies m = n^2 + 1 \) for some int \( n \)

\(-1 \equiv n^2 \pmod{m} \)

\( k \) is a square, so \( k \equiv j^2 \pmod{m} \) for some int \( j \).

Goal: \(-k \equiv q^2 \pmod{m} \) for some int \( q \).

by multiplication. Thm: \(-k \equiv j^2 \cdot n^2 = (jn)^2 \pmod{m} \).
Prove for any prime \( p \geq 2 \) the equation \( x^2 \equiv p+1 \pmod{p} \)
has exactly two solutions when \( 0 \leq x \leq p-1 \).

Hint: Remember \( x^2 - 1 = (x-1)(x+1) \).

\[
x^2 \equiv p+1 \pmod{p} \Rightarrow x^2 - 1 \equiv p = 0 \pmod{p} \\
(x-1)(x+1) \equiv 0 \pmod{p}.
\]

If \( x = 1 \) then \( x^2 - 1 = 0 \equiv 0 \pmod{p} \)
If \( x = p-1 \) then \( x^2 - 1 = p^2 - 2p \equiv 0 \pmod{p} \).

We prove by contradiction.

Suppose \( x \) is a solution and \( x \neq 1, p-1 \).

\[
(x-1)(x+1) \equiv 0 \Rightarrow p \mid (x-1)(x+1)
\]

Since \( p \) is a prime by unique prime factorization the \( p \) is
in prime factors of \( x-1 \) or \( x+1 \). So \( p \mid x-1 \) or \( p \mid x+1 \).

But we know \( 0 \neq x-1, x+1 < p \). This is not possible.

So there is no solution besides \( p-1, 1 \).
Short(x, y) be x is shorter than y.

Ramch is the tallest person.
\( \forall x \ (x \neq \text{Ramch} \rightarrow \text{Shorter}(x, \text{Ramch})) \)

? \( \exists x \ ( \) \( \forall x \ \neg \text{Short}(\text{Ramch}, x) \) \( \) \( \neg (A < B) \) \( A > B \) \( \) \( ) \)
Modular Eq.

\[ a \equiv a + m \pmod{m} \]

\[ m \equiv 0 \pmod{m} \]

\[ a \equiv a \pmod{m} \quad \text{iff} \quad m \mid a - a = 0 \]

\[ a + m \equiv a \pmod{m} \quad \text{additive} \]

\[ a \equiv b \pmod{m} \quad \text{iff} \quad m \mid a - b \]