CSE 311: Foundations of Computing

Midterm Review Session

Predicate Logic

Circuits

Write boolean Algebra expression eqn $(p \to q) \to r$.

(i) Sum of products form

p	q	r	$(p \to q)$	$(p \to q) \to r$
0	0	0	1	0
0	0	1	1	1
0	1	0	1	0
0	1	1	1	1
1	0	0	0	1
1	0	1	0	1
1	1	0	1	0
1	1	1	1	1

$$\underbrace{p'q'r + p'qr}_{p'r} + pq'r' + \underbrace{pq'r + pqr}_{pr(q+q')}$$

$$\underbrace{pr(q+q')}_{pr}$$

$$p'r + pr = r$$

$$r + pq'r' = \boxed{r + pq'}$$

Logic/Predicate Logic

Practice Qn Part (a).

Likes (p, f) Person p likes to eat food f.

Serves (r, f) Restau r serves the food f.

(i) Every restaurant serves a food that no one likes.

$\forall r \, \exists f \, (\text{Serve}(r,f) \wedge \forall p \, \neg \text{Like}(p,f))$

(ii) Every restaurant that serves TOFU also serves a food which RANDY does not like.

$\forall r \, (\text{Serve}(r, \text{TOFU}) \rightarrow \exists f \, (\text{Serve}(r,f) \wedge \neg \text{Like}(\text{RANDY}, f))$

Logic/Predicate Logic

$P(n)$ be " $\sum_{i=0}^{n} x^i = \frac{1-x^{n+1}}{1-x}$ for all $x \neq 1$ ".

free

bound

Proofs

$\text{Rational}(x) = \exists p\ \exists q\ x = \frac{p}{q} \wedge \text{int}(p) \wedge \text{int}(q) \wedge q \neq 0$

π is not rational

Disprove if x, y are irrational then $x+y$ is irrational.

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

π 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 prove $q \to p \wedge q$

1. p [Given]

    2.1. q [Assumption]

    2.2 $p \wedge q$ [Intro of $\wedge$ 1, 2.1]

2. $q \to p \wedge q$ [Direct proof rule]

Proofs

Modular Equations

Mods: $a \equiv b$, $c \equiv d$ $\Rightarrow$ $ac \equiv bd$, $a+c \equiv b+d$

$a \equiv a \bmod m \pmod m$

$b \equiv b \bmod m \pmod m$

$a+b \equiv a \bmod m + b \bmod m \pmod m$

$(a+b) \bmod m = (a \bmod m + b \bmod m) \bmod m$

Euclidean ALG: Part (c):

Which integers in $\{1, \ldots, 8\}$ have multiplicative inverse modulo 9.

These are numbers x s.t. $\gcd(x, 9) = 1$

if $\gcd(x, 9) = 1$ then Extended Euclidean ALG gives it.

Otherwise if $\gcd(x, 9) \neq 1$ $\quad ax \equiv 1 \bmod 9$

$\Rightarrow 9 \mid ax - 1$

$\Rightarrow 9k = ax - 1 \Rightarrow 9k + ax = -1$

$\gcd \mid 9k + ax$ but $\gcd \nmid -1$

1, 2, 4, 5, 7, 8

Modular Exponentiation

Induction

Part (b) practice questions:

$T(n)$ defined as: $T(0)=1$, $T(n) = 2n\,T(n-1)$ for all $n \geq 1$.

Prove $T(n) = 2^n n!$ for all $n \geq 0$.

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

2. Base Case. Goal: $T(0) = 2^0\, 0!$

   $T(0) = 1 = 2^0\, 0!$ ✓ $P(0)$ 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 $k \geq 1$.

IS. 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 implie $P(k+1)$

Conclusion. $x_1 \cdots x_n$ is odd for all n.

Induction

Formal Proof

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

Prove $\neg P(i)$.

1. $\forall x\ P(x) \to Q(x)$ [Given]
2. $\forall x\ Q(x) \to R(x)$ [Given]
3. $P(i) \to Q(i)$ [elim $\forall$ step 1]
4. $Q(i) \to R(i)$ [elim $\forall$ step 2]
5. $\neg R(i)$ [Given]
6. $\neg R(i) \to \neg Q(i)$ [contopositive of 4.]
7. $\neg Q(i)$ [MP 5, 6]
8. $\neg Q(i) \to \neg P(i)$ [contropositive of 3]
9. $\neg R(i)$ [MP 7, 8].

#4 Practice Midterm Part (a)

function takes input $(x_1 x_0)_2$ and outputs 1 iff $3 \mid (x_1 x_0)_2$

Draw truth table.

	x_1	x_0	$3 \mid (x_1 x_0)_2$
$0 \leftarrow$	0	0	1
$1 \leftarrow$	0	1	0
$2 \leftarrow$	1	0	0
$3 \leftarrow$	1	1	1.

Q: $A \subseteq B$ iff $\overline{B} \subseteq \overline{A}$

Assume $A \subseteq B$. Let $x \in \overline{B}$ be arbitrary. So $x \notin B$

$A \subseteq B$ means $(\forall x \quad x \in A \to x \in B)$

$(\forall x \quad x \notin B \to x \notin A)$

So $x \notin A$. and $x \in \overline{A}$

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

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

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

$A \subseteq B \overset{\text{iff}}{\longleftrightarrow} \forall x \quad x \in A \to x \in B$. def of $\subseteq$

$\overset{\text{iff}}{\longleftrightarrow} \forall x \quad x \notin B \to x \notin A$ contra pos

$\overset{\text{iff}}{\longleftrightarrow} \forall x \quad x \in \overline{B} \to x \in \overline{A}$ def of $\overline{B}, \overline{A}$

$\overset{\text{iff}}{\longleftrightarrow} \overline{B} \subseteq \overline{A}$. def of $\subseteq$

6 Practice Exam

Prove if x, y are rational and $x \neq 7$ then $y^2/x-7$ 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.

$$\frac{y^2}{x-7} = \underbrace{y \cdot y \cdot \frac{1}{x-7}}_{\text{all rationals}}$$

product of two rationals is a rational. So $\frac{y^2}{x-7}$ is a rational.

7 Practice Exam

Say k is a square modulo m iff $\exists j$ s.t. $k \equiv j^2 \pmod{m}$

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

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

Since $m \in T$ $\quad m = n^2+1$ for some int n.

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

$m = n^2+1 \Rightarrow m = n^2-(-1) \Rightarrow m \mid n^2-(-1)$

$n^2 \equiv -1 \pmod{m}$

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

$m \in T \Rightarrow m = n^2+1$ for some $n \xRightarrow{\text{part (a)}} -1 \equiv n^2 \pmod{m}$

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 multipli Thm, $-k \equiv j^2 \cdot n^2 = (jn)^2 \pmod{m}$

Prove for any prime $p > 2$ the equation $x^2 \equiv p+1 \pmod p$ has exactly two solutions where $0 \leq x \leq p-1$

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

$$x^2 \equiv p+1 \pmod p \Rightarrow x^2 - 1 \equiv p \equiv 0 \pmod p$$

$$(x-1)(x+1) \equiv 0 \pmod p.$$

if $x = 1 \Rightarrow x^2 - 1 = 0 \equiv 0 \mod p$

if $x = p-1 \Rightarrow x^2 - 1 = p^2 - 2p \equiv 0 \mod p$

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 then p is in prime factori 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.

Rand is the tallest person.

$\forall x \; (x \neq Rand \rightarrow Shorter(x, Rand))$

$\neg \exists x \; (\; Short(Rand, x))$

$\forall x \quad \neg \, \underbrace{shor(Rand, x)}$

$\neg(A < B)$

$A \geq B$

Modular Eq.

$a \equiv a+m \pmod{m}$

$m \equiv 0 \pmod{m}$

$a \equiv a \pmod{m}$ iff $m \mid a-a=0$

$a+m \equiv a \pmod{m}$ add'l

$a \equiv b \pmod{m}$ iff $m \mid a-b$