School of Information Science and Technology
ShanghaiTech University

SI120 Discussion 8

Proposition Logic, Homework 8, Midterm exam

{qiaowh,chenzl}@shanghaitech.edu.cn

May 6, 2022

Agenda

Lecture Review

- Proposition Logic

Homework 8

Midterm Exam

Definition

- Basic operator: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
- The truth table of the operators above.
- The precedence of the operators.
- WFF and its types.

Application

- Logical equivalence.
  $p \rightarrow q \equiv \neg p \vee q$
- Writing formula based on truth table.

Which of the following is *not* a proposition?

- If $0 > 1$, then NASA will be able to put a man on Mars in 2030.
- $\sqrt{2}$ is not a rational number.
- $\sqrt{2}$ is a rational number.
- $x^2 + 1 > 0$.

Question

Let A be a formula in $p_1, p_2, ..., p_n$ and have truth table T, How to find the formula for A?

Example

Let A be the formula with following truth table. Find the formula for A.

p	q	A	
T	**T**	**F**	
T	**F**	**T**	
F	**T**	**F**	
F	**F**	**T**	

Question

Let A be a formula in $p_1, p_2, ..., p_n$ and have truth table T, How to find the formula for A?

Example

Let A be the formula with following truth table. Find the formula for A.

p	q	A	
T	**T**	**F**	$A_1 = \neg p \vee \neg q$
T	**F**	**T**	
F	**T**	**F**	$A_2 = p \vee \neg q$
F	**F**	**T**	

- **Idea:** $A = A_1 \wedge A_2$
  - $A_1 = \mathbf{F}$ iff $(p, q) = (\mathbf{T}, \mathbf{T})$.
  - $A_2 = \mathbf{F}$ iff $(p, q) = (\mathbf{F}, \mathbf{T})$.

Question

Let A be a formula in $p_1, p_2, ..., p_n$ and have truth table T, How to find the formula for A?

Solution: Write with **F**, CNF

Let τ: $[n] \times \{\mathbf{T}, \mathbf{F}\}^n \to \{p_1, ..., p_n, \neg p_1, ..., \neg p_n\}$ be a map defined by:

$$\tau(i, x) = \begin{cases} \neg p_i & \text{if } x_i = \mathbf{T} \\ p_i & \text{if } x_i = \mathbf{F} \end{cases}$$

Then we have:

$$A = \bigwedge_{\substack{x \in \{\mathbf{T}, \mathbf{F}\}^n \\ A(x) = \mathbf{F}}} \left(\bigvee_{i=1}^{n} \tau(i, x) \right)$$

Question

Let A be a formula in $p_1, p_2, ..., p_n$ and have truth table T, How to find the formula for A?

Solution: Write with **T**, DNF

Let τ: $[n] \times \{\mathbf{T}, \mathbf{F}\}^n \to \{p_1, ..., p_n, \neg p_1, ..., \neg p_n\}$ be a map defined by:

$$\tau(i, x) = \begin{cases} p_i & \text{if } x_i = \mathbf{T} \\ \neg p_i & \text{if } x_i = \mathbf{F} \end{cases}$$

Then we have:

$$A = \bigvee_{\substack{x \in \{\mathbf{T}, \mathbf{F}\}^n \\ A(x) = \mathbf{T}}} \left(\bigwedge_{i=1}^{n} \tau(i, x) \right)$$

Question

Let A be a formula in $p_1, p_2, ..., p_n$ and have truth table T, How to find the formula for A?

Example

Let A be the formula with following truth table. Find the formula for A.

p	q	A	
T	**T**	**F**	
T	**F**	**T**	$A_1 = p \wedge \neg q$
F	**T**	**F**	
F	**F**	**T**	$A_2 = \neg p \wedge \neg q$

- **Idea:** $A = A_1 \vee A_2$
  - $A_1 = \mathbf{T}$ iff $(p, q) = (\mathbf{T}, \mathbf{F})$.
  - $A_2 = \mathbf{T}$ iff $(p, q) = (\mathbf{F}, \mathbf{F})$.

Determine the formulas

p	q	r	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A
T	T	T	T	F	F	F	F	F	F	F	F
T	T	F	F	T	F	F	F	F	F	F	T
T	F	T	F	F	T	F	F	F	F	F	F
T	F	F	F	F	F	T	F	F	F	F	T
F	T	T	F	F	F	F	T	F	F	F	F
F	T	F	F	F	F	F	F	T	F	F	T
F	F	T	F	F	F	F	F	F	T	F	T
F	F	F	F	F	F	F	F	F	F	T	T

Determine the formulas

p	q	r	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A
T	T	T	T	F	F	F	F	F	F	F	F
T	T	F	F	T	F	F	F	F	F	F	T
T	F	T	F	F	T	F	F	F	F	F	F
T	F	F	F	F	F	T	F	F	F	F	T
F	T	T	F	F	F	F	T	F	F	F	F
F	T	F	F	F	F	F	F	T	F	F	T
F	F	T	F	F	F	F	F	F	T	F	T
F	F	F	F	F	F	F	F	F	F	T	T

$$A = (\neg p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r)$$

Logical equivalence:

- $A \equiv B$
- $A \leftrightarrow B$ is tautology.
- $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$.
- $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$.

Tautological Implications:

- $A \Rightarrow B$
- $A \rightarrow B$ is tautology.
- $A \wedge \neg B$ is contradiction.
- $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$

Question

Let p, q, r and s be propositional variables. Construct the truth table for the formula $p \to \neg q \vee r \to \neg(\neg r \to s \wedge p)$.

- Notation: $\{0, 1\}$ is not appropriate to represent $\{T, F\}$.
- Pay attention to the number of lines.
- Solution: omitted.

Question

Let p, q, r and s be propositional variables. Determine the types of the following formulas (tautology, contradiction or contingency). Explain your answers.

(1) $(\neg p \vee q) \wedge (q \to \neg r \wedge \neg p) \wedge (p \vee r)$

(2) $(q \to r) \wedge (p \to q) \to (p \to r)$

(3) $(p \to r) \wedge (q \to s) \wedge (p \vee q) \to (r \vee s)$

Solution to (1)

Contigency.

- It is easy to be false. Just $(p, r) = (F, F)$.
- It also can be true, when $(p, q, r) = (F, F, T)$.

Question

Let p, q, r and s be propositional variables. Determine the types of the following formulas (tautology, contradiction or contingency). Explain your answers.

(1) $(\neg p \vee q) \wedge (q \rightarrow \neg r \wedge \neg p) \wedge (p \vee r)$

(2) $(q \rightarrow r) \wedge (p \rightarrow q) \rightarrow (p \rightarrow r)$

(3) $(p \rightarrow r) \wedge (q \rightarrow s) \wedge (p \vee q) \rightarrow (r \vee s)$

Solution to (2)

Obviously tautology.

- It is false only if $(q \rightarrow r) \wedge (p \rightarrow q)$ is true and $p \rightarrow r$ is false.
- $p \rightarrow r$ is false only if p is true and r is false.
- Then $(q \rightarrow r) \wedge (p \rightarrow q)$ can not be true.

Question

Let p, q, r and s be propositional variables. Determine the types of the following formulas (tautology, contradiction or contingency). Explain your answers.

(1) $(\neg p \vee q) \wedge (q \rightarrow \neg r \wedge \neg p) \wedge (p \vee r)$

(2) $(q \rightarrow r) \wedge (p \rightarrow q) \rightarrow (p \rightarrow r)$

(3) $(p \rightarrow r) \wedge (q \rightarrow s) \wedge (p \vee q) \rightarrow (r \vee s)$

Solution to (3)

Obviously tautology.

- It is false only if $(p \rightarrow r) \wedge (q \rightarrow s) \wedge (p \vee q)$ is true and $r \vee s$ is false.
- $r \vee s$ is false only if r is false and s is false.
- Then $(p \rightarrow r) \wedge (q \rightarrow s) \wedge (p \vee q)$ can not be true.

Let a, b, c and d be the following propositions:

- a: Alice attends the meeting
- b: Bob attends the meeting.
- c: Charlie attends the meeting.
- d: David attends the meeting.

Translate the following statements into propositional formulas in a, b, c and d.

(1) David attends the meeting if and only if Charlie attends and Alice doesn't attend.

(2) Charlie attends the meeting provided that David doesn't attend, but, if David attends, then Bob doesn't attend.

(3) A necessary condition for Alice attending the meeting, is that, if Bob and Charlie aren't attending, David attends.

(4) Alice, Bob and Charlie attend the meeting if and only if David doesn't attend, but, if neither Alice nor Bob attend, then David attends only if Charlie attends.

(1) David attends the meeting if and only if Charlie attends and Alice doesn't attend.

(2) Charlie attends the meeting provided that David doesn't attend, but, if David attends, then Bob doesn't attend.

(3) A necessary condition for Alice attending the meeting, is that, if Bob and Charlie aren't attending, David attends.

(4) Alice, Bob and Charlie attend the meeting if and only if David doesn't attend, but, if neither Alice nor Bob attend, then David attends only if Charlie attends.

Attention

- If v.s. only if
- Provided that = if
- but = and
- Necessary condition v.s. sufficient condition
- Precedence

(1) David attends the meeting if and only if Charlie attends and Alice doesn't attend.

(2) Charlie attends the meeting provided that David doesn't attend, but, if David attends, then Bob doesn't attend.

(3) A necessary condition for Alice attending the meeting, is that, if Bob and Charlie aren't attending, David attends.

(4) Alice, Bob and Charlie attend the meeting if and only if David doesn't attend, but, if neither Alice nor Bob attend, then David attends only if Charlie attends.

Solution

(1) $d \leftrightarrow c \wedge \neg a$

(2) $(\neg d \rightarrow c) \wedge (d \rightarrow \neg b)$

(3) $a \rightarrow (\neg b \wedge \neg c \rightarrow d)$

(4) $((a \wedge b \wedge c) \leftrightarrow \neg d) \wedge ((\neg a \wedge \neg b) \rightarrow (d \rightarrow c))$

Homework
Question 4

Let l, q, n and b be the following propositions:

- l: The file system is locked.
- q: New messages will be queued.
- n: The system is functioning normally.
- b: New messages will be sent to the message buffer.

Determine if the following system specifications are consistent using l, q, n and b:

(1) If the file system is not locked, then new messages will be queued.

(2) If the file system is not locked, then the system is functioning normally, and conversely.

(3) If new messages are not queued, then they will be sent to the message buffer.

(4) If the file system is not locked, then new messages will be sent to the message buffer.

(5) New messages will not be sent to the message buffer.

Let l, q, n and b be the following propositions:

- l: The file system is locked.
- q: New messages will be queued.
- n: The system is functioning normally.
- b: New messages will be sent to the message buffer.

Translation

(1) $\neg l \to q$

(2) $\neg l \leftrightarrow n$

(3) $\neg q \to b$

(4) $\neg l \to b$

(5) $\neg b$

Truth Assignment: $(l, q, n, b) = (T, T, F, F)$

Let $u=$"You can upgrade your operating system", $b_{32}=$"You have a 32-bit processor", $b_{64}=$"You have a 64-bit processor", $g_1=$"Your processor runs at 1 GHz or faster", $g_2=$"Your processor runs at 2 GHz or faster". Which of the following is the correct translation of "You can upgrade your operating system only if you have a 32-bit processor running at 1 GHz or faster, or a 64-bit processor running at 2 GHz or faster."?

- $(b_{32} \wedge g_1) \vee (b_{64} \wedge g_2) \rightarrow u$.
- $u \rightarrow (b_{32} \wedge g_1) \vee (b_{64} \wedge g_2)$.
- $(u \rightarrow (b_{32} \wedge g_1)) \wedge (u \rightarrow (b_{64} \wedge g_2))$.
- $((b_{32} \wedge g_1) \rightarrow u) \wedge ((b_{64} \wedge g_2) \rightarrow u)$.

Prove by rule of replacement:

$$(P \wedge Q \wedge S) \vee (P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge \neg S) \vee \neg(P \wedge R \rightarrow Q) \equiv P$$

Solution

$$
\begin{aligned}
&(P \wedge Q \wedge S) \vee (P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge \neg S) \vee \neg(P \wedge R \rightarrow Q) \\
&\equiv (P \wedge Q \wedge S) \vee (P \wedge Q \wedge \neg S) \vee (P \wedge \neg Q \wedge \neg R) \vee \neg(\neg(P \wedge R) \vee Q) \\
&\equiv (P \wedge Q) \vee (P \wedge \neg Q \wedge \neg R) \vee (P \wedge R \wedge \neg Q) \\
&\equiv (P \wedge Q) \vee (P \wedge \neg Q) \\
&\equiv P
\end{aligned}
$$

Question:

Let $\triangle$ be the unary logical connective defined by the follow truth table

p	$\triangle p$
T	F
F	F

Represent the following formulas

(a) $\neg p$

(b) $p \wedge q$

(c) $p \vee q$

as formulas that only use the connectives $\triangle$ and $\rightarrow$.

Solution:

- $\neg p \equiv \neg p \vee F \equiv p \rightarrow F \equiv p \rightarrow \triangle p$
- $p \wedge q \equiv \neg(\neg p \vee \neg q) \equiv \neg(p \rightarrow \neg q) \equiv (p \rightarrow (q \rightarrow \triangle q)) \rightarrow \triangle p$
- $p \vee q \equiv \neg p \rightarrow q \equiv (p \rightarrow \Delta p) \rightarrow q$

6.

(a) $p \to \triangle p$

p	$p \to \triangle p$	$\neg p$
T	F	F
F	T	T

(b) $p \wedge q \equiv \neg(p \to \neg q)$
$\equiv \neg(p \to (q \to \triangle q))$
$\equiv (p \to (q \to \triangle q)) \to \triangle(p \to (q \to \triangle q))$

p	q	$\neg(p \to \neg q)$	$p \wedge q$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

Or $((p \to q) \to (p \to \triangle q)) \to \triangle q$ S

Or $p \to (q \to \triangle q) \to \triangle p$ A

Or $(p \to q) \to (p \to \triangle p) \to \triangle p$ B

Or $\neg(q \to (p \to \triangle q))$ C

Or $p \to (q \to \triangle p) \to \triangle p$ D

Or $\neg(p \to \neg(p \to q))$ E

Or $p \to (p \to q \to \triangle p) \to \triangle p$ F

p	q	S
T	T	T
T	F	F
F	T	F
F	F	F

p	q	A
T	T	T
T	F	F
F	T	F
F	F	F

p	q	B
T	T	T
T	F	F
F	T	F
F	F	F

p	q	C
T	T	T
T	F	F
F	T	F
F	F	F

p	q	D
T	T	T
T	F	F
F	T	F
F	F	F

(c) $p \vee q \equiv \neg p \to q$
$\equiv (p \to \triangle p) \to q$

p	q	$\neg p \to q$	$p \vee q$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

Or $p \to q \to q$ S

p	q	S
T	T	T
T	F	T
F	T	T
F	F	F

Or $p \to \triangle p \to q \to \triangle q \to \triangle q$ A

p	q	A
T	T	T
T	F	T
F	T	T
F	F	F

Or $(p \to \triangle p) \to (q \to \triangle p) \to p$ B

p	q	B
T	T	T
T	F	T
F	T	T
F	F	F

Or $q \to \triangle q \to p \to \triangle p \to q$ C

p	q	C
T	T	T
T	F	T
F	T	T
F	F	F

Or $\neg q \to (\neg p \to \triangle p)$
$(q \to \triangle q) \to (p \to \triangle p \to \triangle p)$ D

p	q	D
T	T	T
T	F	T
F	T	T
F	F	F

Question

Let p be an odd prime. Wilson's theorem says that $(p-1)! \equiv -1 \pmod{p}$.

1. Show that $\sum_{\alpha \in \mathbb{Z}_p^*} = [0]_p$.
2. Show that the numerator of the fraction $\sum_{i=1}^{p-1} \frac{1}{i}$ is a multiple of p.

Key Idea:

Show that $\sum_{\alpha \in \mathbb{Z}_p^*} = [0]_p$.

- $\sum_{i=1}^{p-1} \frac{1}{i} = \frac{p(p-1)}{2}$

Question

Let p be an odd prime. Wilson's theorem says that $(p-1)! \equiv -1 \pmod p$.

Key Idea:

Show that the numerator of the fraction $\sum_{i=1}^{p-1} \frac{1}{i}$ is a multiple of p

- $\sum_{i=1}^{p-1} \frac{1}{i} = \frac{p(p-1)}{2}$
- $\sum_{i=1}^{p-1} \frac{1}{i} = \frac{1}{(p-1)!} \sum_{i=1}^{p-1} \frac{(p-1)!}{i}$
- $\left[\frac{(p-1)!}{i}\right]_p = -([i]_p)^{-1}$ by Wilson's theorem.
- $\left[\sum_{i=1}^{p-1} \frac{(p-1)!}{i}\right]_p = \sum_{i=1}^{p-1} \left[\frac{(p-1)!}{i}\right]_p = -\sum_{i=1}^{p-1}([i]_p)^{-1} = -\sum_{i=1}^{p-1}[i]_p = [0]_p$

Question

In the RSA public key cryptosystem, if $N = pq$ is the product of two odd primes, we always choose the public encryption exponent e such that $0 \leq e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$. Show that the number of all possible choices of e is at most $\frac{1}{2}\varphi(N)$. Find a specific N such that this number is exactly equal to $\frac{1}{2}\varphi(N)$.

Idea:

Determine $|\mathbb{Z}^*_{\varphi(N)}| = \varphi(\varphi(N))$!

Solution:

In RSA, the number of possible choices of e equals to $|\mathbb{Z}^*_{\varphi(N)}| = \varphi(\varphi(N))$. As $\varphi(N) = \varphi(pq) = (p-1)(q-1)$ and p, q are odd primes, $\varphi(N)$ is even. By the fundamental theorem of arithmetic, there exist distinct primes $p_1 (= 2), p_2, \ldots, p_r$ and integers $e_1, e_2, \ldots, e_r \geq 1$ such that $\varphi(N) = p_1^{e_1} \cdots p_r^{e_r}$. According to the properties of Euler's Phi function, we have

$$\begin{aligned}\varphi(\varphi(N)) =& \varphi(N)\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_r}\right)\\ =& \frac{1}{2}\varphi(N)\prod_{i=2}^{r}\left(1 - \frac{1}{p_i}\right) \leqslant \frac{1}{2}\varphi(N).\end{aligned}$$

$\varphi(\varphi(N)) = \frac{1}{2}\varphi(N)$ only if $r = 1$, i.e., when $\varphi(N)$ is exactly a power of 2. An integer N that satisfies $\varphi(\varphi(N)) = \frac{1}{2}\varphi(N)$ is $N = 15 = 3 \times 5$.

Question

Let n_1, n_2, n_3 be three positive integers such that $\gcd(n_1, n_2) = \gcd(n_1, n_3) = \gcd(n_2, n_3) = 1$. Let a_1, a_2, a_3 and b_1, b_2, b_3 be integers. Let $d_i = \gcd(a_i, n_i)$ for $i = 1, 2, 3$. Show that there is an integer z such that $a_i z \equiv b_i \pmod{n_i}$ for all $i \in \{1, 2, 3\}$ if and only if $d_i | b_i$ for all $i \in \{1, 2, 3\}$.

Solution:

Only if:
This is obvious because for every $i \in \{1, 2, 3\}$, $d_i | b_i$ is a necessary condition for the linear congruence equation $a_i z \equiv b_i \pmod{n_i}$ to have a solution.

Solution:

If:

For every $i \in \{1,2,3\}$, we have that $\gcd(a_i/d_i, n_i/d_i) = 1$, because $\gcd(a_i, n_i) = d_i$. Let

$$t_i = \left(\frac{a_i}{d_i}\right)^{-1} \bmod \frac{n_i}{d_i}.$$

Then for every $i \in \{1,2,3\}$, the equation $a_i z \equiv b_i (\bmod\ n_i)$ is equivalent to

$$z \equiv \frac{b_i}{d_i} t_i \left(\bmod\ \frac{n_i}{d_i}\right). \tag{1}$$

Since n_1, n_2 and n_3 are pairwise relatively prime, so are $\frac{n_1}{d_1}, \frac{n_2}{d_2}$ and $\frac{n_3}{d_3}$. The Chinese Remainder Theorem implies that there is an integer z that satisfies (1) for all $i \in \{1,2,3\}$. That is, there is an integer z such that $a_i z \equiv b_i (\bmod\ n_i)$ for all $i \in \{1,2,3\}$.

Question

For any prime p, $\mathbb{Z}_p$ is a cyclic group with respect to the addition of residue classes modulo p. For example, $[1]_p$ is a generator of $\mathbb{Z}_p$ because $\mathbb{Z}_p = \langle [1]_p \rangle$: any $[k]_p \in \mathbb{Z}_p$ can be expressed as the addition of k copies of $[1]_p$, i.e.,

$$[k]_p = \underbrace{[1]_p + \cdots + [1]_p}_{k}.$$

Show that an element $[g]_p \in \mathbb{Z}_p$ is a generator of $\mathbb{Z}_p$ if and only if $\gcd(g, p) = 1$.

Question

Show that an element $[g]_p \in \mathbb{Z}_p$ is a generator of $\mathbb{Z}_p$ if and only if $\gcd(g, p) = 1$.

Proof: Only if

If $[g]_p$ is a generator of $\mathbb{Z}_p$, then there must exist an integer ℓ such that

$$[1]_p = \underbrace{[g]_p + \cdots + [g]_p}_{\ell},$$

i.e., $[1]_p = [\ell g]_p$. Then there exists an integer m such that $1 = \ell g + mp$. From this equality, we conclude that $\gcd(g, p) = 1$.

Question

Show that an element $[g]_p \in \mathbb{Z}_p$ is a generator of $\mathbb{Z}_p$ if and only if $\gcd(g, p) = 1$.

Proof: If

$\Leftarrow$: If $\gcd(g, p) = 1$, then there exist $s, t \in \mathbb{Z}$ such that

$$gs + pt = 1.$$

For any $k \in \{0, 1, \dots, p-1\}$, we have that

$$k = k \cdot 1 = k \cdot (gs + pt) = kgs + kpt.$$

Then $[k]_p = [ksg]_p = ks[g]_p$. So g is a generator of $\mathbb{Z}_p$.

Question

Let p be a large odd prime and let $[g]_p$ be a generator of the additive group $G = \mathbb{Z}_p$, where $0 \le g < p$. We modify the Diffie-Hellman key exchange protocol as follows:

- Alice: choose $a \in \{0, 1, \ldots, p-1\}$ uniformly at random; compute $[A]_p = \underbrace{[g]_p + \cdots + [g]_p}_{a}$, where $0 \le A < p$; send (p, G, g, A) to Bob;
- Bob: choose $b \in \{0, 1, \ldots, p-1\}$ uniformly at random; compute $[B]_p = \underbrace{[g]_p + \cdots + [g]_p}_{b}$, where $0 \le B < p$; send B to Alice; output the integer K $(0 \le K < p)$ such that $[K]_p = \underbrace{[A]_p + \cdots + [A]_p}_{b}$.
- Alice: output the integer K $(0 \le K < p)$ such that $[K]_p = \underbrace{[B]_p + \cdots + [B]_p}_{a}$.

Question

Show that it's easy to compute a from (p, G, g, A) and so this modified protocol is not secure. (**Hint**: $\gcd(g, p) = 1$)

Solution

According to the modified protocol, $ga \equiv A(\bmod\ p)$. As g is a generator of $\mathbb{Z}_p$, $\gcd(g, p) = 1$. Clearly, $\gcd(g, p)|A$ and so the linear congruence equation $ga \equiv A(\bmod\ p)$ is solvable. A solution $a \in \{0, 1, \ldots, p-1\}$ of the equation $ga \equiv A(\bmod\ p)$ can be calculated efficiently (for example, by using the Extended Euclidean Algorithm).

Question

Determine whether the set $A = \{(x, y, z) : (x, y, z) \in \mathbb{R}^3, x^2 + y^2 + z^2 = 1\}$ and the set $\mathbb{R}$ of real numbers have the same cardinality. Show your answer.

Key Idea:

- $|A| = |[0, 2\pi) \times [0, \pi]|$
- $|[0, 2\pi) \times [0, \pi]| = |(0, 1) \times (0, 1)|$
- $|(0, 1) \times (0, 1)| = |(0, 1)|$
- $|(0, 1)| = |\mathbb{R}|$

Question

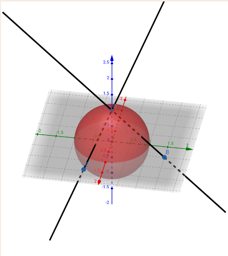
Determine whether the set
$A = \{(x, y, z) : (x, y, z) \in \mathbb{R}^3, x^2 + y^2 + z^2 = 1\}$ and the set $\mathbb{R}$ of real numbers have the same cardinality. Show your answer.

Idea: Bijection between A and $2D$-plane

- $|A| = |[0, 2\pi) \times (0, \pi)|$
  - $f(\theta, \phi) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$.
  - Pay attention to $(0, 0, 1)$ and $(0, 0, -1)$.
- $|A| = |\mathbb{R}^2|$
  - For any line pass through $(0, 0, 1)$, map the intersection with A to its intersection with xOy plane.
  - Pay attention to $(0, 0, 1)$ itself.

Idea: Bijection between A and $2D$-plane

- $|A| = |\mathbb{R}^2|$
  - For any line pass through $(0, 0, 1)$, map the intersection with A to its intersection with xOy plane.
  - Pay attention to $(0, 0, 1)$ itself.



Question

Suppose that $n = p_1 p_2 p_3 p_4$ is the product of four distinct primes p_1, p_2, p_3 and p_4. Determine the number of integers in $[n] = \{1, 2, \ldots, n\}$ that are divisible by at least three of the primes p_1, p_2, p_3 and p_4.

Idea:

Principle of Inclusion-Exclusion.

Solution:

for every $i \in \{1,2,3,4\}$, define $A_i = \{k : k \in [n], (n/p_i)|k\}$.
Then $|A|_i = p_i$ for every $i \in \{1,2,3,4\}$ and the intersection of any ≥ 2 of the sets A_1, A_2, A_3 and A_4 contains exactly one element, i.e., n. Let

$$A = \{k : k \in [n], k \text{ is divisble by at least 3 of } p_1, p_2, p_3, p_4\}.$$

According to the principle of inclusion-exclusion,

$$\begin{aligned}|A| = \left|\bigcup_{i=1}^{4} A_i\right| = &\sum_{t=1}^{4}(-1)^{t-1} \sum_{1\leq i_1\leq\cdots\leq i_t\leq 4} |A_{i_1} \cap \cdots \cap A_{i_t}| \\ = &p_1 + p_2 + p_3 + p_4 - 6 + 4 - 1 \\ = &p_1 + p_2 + p_3 + p_4 - 3.\end{aligned}$$

Question

Show that there exists a positive integer n such that

$$\left|\left\{\{x_1, x_2, x_3, x_4\} : x_1, x_2, x_3, x_4 \in \mathbb{Z}^+, x_1 < x_2 < x_3 < x_4, x_1^3 + x_2^3 + x_3^3 + x_4^3 = n\right\}\right|$$

Idea:

Pigeon-hole Theorem.

Solution:

For any integer $N \geq 4$, the set $[N]$ has exactly
$\binom{N}{4} = \dfrac{N(N-1)(N-2)(N-3)}{24}$ different subsets of cardinality 4.
For every 4-subset $\{x_1, x_2, x_3, x_4\} \subseteq [N]$, we have that

$$1 \leq x_1^3 + x_2^3 + x_3^3 + x_4^3 \leq 4N^3.$$

By the pigeonhole principle, there must exist an integer $n \in [4N^3]$ such that

$$\left|\left\{\{x_1, x_2, x_3, x_4\} : x_1^3 + x_2^3 + x_3^3 + x_4^3 = n\right\}\right| \geq \left\lceil \binom{N}{4} / (4N^3) \right\rceil.$$

By choosing N such that $\lceil \binom{N}{4} / (4N^3) \rceil \geq 2^{2022}$, we can conclude the existence of n.

Question

Suppose that $\{a_n\}_{n\geq 0}$ is a sequence such that $a_0 = a_1 = 0, a_2 = 1$ and $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ for every $n \geq 3$. Find the generating function of $\{a_n\}_{n\geq 0}$.

Solution:

According to the definition of generating function:

$$
\begin{aligned}
A(x) = \sum_{n=0}^{\infty} a_n x^n &= a_0 + a_1 x + a_2 x^2 + \sum_{n=3}^{\infty} a_n x^n \\
&= x^2 + \sum_{n=3}^{\infty} a_n x^n = x^2 + \sum_{n=3}^{\infty} (6a_{n-1} - 11a_{n-2} + 6a_{n-3}) x^n \\
&= x^2 + \sum_{n=3}^{\infty} 6a_{n-1} x^n - \sum_{n=3}^{\infty} 11a_{n-2} x^n + \sum_{n=3}^{\infty} 6a_{n-3} x^n
\end{aligned}
$$

Question

Suppose that $\{a_n\}_{n\geq 0}$ is a sequence such that $a_0 = a_1 = 0, a_2 = 1$ and $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ for every $n \geq 3$. Find the generating function of $\{a_n\}_{n\geq 0}$.

Solution:

According to the definition of generating function:

$$\begin{aligned} A(x) =& x^2 + 6x\sum_{n=2}^{\infty} a_n x^n - 11x^2 \sum_{n=1}^{\infty} a_n x^n + 6x^3 \sum_{n=0}^{\infty} a_n x^n \\ =& x^2 + 6x(A(x) - 0) - 11x^2(A(x) - 0) + 6x^3(A(x)) \\ =& x^2 + (6x - 11x^2 + 6x^3)A(x) \end{aligned}$$

So we have:

$$A(x) = \frac{x^2}{1 - 6x + 11x^2 - 6x^3}$$

Question

For every integer $r \geq 1$, let a_r be the number of ways of distributing r labeled balls into four labeled boxes such that the first box receives an odd number of balls, the second box receives an even number of balls, the third box receives at least 2 balls. Determine a_{100}

Idea:

Here, we need to count permutations with generating function. According to the constrains

$$
\begin{aligned}
R_1 =& \{0, 2, 4, \cdots\} \qquad & R_2 = \{1, 3, 5, \cdots\} \\
R_3 =& \{2, 3, 4, \cdots\} \qquad & R_2 = \{0, 1, 2, \cdots\}
\end{aligned}
$$

Solution:

According to theorem, we have

$$\sum_{r=0}^{\infty} \frac{a_r}{r!} x^r = \prod_{i=1}^{4} \sum_{j \in R_i} \frac{x^j}{j!}$$
$$= \left(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right)\left(x + \frac{x^3}{3!} + \cdots\right)\left(\frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)\left(1 + x -\right.$$
$$= \frac{e^x - e^{-x}}{2} \cdot \frac{e^x + e^{-x}}{2} \cdot (e^x - x - 1) \cdot e^x$$
$$= \frac{1}{4}\left[e^{4x} - 1 - (x+1)\left(e^{3x} - e^{-x}\right)\right]$$
$$= \frac{1}{4} \sum_{r=0}^{\infty} \left[\frac{(4x)^r}{r!} - \frac{(3x)^r}{r!} + \frac{(-x)^r}{r!} - \frac{(3x)^r}{r!} \cdot x + \frac{(-x)^r}{r!} \cdot x\right] - \frac{1}{4}.$$

Solution:

So we have $a_0 = 0$ and

$$a_r = \frac{1}{4}\left[4^r - 3^r + (-1)^r - 3^{r-1}r + (-1)^{r-1}r\right]$$

for all $r \geq 1$. Hence,

$$\begin{aligned} a_{100} =& \frac{1}{4}\left(4^{100} - 3^{100} + 1 - 3^{99} \times 100 - 100\right) \\ =& \frac{1}{4}\left(4^{100} - 103 \times 3^{99} - 99\right). \end{aligned}$$

Thank you for attending.