CS201 Mathematics For Computer Science Indian Institute of Technology, Kanpur

Group Number: 5 Devanshu Singla (190274), Sarthak Rout (190772), Yatharth Goswami (191178)



Date of Submission:

Question 1

Let $S = \{(a, b, c) | a, b, c \in \mathbb{Z}\}$ be the set of all triplets of integers. Show that $|S| = \aleph_0$.

Solution

Consider function $f: \mathbb{N}^2 \to \mathbb{N}$,

$$f((x,y)) = 2^{x}(2y - 1)$$

Let for some $(x_1, y_1), (x_2, y_2) \in \mathbb{N}^2, f((x_1, y_1)) = f((x_2, y_2))$ $\Rightarrow 2^{x_1}(2y_1 - 1) = 2^{x_2}(2y_2 - 1)$ $\Rightarrow 2^{x_1} = 2^{x_2}, \quad 2y_1 - 1 = 2y_2 - 1$ $\Rightarrow x_1 = x_2, \quad y_1 = y_2$ $\therefore \forall (x_1, y_1), (x_2, y_2) \in \mathbb{N}^2, f((x_1, y_1)) = f((x_2, y_2)) \Rightarrow x = y$ Hence, f is injective.

Consider function $f': \mathbb{N} \to \mathbb{N}^2$,

$$f'(x) = (0, x)$$

Let for some $x, y \in \mathbb{N}, f'(x) = f'(y)$, $\Rightarrow (x, 0) = (y, 0)$ $\Rightarrow x = y$ $\therefore \forall x, y \in \mathbb{N}, f'(x) = f'(y) \Rightarrow x = y$ Hence, f' is injective. Since there exist one one function from \mathbb{N} to \mathbb{N}^2 and from \mathbb{N}^2 to \mathbb{N} , there exist bijection between them say, $g: \mathbb{N}^2 \to \mathbb{N}$.

 $\Rightarrow |\mathbb{N}| = |\mathbb{N}^2|$ Consider function $h : \mathbb{N}^3 \to \mathbb{N}^2$,

$$h((x, y, z)) = (x, g(y, z))$$

Claim: *h* is bijective. **Proof:**

1. Injectivity

Let for some
$$(x_1, y_1, z_1), (x_2, y_2, x_2) \in \mathbb{N}^3, h((x_1, y_1, z_1)) = h((x_2, y_2, x_2))$$

 $\Rightarrow (x_1, g(y_1, z_1)) = (x_2, g(y_2, z_2))$
 $\Rightarrow x_1 = x_2, y_1 = y_2, z_1 = z_2 \quad (g \text{ is injective})$
 $\therefore \forall X, Y \in \mathbb{N}^3, h(X) = h(Y) \Rightarrow X = Y$
Hence, *h* is injective.

2. Surjectivity

 $\forall Y = (x,k) \in \mathbb{N}^2, \exists X = (x,y,z), where(y,z) = g^{-1}(k), s.t.$

$$h(x, y, z) = (x, g(y, z)) = (x, k) = Y$$

 $\therefore h$ is surjective

Since *h* is both injective and surjective, \Rightarrow *h* is bijective.

Since there exist a bijection between \mathbb{N}^3 and \mathbb{N}^2 , $\Rightarrow |\mathbb{N}^3| = |\mathbb{N}^2|$

 $\Rightarrow |\mathbb{N}^3| = |\mathbb{N}|$

 \therefore there exists a bijection between \mathbb{N}^3 and \mathbb{N} , say $F: \mathbb{N}^3 \to \mathbb{N}$

Since, $|\mathbb{Z}| = |\mathbb{N}|$, \Rightarrow there exists a bijection between \mathbb{Z} and \mathbb{N} , say $N : \mathbb{Z} \to \mathbb{N}$ Consider function $Z : \mathbb{Z}^3 \to \mathbb{N}$,

$$Z((x, y, z)) = F(N(x), N(y), N(z))$$

Claim: *Z* is bijective.

1. Injectivity

let for some $X, Y \in \mathbb{Z}^3, Z(X) = Z(Y)$, $\Rightarrow F(N(x_1), N(x_2), N(x_3)) = F(N(y_1), N(y_2), N(y_3))$ $\Rightarrow N(x_1) = N(y_1), \quad N(x_2) = N(y_2), \quad N(x_3) = N(y_3), \quad (F \text{ is injective})$ $\Rightarrow x_1 = y_1, \quad x_2 = y_2, \quad x_3 = y_3, \quad (N \text{ is injective})$ $\Rightarrow X = Y$ $\therefore \forall X, Y \in \mathbb{Z}^3, Z(X) = Z(Y) \Rightarrow X = Y$ Hence Z is injective.

2. Surjectivity

 $\forall Y \in \mathbb{N}, \exists (x_1, x_2, x_3) \in \mathbb{Z}^3$, where $x_i = N^{-1}(y_i)$ for i = 1, 2, 3 and $(y_1, y_2, y_3) = F^{-1}(Y)$, s.t.

$$Z((x_1, x_2, x_3)) = F(N(x_1), N(x_2), N(x_3)) = F(y_1, y_2, y_3) = Y$$

 $\therefore Z$ is surjective.

Since Z is both injective and surjective, Z is bijective. \therefore there exists a bijection between \mathbb{Z}^3 and \mathbb{N} ,

 $\begin{aligned} \Rightarrow |\mathbb{Z}^3| &= |\mathbb{N}| \\ \Rightarrow |\mathbb{Z}^3| &= \aleph_0 \quad (|\mathbb{N}| &= \aleph_0|) \\ \text{Hence proved.} \end{aligned}$

For any $a, b, c, d \notin \{-\infty, \infty\}$, show that |[a, b]| = |[c, d]| where [x, y] is the set of all real numbers between x and y

Solution

Consider the function $f : [a, b] \rightarrow [c, d]$,

$$f(x) = c + \frac{x - a}{b - a}(d - c)$$
(2.1)

Since linear functions are bijective in their range and f is linear with range [c, d]

 \Rightarrow *f* is a bijective function.

As there exist a bijective function between [a, b] and [c, d],

 $\Rightarrow |[a,b]| = |[c,d]|$

Show that $|[0,1]| = \aleph_1$ where [0,1] is the set of all real numbers between 0 and 1.

Solution

Consider function $f:[0,1] \rightarrow \mathbb{R}$,

f(x) = x

Since a linear function is injective, so f is injective.

Consider function $g: \mathbb{R} \to [0, 1]$,

$$g(x) = \frac{1}{1 + e^x}$$

Since, g is continuous function and $g'(x) = \frac{-e^x}{(1+e^x)^2} < 0, \forall x \in \mathbb{R}$,

 \Rightarrow *g* is strictly decreasing function and hence is injective.

Since there exist a injective function from \mathbb{R} to [0, 1] and from [0, 1] to \mathbb{R} , there exist a bijective function between [0, 1] and \mathbb{R}

$$\Rightarrow |[0,1]| = |\mathbb{R}|$$

$$\Rightarrow |[0,1]| = \aleph_1 \quad (|\mathbb{R}| = \aleph_1)$$

Show that $|\{0,1\}^*| = \aleph_1$ where $\{0,1\}^*$ is the set of all binary strings of infinite length.

Solution

The main idea of the solution revolves around proving that there exists a one-one mapping from the set of all binary strings of infinite length to the power set of naturals and vice-versa.

Observation-1: There exists a one to one mapping from the set of all binary strings of infinite length to power set of natural numbers.

Proof. Consider an arbitrary binary string of infinite length and define x_i as the *ith* element of the binary string, where each x_i takes value of either 0 or 1 and $i \in \mathbb{N}$. Now, we will define a function f that maps this binary string (S) to a set of naturals (say A) according to the rule that an integer $i \in A$ iff $x_i = 1$.

$$f(S) = \{i \mid x_i = 1\}$$
(4.1)

Also, it is easy to see that this is indeed a one-one mapping since if we choose two different binary strings (say S_1 and S_2) then these will differ at some place say j and therefore only one of the two sets $f(S_1)$ and $f(S_2)$ will contain j as it's element and hence,

$$S_1 \neq S_2 \Rightarrow f(S_1) \neq f(S_2) \tag{4.2}$$

Now, applying this function *f* to each element in the set of all binary strings will produce a unique set of natural numbers which will belong to power set of naturals. Hence, proved that this type of construction leads to a one-one mapping between set of binary strings of infinite length and power set of naturals.

Observation-2: There exists a one to one mapping between the power set of naturals to the set of all binary strings of infinite length.

Proof. Consider an arbitrary set of natural numbers (say A) and by definition of power set, it will be a part of the power set of \mathbb{N} .

Now, we will define a function that maps this set A to an element of the set of binary strings of infinite length according to the rule that the *i*th element of the string i.e. S_i is 1 if $i \in A$.

$$f(A) = S where S_i = 1 if i \in A$$
(4.3)

It is also easy to show the one-one characteristics of the mapping f, since if two sets A and B from the power set of \mathbb{N} differ in atleast one element (say x) then the corresponding binary strings will also differ in value of S_x . Hence,

$$A \neq B \Rightarrow f(A) \neq f(B) \tag{4.4}$$

Now applying this function f to every element in the power set of \mathbb{N} will lead to a unique binary string. Hence, proved that this type of construction provides a one to one mapping between the power set of \mathbb{N} to the set of all binary strings of infinite length.

Conclusion: From the above two Observations, we conclude that there exists a oneone mapping from the set of all binary strings of infinite length to the power set of naturals and a one-one mapping from the set of power set of naturals to the set of all binary strings of infinite length.

Hence, by **Cantor-Bernstein-Schroeder Theorem**, there exists a bijection between the the sets of all binary strings of infinite length and $\mathcal{P}(\mathbb{N})$ and hence they have the same cardinality i.e. \aleph_1 .

Suppose *R* is a partial order on *A* and *S* be a partial order on *B*. Let *L* be a binary relation on $A \times B$ defined as (a, b)L(a', b') iff

- $a \neq a'$ and aRa'
- a = a' and bSb'.

Show that *L* is also a partial order on $A \times B$. Is it a total order?

Solution

Showing that a particular relation in a partial order on a particular requires that relation to be **transitive**, **reflexive** and **anti-symmetric**. So we will show that *L* is transitive, reflexive and anti-symmetric on the set $A \times B$ one by one.

L is transitive : To show that *L* is transitive, we need to show the property that any three elements *a*, *b* and *c* which belong to the set, if *aLb* and *bLc* then *aLc*. To show this on this set, let's take three elements (*a*₀, *b*₀), (*a*₁, *b*₁) and (*a*₂, *b*₂) such that (*a*₀, *b*₀)*L*(*a*₁, *b*₁) and (*a*₁, *b*₁)*L*(*a*₂, *b*₂). We will show that (*a*₀, *b*₀)*L*(*a*₂, *b*₂).

Proof. Now, since the relation is piecewise, we will consider different cases to account for that.

Case (a): $a_0 \neq a_1 \neq a_1 \Rightarrow$ In this case the first condition that $(a_0, b_0)L(a_1, b_1)$ implies that a_0Ra_1 and the second condition $(a_1, b_1)L(a_2, b_2)$ implies that a_1Ra_2 . Now, since R is a partial order on A and hence is transitive, therefore a_0Ra_1 and a_1Ra_2 implies that a_0Ra_2 and since $a_0 \neq a_2$, therefore $(a_0, b_0)L(a_2, b_2)$.

Case (b): $a_0 = a_1 \neq a_2 \Rightarrow$ In this case the first condition that $(a_0, b_0)L(a_1, b_1)$ implies that b_0Sb_1 and the second condition $(a_1, b_1)L(a_2, b_2)$ implies that a_1Ra_2 . Now, since R is a partial order on A and hence is transitive and reflexive therefore a_0Ra_1 (because of the reflexivity) and a_1Ra_2 implies that a_0Ra_2 and since $a_0 \neq a_2$, therefore $(a_0, b_0)L(a_2, b_2)$.

Case (c): $a_0 = a_1 = a_2 \Rightarrow$ In this case the first condition that $(a_0, b_0)L(a_1, b_1)$ implies that b_0Sb_1 and the second condition $(a_1, b_1)L(a_2, b_2)$ implies that b_1Sb_2 . Now, since S is a partial order on B and hence is transitive, therefore b_0Sb_1 and b_1Sb_2 implies that b_0Sb_2 and since $a_0 = a_2$, therefore $(a_0, b_0)L(a_2, b_2)$.

Case (d): $a_0 = a_2 \neq a_1 \Rightarrow$ In this case the first condition that $(a_0, b_0)L(a_1, b_1)$ implies that a_0Ra_1 and the second condition $(a_1, b_1)L(a_2, b_2)$ implies that a_1Ra_2 . Now, since R is a partial order on A and hence is anti-symmetric, therefore a_0Ra_1 and a_1Ra_2 implies that $a_0 = a_1$ and therefore this cases reduces to Case (c). Hence, proved that L is transitive relation.

• *L* is reflexive: To show that *L* is reflexive, we need to show the property that for any element $(a, b) \in A \times B$, (a, b)L(a, b).

Proof. By definition of L, (a, b)L(a, b) iff bSb which is true because S is a partial order on B and hence is reflexive in nature. Hence proved that L is reflexive in nature.

• *L* is anti-symmetric: To show that *L* is anti-symmetric, we need to show the property that any two elements *a b* which belong to the set, if *aLb* and *bLa* then a = b. To show this on this set, let's take two elements (a_0, b_0) and (a_1, b_1) such that $(a_0, b_0)L(a_1, b_1)$ and $(a_1, b_1)L(a_0, b_0)$. We will show that $(a_0, b_0) = (a_2, b_2)$.

Proof. To prove this, we need to take two cases to exhaust all possibilities. **Case (a)**: $a_0 = a_1 \Rightarrow$ In this case the first condition that $(a_0, b_0)L(a_1, b_1)$ implies that b_0Sb_1 and the second condition $(a_1, b_1)L(a_0, b_0)$ implies that b_1Sa_2 . Now, since S is a partial order on B and hence is anti-symmetric therefore b_0Sb_1 and b_1Sb_0 implies that $b_0 = b_1$. Therefore, $(a_0, b_0) = (a_1, b_1)$.

Case (b): $a_0 \neq a_1 \Rightarrow$ In this case the first condition that $(a_0, b_0)L(a_1, b_1)$ implies that a_0Ra_1 and the second condition $(a_1, b_1)L(a_0, b_0)$ implies that a_1Ra_0 . Now, since R is a partial order on A and hence is anti-symmetric, therefore a_0Ra_1 and a_1Ra_0 implies that $a_0 = a_1$ and therefore this case reduces to the first case. Hence proved that L is anti-symmetric in nature.

We can show that *L* is not a total order in $A \times B$ since we can choose such a doublet of pairs (p, q) and (r, s) such that neither *p* is related to *r* nor vice-versa. The existence of such a doublet is guaranteed by *R* being a partial order on *A*. Hence, these two pairs will not be related under *L* and hence L is not a total order.

Let *R* be a binary relation on \mathbb{N} defined as *aRb* if $b = 2^k a$ where *k* is a non-negative integer. Show that *R* is a partial order on \mathbb{N} .

Solution

We can show that relation *R* is a partial order by showing that it is **transitive**, **reflexive** and **anti-symmetric** in nature, which we will show one by one.

• *R* is transitive: To show that *R* is transitive, we need to show that for any three elements *a*, *b* and *c* belonging to set \mathbb{N} if *aRb* and *bRc*, then *aRc* as well.

Proof. From the above two relations, we get

$$aRb \Rightarrow b = 2^{k_1}a \text{ for some } k_1 \in \mathbb{W}$$
 (6.1)

$$bRc \Rightarrow c = 2^{k_2}b \text{ for some } k2 \in \mathbb{W}$$
 (6.2)

Combining the equations (6.1) and (6.2) leads to

$$c = 2^{k_1 + k_2} a \tag{6.3}$$

Now, let $k_1 + k_2 = k$, therefore since $k \in W$ by equation (6.3) we get *aRc*. Hence proved that *R* is transitive.

• *R* is reflexive: To show that *R* is reflexive, we need to show the property that for any element $a \in \mathbb{N}$, *aRa*.

Proof. We need to find a $k \in \mathbb{Z}$ such that $a = 2^k a$. Choosing k = 0 will work and hence, the relation R is reflexive in nature.

• *R* is anti-symmetric: To show that *R* is anti-symmetric, we need to show the property that any two elements *a b* which belong to the set, if *aRb* and *bRa* then *a* = *b*.

Proof. From the above two relations, we get

$$aRb \Rightarrow b = 2^{k_1}a \text{ for some } k1 \in \mathbb{W}$$
 (6.4)

$$bRc \Rightarrow a = 2^{k_2}b$$
 for some $k_2 \in \mathbb{W}$ (6.5)

Combining the equations (6.4) and (6.5) leads to

$$a = 2^{k_1 + k_2} a \tag{6.6}$$

Now, from the equation (6.6), we get $k_1 + k_2 = 0$ and since k_1 and k_2 belongs to \mathbb{W} . Therefore both of them have to be 0. Plugging $k_1 = k_2 = 0$ in equation (6.4) or (6.5) yields a = b. Hence proved that *R* is anti-symmetric in nature.

Hence, proved that R is a partial order on the set of \mathbb{N} .

Let *n* be a positive integer. Consider the relation \equiv_n on \mathbb{Z} such that $a \equiv_n b \iff a = b \mod n$. Show that \equiv_n is an equivalence relation on \mathbb{Z} . What are the equivalence classes?

Solution

An equivalence relation must be **reflexive**, **symmetric** and **transitive** on the set \mathbb{Z} . We are assuming that mod *n* relation relates two elements whose difference is divisible by *n* i.e. $a \equiv_n b$ iff $n \mid a - b$.

Otherwise, if we consider $a \mod n$ to be equal to the **euclidean remainder** that we get after dividing a by n, then it will not be reflexive and symmetric. Ex: $2 = 5 \mod 3$ but $5 \neq 2 \mod 3$ and $5 \neq 5 \mod 3$.

Under such assumptions, always, $n \mid a-b \iff a-b = kn$ where $k \in \mathbb{Z}$. Also, $-k \in \mathbb{Z}$ as subtraction is closed under addition and each element in \mathbb{Z} has an additive inverse. This implies that $b - a = -kn \iff n \mid b - a \iff b = a \equiv_n$. Hence, this relation is **symmetric**.

As every integer *a* divides 0, $n \mid 0 \iff n \mid a - a \forall a \in \mathbb{Z} \iff a \equiv_n a$. Hence, this relation is **reflexive**.

Consider 3 numbers a, b, c, $\in \mathbb{Z}$ such that $a \equiv_n b$ and $b \equiv_n c$. This implies, $n \mid a - b$ and $n \mid b - c \iff a - b = k_1 n$ and $b - c = k_2 n$. Adding both of these equations, $a - c = (k_1 + k_2)n \iff n \mid a - c \iff a \equiv_n c$. $(k_1 + k_2 \in \mathbb{Z}$ as addition is closed under \mathbb{Z}). Hence, this relation is **transitive** and is an equivalence relation.

Consider $a \equiv_n b$ and a = kn + r and b = ln + s where $0 \leq r, s \leq n - 1$ are the euclidean remainders. $n \mid a - b \implies n \mid kn + r - ln - s \implies n \mid r - s$. Now, $-(n-1) \leq r - s \leq n - 1 \implies r - s = 0$ as no other number is divisible by *n*. So, we see that for any two integers to be related, their **euclidean remainder must be the same**. There are *n* possible remainders.

So, there each *n* equivalence classes, each having integers leaving same remainder when divided by *n*. An equivalence class of remainder *r* would be represented as $\{x \mid x \in \mathbb{Z} \text{ and } x\%n = r\}$ where % gives the remainder left after euclidean division.

Consider the relation S on \mathbb{N} such that $aSb \iff ab$ is a perfect square. Show that S is an equivalence relation on \mathbb{N} . What are the equivalence classes?

Solution

An equivalence relation must be **reflexive**, **symmetric** and **transitive** on the set \mathbb{N} . By definition, a perfect square is a number which can represented as a product of a number with itself.

As $a \cdot a = a^2$ is a perfect square, we have aSa trivially. So, this relation is **reflexive**. Consider $a, b \in \mathbb{N}$ such that $aSb \iff ab$ is a perfect square. Multiplication is commutative over natural numbers, hence $a \cdot b = b \cdot a$ is a perfect square. Hence, $aSb \iff bSa$ and the relation is **symmetric**.

Consider 3 natural numbers, a, b, c such that aSb and $bSc \iff ab$ is a perfect square and bc is a perfect square. Let $a \cdot b = p^2$ and $b \cdot c = q^2$ where $p, q \in \mathbb{N}$. This implies $ab^2c = p^2 \cdot q^2 \implies b^2 \mid p^2 \cdot q^2 \implies b \mid p \cdot q \implies ac = (\frac{pq}{b})^2$ and $ac \in \mathbb{N}$. So, ac is a perfect square. Hence, this relation is **transitive** and is an equivalence relation.

Every number can be represented as a product of 2 numbers: a **perfect square** and a **square-free** number. This is unique (From the fundamental theorem of arithmetic, we have unique prime factorisation. Then the square-free part is product of all primes which have odd powers and the perfect square is product of remaining factors i.e. x is square-free means x can be represented as $p_1p_2 \dots p_i$).

Consider two naturals, $a, b \in \mathbb{N}$ such that ab is a perfect square. Let $a = mx^2$ and $b = ny^2$ where m and n are square free and x^2 and y^2 are perfect square parts. As ab is a perfect square, mn is also a perfect square (as rest of all factors are perfect squares). Ex: $180 = (5) * (6)^2, 420 = (3 * 5 * 7) * (2)^2$

It is easy to see, if $m \neq n$ then, there are is at least one prime in m, not in n, which means there product can't have that prime twice. So, if mn is a perfect square, **m** = **n**. This defines the equivalence class, that, there square-free part in prime factorisation must be same.

Ex: $\{x \mid x \in \mathbb{N}, x = mk^2, k \in \mathbb{N}\}$ where $m \in N$ and m is square free and fixed is an arbitrary equivalence class on \mathbb{N} .

There was an ambiguity in the definition of a well-ordering in the lectures. It is clarified here.

A well-ordering R on set A is a partial order such that for every subset $B \subseteq A$, B has an element m such that mRb for every $b \in B$.

In lecture 6, a partial order is shown to be a well-ordering twice: once during proof of the implication that Axiom of Choice implies Zorn's Lemma, and next during proof of the implication that Zorn's Lemma implies Well-Ordering Principle. Redo both these proofs in light of the above clarification.

Solution

Axiom of Choice \implies Zorn's Lemma

We have "g-set" as a subset of G of A such that G is well-ordered and for every $a \in G$:

$$g(\{c \mid cRa \text{ and } c \in G \text{ and } c \neq a\}) = a$$

Let U be the union of all g-sets. We have to prove that U is well-ordered.

- Consider any subset V of U. V intersects one the g-sets W making up U because W is a set of g-sets making up U.
- As W is well-ordered, W \cap V has a least element, say, m_W . Suppose, there is $m \in V$ such that mRm_w .
- If $m \in W$, then $m_w Rm$ showing that $m = m_w$ due to anti-symmetric property.
- If m ∉ W,∃g-set H such that m ∈ H, as ultimately m ∈ U and any super set of V will contain m. This means m ∈ H\W, W is a initial segment of H (as 2 g-sets are initial segments of each other), implying m_wRm. Therefore, again m = m_w and minimal element of V is m_w.

Zorn's Lemma \implies Well-Ordering Principle

- We have $\mathcal{Z} = \{(B), R_B \mid B \subseteq A \text{ and } (A, R_B) \text{ a partial order and } (B, R_B) \text{ a well-ordering} \}$ and relation \mathcal{R} is a partial order on \mathcal{Z} relating initial segments of pair-elements in \mathcal{Z} .
- Let C be a chain on (Z, \mathcal{R}) and U be the union of sets in C. R_U is a relation such that, if two elements in a chain C are related by some relation R_C , only then aR_Ub and vice-versa.
- We have to prove that R_U is a well-ordering on U. Consider a subset V of U.
- Then, $V \cap U$ is not empty for some pair-element (C, R_C) in the chain C because V contains some elements from the union of the sets, U.
- As, R_C is a well-ordering on C as defined in $\mathcal{Z}, V \cap C \subseteq C$ has a least element, say, m_C due to well-ordering theorem.
- Let there be some element $m \in V$ with mR_Um_C . Since, $m \in U$, there exists some pair-element D, in chain C such that $m \in D$.
- Suppose (C, R_C) is an initial segment of (D, R_D) . Then, $m_C R_D m$ showing $m_C R_U m$, which implies $m = m_C$.
- Otherwise, let (D, R_D) be an initial segment of (C, R_C) . Then $m \in C$ which implies, $m \in V \cap U$. So, $m_C R_U m$, which again implies, $m = m_C$.

References