Harvard University
Computer Science 20

Problem Set 4

PROBLEM 1

Show that for every integer $n > 2$ there is a prime between n and $n! = 1 \cdot 2 \cdots (n-1) \cdot n$. (Hint: look for prime factors of $n! - 1$.)

Solution.
We will prove the claim via contraposition by assuming that (n! - 1) cannot be a prime but must a composite integer.
Since (n! - 1) is a composite it must contain a factor, so let $a \in \mathbb{N}$ where $n < a$ and $2 < n$ such that $a|(n! - 1)$.
$a|n!$ (because $a \leq n$) and $a|(n! - 1)$, a must also be a factor of 1 $\therefore$ a must equal 1.
This forms a contradiction because a which is supposed to be a prime number turns out to be equal to 1, which is betrays one of the conditions for prime numbers. If 'a' was to be equal to 1, forcing (n! - 1) to be prime. QED.

PROBLEM 2

Prove by contradiction that $\sqrt{3}+\sqrt{2}$ is irrational. *Hint:* Consider $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2})$

Solution.
W will prove that $\sqrt{3}+\sqrt{2}$ is irrational by contradiction. Assume $\sqrt{3}+\sqrt{2}$ is rational.

$\sqrt{2}$ and $\sqrt{3}$ are known irrational numbers. let $p,q \in \mathbb{Z}$ where $q \neq 0; GCD(p,q) = 1;$ such that $(\sqrt{3}+\sqrt{2}) = \frac{p}{q}$
if $p/q = (\sqrt{3}+\sqrt{2})$ and $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2}) = 1$ then $(\sqrt{3}-\sqrt{2}) = \frac{q}{p}$ and $(\sqrt{3}-\sqrt{2}) = \frac{q}{p}$ is a rational number too.

$\frac{p}{q} + \frac{q}{p} = (\sqrt{3}+\sqrt{2}) + (\sqrt{3}-\sqrt{2})$
$\frac{p^2}{qp} + \frac{q^2}{pq} = 2\sqrt{3}$
$\frac{p^2+q^2}{pq} = 2\sqrt{3}$
let $m,n \in \mathbb{Z}$ such that $m = p^2+q^2$ and $n = pq$ due to the closure properties of integers
$\frac{m}{n} = 2\sqrt{3}$
let $r \in \mathbb{R}$ such that $r = \frac{m}{n}$
$r = 2\sqrt{3}$

After subtracting two expressions (assumed to be rational), and drawing chains of equivalences a contradiction appears when the product of the numbers we assumed to be rational is 'equal' to an irrational number $2 * \sqrt{3}$ (a number know to be irrational).

[solution,letterpaper]cs20 enumerate tikz pgf hyperref circuitikz caption

Harvard University
Computer Science 20

Problem Set 4

PROBLEM 3

Show that for every integer $n > 2$ there is a prime between n and $n! = 1 \cdot 2 \cdots (n-1) \cdot n$. (Hint: look for prime factors of $n! - 1$.)

Solution.
We will prove the claim via contraposition by assuming that (n! - 1) cannot be a prime but must a composite integer.
Since (n! - 1) is a composite it must contain a factor, so let $a \in \mathbb{N}$ where $n < a$ and $2 < n$ such that $a|(n! - 1)$.
$a|n!$ (because $a \leq n$) and $a|(n! - 1)$, a must also be a factor of 1 $\therefore$ a must equal 1.
This forms a contradiction because a which is supposed to be a prime number turns out to be equal to 1, which is betrays one of the conditions for prime numbers. If 'a' was to be equal to 1, forcing (n! - 1) to be prime. QED.

PROBLEM 4

Prove by contradiction that $\sqrt{3}+\sqrt{2}$ is irrational. *Hint:* Consider $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2})$

Solution.
W will prove that $\sqrt{3}+\sqrt{2}$ is irrational by contradiction. Assume $\sqrt{3}+\sqrt{2}$ is rational.

$\sqrt{2}$ and $\sqrt{3}$ are known irrational numbers. let $p,q \in \mathbb{Z}$ where $q \neq 0; GCD(p,q) = 1;$ such that $(\sqrt{3}+\sqrt{2}) = \frac{p}{q}$
if $p/q = (\sqrt{3}+\sqrt{2})$ and $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2}) = 1$ then $(\sqrt{3}-\sqrt{2}) = \frac{q}{p}$ and $(\sqrt{3}-\sqrt{2}) = \frac{q}{p}$ is a rational number too.

$\frac{p}{q} + \frac{q}{p} = (\sqrt{3}+\sqrt{2}) + (\sqrt{3}-\sqrt{2})$
$\frac{p^2}{qp} + \frac{q^2}{pq} = 2\sqrt{3}$
$\frac{p^2+q^2}{pq} = 2\sqrt{3}$
let $m,n \in \mathbb{Z}$ such that $m = p^2+q^2$ and $n = pq$ due to the closure properties of integers
$\frac{m}{n} = 2\sqrt{3}$
let $r \in \mathbb{R}$ such that $r = \frac{m}{n}$
$r = 2\sqrt{3}$

After subtracting two expressions (assumed to be rational), and drawing chains of equivalences a contradiction appears when the product of the numbers we assumed to be rational is 'equal' to an irrational number $2 * \sqrt{3}$ (a number know to be irrational).

PROBLEM 5

Prove that if S is any set of 10 integers between 1 and 100 (inclusive), then there must exist two *distinct* subsets X and Y for which the sum of elements in X equals the sum of the elements in Y.

Solution.
We will prove that for a set S of 10 integers between 1 and 100, there exists distinct subsets X and Y for which the sum of the elements of X equals the sum of elements of Y. We can prove this by determining the number of possible sums of subsets (of 10 integers between 1 and 100), determining the number of possible subsets (of 10 integers between 1 and 100), then applying the pigeonhole principle where the number of possible sums is the number of pigeonholes.

The number of possible of sums (number of pigeonholes) is equal to $\sum_{x=91}^{100} x$. In other words, the number of possible sums is at most the sum of the set of the largest integers: $100 + 99 + \cdots + 91$ or approximately $100 * 10$.
$\sum_{x=91}^{100} x = 955$ possible sums or 'pigeonholes'

The number of possible combinations is $\sum_{k=1}^{n} \binom{n}{k} = 2^n - 1$ where n is the number of possible elements in the subset. Therefore the number of possible combinations/subsets of a set of 10 elements is $2^10 - 1$ (-1 because we exclude empty set) or 1023. Therefore there are 1023 possible combinations / 'pigeons'

According to the pigeonhole principle if there are most pigeons (1023) than pigeonholes (955), there must be 'pigeons' (subsets) which share a 'pigeonhole' (sum). Since in our case the are more set combinations than possible sums for a set of 10 integers from 1 to 100, there must be at least 2 sets which share a sum. QED.

PROBLEM 6

Show, by giving an example for each case, that the intersection of two uncountable sets can be: empty, finite, countably infinite, or uncountably infinite. **Solution.**

Empty: $\mathbb{I} \cap \mathbb{R}$
Finite: $\mathbb{R}^+ \cap \mathbb{R}^-$ (where $\mathbb{R}^+$ and $\mathbb{R}^-$ are defined to be inclusive are 0)
Countably infinite: $A = \mathbb{R}^- \cup \mathbb{Z}^+; B = \mathbb{R}^+ \cup \mathbb{Z}^-; A \cap B$
Uncountably infinite: $\mathbb{C} \cap \mathbb{R}$

PROBLEM 7

Determine whether the following sets are finite, countably infinite, or uncountable. Justify your answers.

(A) The set of all total functions from domain $\{0, 1\}$ to co-domain $\{0, 1\}$

(B) The set of all total functions from domain $\mathbb{N}$ to co-domain $\{0, 1\}$

(C) The set of all total functions from domain $\{0, 1\}$ to co-domain $\mathbb{N}$

Solution.
(A)
Finite. The number of mappings can be determined by cardinality of co-domain$^{\text{cardinality of domain}}$ because each element in the codomain can map to |co-domain| elements. In the case of $\{0, 1\}^{\{0,1\}}$, the size of domain and co-domain is both 2 so the finite size of $|\{0, 1\}^{\{0,1\}}| = 4$
(B)
Uncountably infinite. We are mapping $|\mathbb{N}|$ integers to $\{0, 1\}$ (either 1 or 0). This can be compared choosing subsets of a $\mathbb{N}$ to map to 1 while the others map to 0 (or the other way around). Another question exist is how many distinct subsets exist on $\mathbb{N}$ or what is the cardinality of P($\mathbb{N}$). Therefore there are $2^{\mathbb{N}}$ possible mappings. $|2^{\mathbb{N}}| \neq |\mathbb{N}|$ and $|2^{\mathbb{N}}| > |\mathbb{N}|$ therefore there are uncountable infinitely many mappings between $\mathbb{N}$ and 2.

(C)
Countably infinite. We need to map 0 to one of $\mathbb{N}$ values, and we need to map 1 to one of $\mathbb{N}$ values simultaneously. If we were to place the mappings on a $\mathbb{N}^2$ coordinate plane where the index on one axis corresponds to the output value of 0 and the index of the other axis corresponds to the output when mapping 1 Eg. a function which maps $0 \to 5$ and $1 \to 8$ would be placed at (5,8) on the $\mathbb{N}^2$ coordinate plane, or a function which maps $0 \to 96$ and $1 \to 1$ would be placed at (96, 1) on the coordinate plane.

Since it is known $\mathbb{N}^2$ is countably infinite (because it can be mapped to $\mathbb{N}$ via dovetailing, and we have a successful map from the set of all function ($\{0, 1\} \to \mathbb{N}$) to $\mathbb{N}^2$, the set of all functions ($\{0, 1\} \to \mathbb{N}$) too is countably infinite.

PROBLEM 8

Recall that we saw that the set $\mathbb{R}_{(0,1)} = \{r \in \mathbb{R} : 0 < r < 1\}$ is uncountably infinite using Cantor's diagonalization method.

(A) The Schröder-Bernstein Theorem states that for sets S and T, if there exist injective functions $f : S \to T$ and $g : T \to S$, then S and T have the same cardinality. Using the Schröder-Bernstein Theorem show that the cardinality of the set of real numbers in the closed interval $[0, 1]$ is the same as the cardinality of the set of all real numbers in the open interval $(0, 1)$. To receive full credit on this problem you must formally define two total injective functions $f : \mathbb{R}_{(0,1)} \to \mathbb{R}_{[0,1]}$ and $g : \mathbb{R}_{[0,1]} \to \mathbb{R}_{(0,1)}$.

(B) Using what we have proved about intervals of the real number line, prove that there are at least a countably infinite number of uncountably infinite sets.

Solution.
(A)
f(x) = (x + 1) / 2
g(x) = (x + 1) / 3

The Schröder-Bernstein theorem states that if there exists a total inject function from set S to set T and there exist a total injective function from T to S, the the cardinality of the sets is the same. Since there exists a total injective function f which maps from $\mathbb{R}_{(0,1)} \to \mathbb{R}_{[0,1]}$ and there exists a total injective function g which maps from $\mathbb{R}_{[0,1]} \to \mathbb{R}_{(0,1)}$ the cardinality of $\mathbb{R}_{[0,1]}$ and $\mathbb{R}_{(0,1)}$ is the same.

(B)
It is known that $\mathbb{R}_{(0,1)}$ is uncountably infinite due to cantor's diagonalization. With the same reasoning (cantors diagonalization) and as supported in part A above, $\mathbb{R}_{[0,1]}$ and $\mathbb{R}_{(0,1]}$ are also uncountable uncountably infinite.

Lemma: the cardinality of real numbers between any two integers is uncountably infinite. According to the Schröder-Bernstein theorem, $\mathbb{R}_{(a-1,a)}$ must also be uncountably infinite, because total injective functions exist to map $\mathbb{R}_{(a,a+1]}$ to $\mathbb{R}_{(0,1)}$ this class of function can be defined as $f(x : \mathbb{R}_{(0,1)}, a : \mathbb{Z}) = x + a$ and their inverses $f(x : \mathbb{R}_{(0,1)}, a : \mathbb{Z}) = x - a$ where 'x' represents the original value and 'a' the desired output range.
Due to the existance of total injective functions mapping with inverses from $\mathbb{R}_{(0,1)}$ to any $\mathbb{R}_{(a,a+1)}$, the cardinality of the range of rational numbers between any two integers must be uncountably infinite.

The cardinality of integers is countably infinite because a bijective mapping can be formed between the integers and natural numbers. The real number line consists of the integers and the sets real numbers between each consecutive integers. Since the cardinality of integers is countably infinite and the there are uncountably infinite integers in between any two integers (as well as any two integers 1 apart), we can say that there exists at least countably many uncountable sets on the real number line.