Indian Institute of Information Technology
Design and Manufacturing, Kancheepuram
Chennai 600 127, India
An Autonomous Institute under MHRD, Govt of India
An Institute of National Importance
www.iiitdm.ac.in
COM205T Discrete Structures for Computing-Lecture Notes

Instructor
N.Sadagopan
Scribe:
S.Dhanalakshmi

Functions and Infinite Sets

Objective: We shall introduce functions, special functions and related counting problems. We shall see the importance of functions in the context of infinite sets and discuss infinite sets in detail. Further, we introduce the notion of counting in the context of infinite sets.

Definition 1 (Function) *Let A and B be two non-empty sets. A* function *or a* mapping *f from A to B, written as $f : A \rightarrow B$, where every element $a \in A$ is mapped to a unique element $b \in B$.*

Note:
1. The element $b \in B$ is called the *image* of $'a'$ under f and is written as $f(a)$.
2. If $f(a) = b$ then $'a'$ is called the *pre-image* of b under f.
3. A is called the *domain* of f and $\{f(a) \mid a \in A\}$ is called the *range* of f. B is called the *co-domain* of f.
4. Examples for function:
   a) Domain = Set of apples and Range = weight of apples.
   b) Domain = Set of students and Range = CGPA of students.
5. Every function is a relation but the converse is not true. i.e. Every relation is not a function.
6. For every element $a \in A$, there exist an image $f(a)$. i.e., $f(a)$ is well defined.
7. Let $\mid A \mid= n$ and $\mid B \mid= m$. The number of different functions $f : A \rightarrow B$ is m^n, where $|A|$ represents the cardinality of A, the number of elements of A.
8. Let $\mid A \mid= n$ and $\mid B \mid= m$. If $X = \{R \mid R$ is a relation defined w.r.t $(A, B)\}$ and $Y = \{R \mid R$ is a function w.r.t $(A, B)\}$ then, $\mid X \mid\geq\mid Y \mid$ (Since, $\mid X \mid= 2^{mn}$ and $\mid Y \mid= m^n$).

Things to know:
1. Is there a function $f : A \rightarrow B$, if $A = \emptyset$ and $B \neq \emptyset$? Yes, an empty function.
2. Is there a function $f : A \rightarrow B$, if $A \neq \emptyset$ and $B = \emptyset$? No.
3. Is there a function $f : A \rightarrow B$, if $A = \emptyset$ and $B = \emptyset$? Yes, void function.

Definition 2 (One-one function/Injective) *A function is said to be injective if for every element in the range there exists a unique pre-image. i.e., no two elements in the domain map to same element in the co-domain.*

Definition 3 (Onto function/Surjective) *A function is said to be surjective if for every element in the co-domain there exists a pre-image.*

- A function is said to be *bijective* if it is both one-one and onto function.

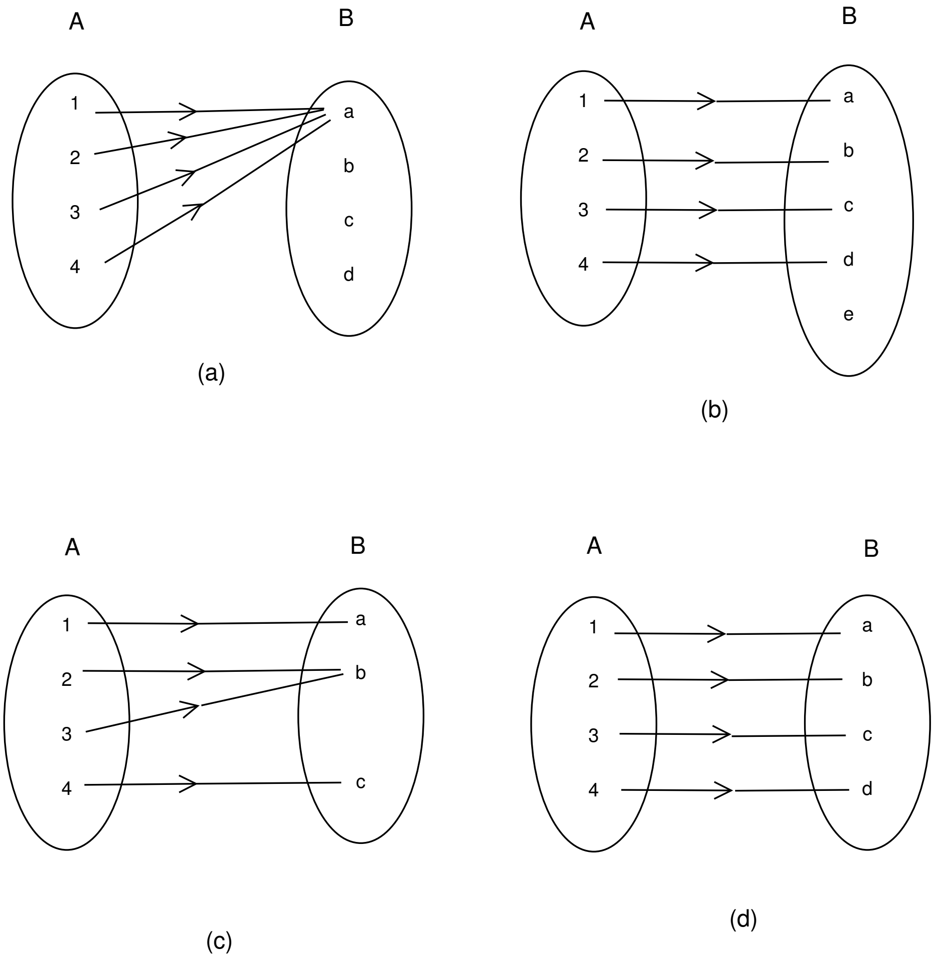

Fig. 1. (a) Not one-one and not onto (b) one-one but not onto (c) onto but not one-one (d) one-one and onto

- Let $A = B = N$(set of natural numbers).
  - Give an example of a function $f : N \to N$, that is one-one and not onto ? $f(x) = x + 1$
  - Give an example of a function $f : N \to N$, that is not one-one but onto ? $f(x) = \lceil \frac{x}{2} \rceil$
  - Give an example of a function $f : N \to N$, that is one-one and onto ? $f(x) = x$

- Let $A = B = I$(set of integers).
  - Give an example of a function $f : I \to I$, that is one-one and not onto ? $f(x) = 2x$
  - Give an example of a function $f : I \to I$, that is not one-one but onto ? $f(x) = \lceil \frac{x}{2} \rceil$, if $x \geq 1$ and $f(x) = x$, if $x \leq 0$.
  - Give an example of a function $f : I \to I$, that is one-one and onto ? $f(x) = x$

- Give a bijective function $f : (0, 1) \to (4, 5)$ in real numbers ? $f(x) = x + 4$.

- Let $\mid A \mid= n$ and $\mid B \mid= m$. The number of different one-one functions are $m_{C_n} \times n! = m_{P_n}$.

Food for Thought

1. Let $\mid A \mid= n$ and $\mid B \mid= m$. The number of different onto functions ?
2. Let $\mid A \mid= n$ and $\mid B \mid= m$. The number of different bijective functions ?
3. Give a bijective function $f : (0, 1) \to (a, b)$ in real numbers ?

An invitation to infinite sets

Motivation:

- Many interesting sets such as
  (i) Set of prime numbers
  (ii) Set of C-programs
  (iii) Set of C-programs with exactly three statements
  are infinite in nature.
- Between I and N, which set is bigger ?
- Between I and $N \times N$, which set is bigger ?
- Is $[0, 1]$ is bigger than R ?
- Can we list all C-programs ?

Definition 4 (Finite) *A set $'A'$ is finite if there exists $n \in N$, n-represents the cardinality of A such that there is a bijection $f : \{0, 1, \ldots, n-1\} \rightarrow A$. A is infinite if A is not finite.*

Definition 5 (Infinite) *Let A be a set. If there exists a function $f : A \rightarrow A$ such that f is an injection and $f(A) \subset A$ then A is infinite.*

- Let B be a finite set, $B = \{1, 2, \ldots, 10\}$. Can you establish a 1-1 function $f : B \rightarrow B$ such that $f(B) \subset B$? No.

- Can you establish a 1-1 function $f : N \rightarrow N$ such that $f(N) \subset N$? Yes, $f(x) = x + 1$.

- Every 1-1 function from $f : B \rightarrow B$ is also a bijection from $B \rightarrow B$ if B is finite.

Problem 1: Show that N is infinite.

Proof by contradiction: Suppose N is finite. By definition, there exists n, n represents the cardinality of N such that $f(n) = a_n$. Let $K = MAX\{f(0), f(1), \ldots, f(n-1)\} + 1$. There does not exist a $x \in \{0, 1, \ldots, n-1\}$ such that $f(x) = k$.
Therefore, f is not onto and thus, f is not a bijection. Hence, our assumption is wrong and N is infinite.

Problem 2: Show that R is infinite.

Proof: To prove R is infinite, establish a function $f : R \rightarrow R$ such that f is 1-1 and $f(R) \subset R$. Consider $f : R \rightarrow R$ such that $f(x) = x + 1$, if $x \geq 0$ and $f(x) = x$, if $x < 0$. This function f is 1-1 but not onto (Since, 0 does not have a pre-image) and $f(R) \subset R$. Hence, R is infinite.

Problem 3: Let $\sum = \{a, b\}$ and $f : \sum^* \rightarrow \sum^*$. Show that $\sum^*$ is infinite.

Proof: To prove $\sum^*$ is infinite, establish a function $f : \sum^* \rightarrow \sum^*$ such that f is 1-1 and $f(\sum^*) \subset \sum^*$.
Consider $f : \sum^* \rightarrow \sum^*$ such that $f(x) = ax$. The elements $\epsilon, b, ba, bb, \ldots$ will not have a pre-image. Therefore f is not onto but 1-1 and $f(\sum^*) \subset \sum^*$. Hence, $\sum^*$ is infinite.

Problem 4: Show that $[0, 1]$ is infinite.

Proof: Consider $f : [0, 1] \to [0, 1]$ such that $f(x) = \frac{x}{2}$. This function f is 1-1 but not onto (Since, $(\frac{1}{2}, 1]$ does not have a pre-image) and $f([0, 1]) \subset [0, 1]$. Hence, $[0, 1]$ is infinite.

Claim: 1 Let A' be a subset of A. If A' is infinite then A is infinite.
Proof: Given A' is infinite. Therefore, there exist a function $g : A' \to A'$ such that g is 1-1 and $g(A') \subset A'$.
Consider a function $f : A \to A$ such that $f(x) = x$, if $x \in A \backslash A'$ and $f(x) = g(x)$, if $x \in A'$. The function f is also 1-1 and $f(A) \subset A$ (Since, g is 1-1 and $g(A') \subset A'$). Thus, A is infinite.

Corollary: Every subset of a finite set is a finite set.

Claim 2: Let $f : A \to B$ be an injection. If A is infinite then B is infinite.
Proof: Since f is 1-1 and A is infinite, $f(A)$ is infinite. By previous claim, B is infinite (since, $f(A) \subseteq B$).

Problem 5: A is infinite. Show that (i) $P(A)$, power set of A is infinite. (ii) $A \cup B$ is infinite. (iii) $A \times B$ is infinite. (iv) A^B, the set of all functions from B to A, is infinite.

Solutions:
(i) Consider a function $f : A \to P(A)$ such that $f(x) = \{x\}$. The function f is 1-1 but not onto i.e.,$A \subseteq P(A)$. Thus, $P(A)$ is infinite.

(ii) We know that, $A \subset A \cup B$. Since A is infinite, $A \cup B$ is infinite (by claim 1).

(iii) Consider a function $f : A \to A \times B$ such that $f(x) = (x, a)$ for some $a \in B$. Clearly, the function f is 1-1 but not onto. Thus, $A \times B$ is infinite.

(iv) Every element in A^B is a function from $B \to A$. Consider a function $f : A \to A^B$ such that $f(x) = g$, g is a function from $B \to A$ such that $g(b) = x$, $\forall\ b \in B$. This function f is 1-1 but not onto. Thus, A^B is infinite.

Definition 6 (Countable) *A set A is countable if A is finite or if A has an enumeration (Listing elements of A) or if there exists a bijection from N to A.*

- A set A is said to be Countably infinite if there exist a bijection from N to A or if there exists an enumeration.
- Countable sets are either countably finite or countably infinite.
- $| A |=| B |$ if and only if there exists a bijection from A to B.

Problem 6: Prove: $| N |=| I |$
Solution: To prove there exist a bijection from N to I. Consider the function $f : N \to I$ such that $f(x) = \frac{-(x+1)}{2}$, if $x = 2k + 1$, for some integer k and $f(x) = \frac{x}{2}$, if $x = 2k$, for some integer k. Clearly, this function is 1-1 and onto. Thus, $| N |=| I |$.

Problem 7: Prove that the set P of prime numbers is infinite.
Solution: For every prime number x, we know that there exists a prime number $y > x$. Therefore,

we establish a map between N and the set of prime numbers. $f : N \rightarrow P$ such that $f(i) = P_i$. i.e., i^{th} natural number maps to P_i. Therefore, there exists an enumeration and hence P is countably infinite.

Problem 8: Prove that the set of positive rational numbers, Q^+, is infinite.
Solution: We below enumerate(list) elements of Q^+ in a systematic way as illustrated in the Figure. We then establish a bijective function from N to Q^+ by following the arrows as illustrated in the figure. This yields an enumeration and a mapping to N, therefore Q^+ is infinite. Thus, Q^+ is countably infinite.

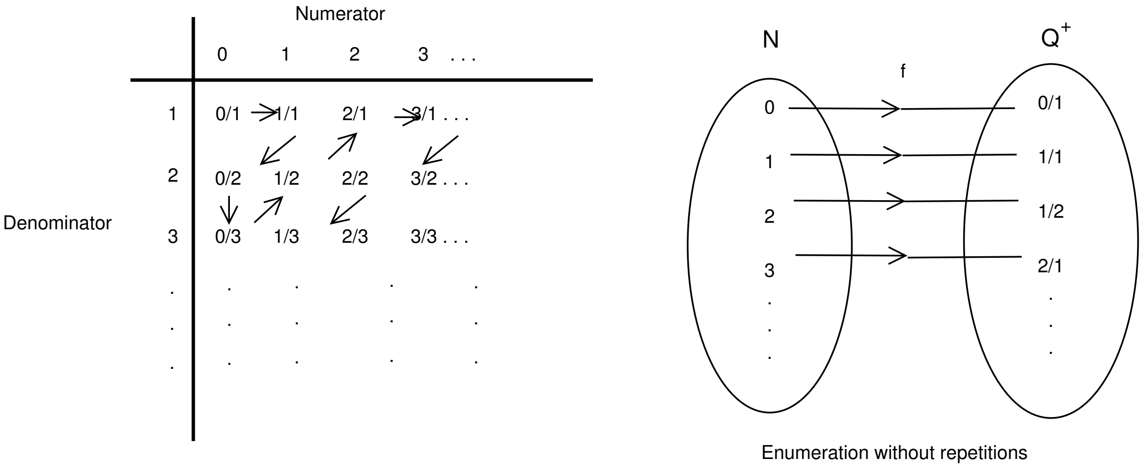

Fig. 2. Enumeration of Q^+

Problem 9: Prove that the cardinality of $\sum^*$ is countably infinite.
Solution: We shall establish this claim by listing the elements of $\sum^*$ using standard ordering. i.e., we first list strings of length one, followed by strings of length two, and so on. Strings having same length will be listed as per lexicographic ordering. An illustration as per standard ordering is shown below.

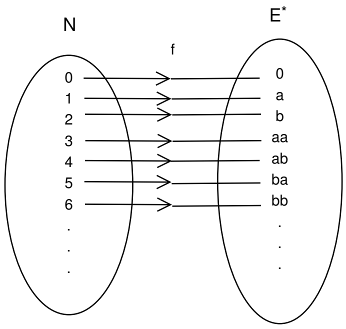

Fig. 3. Enumeration and a bijective function from N to $\sum^*$

Problem 10: Prove that the number of C-programs is countably infinite.
Solution: Let $\sum = \{a, b, \ldots, z, A, B, \ldots, Z, \$, \{, \}, \backslash, \ldots\}$ and $\sum^* = \{\epsilon, String1, String2, \ldots\}$. Note that $\sum$ is precisely the set of keys available in a key board (ASCII characters). It is easy to

see that every C-program is an element in $\sum^*$, i.e, imagine the case where we write a C-program in horizontal fashion instead of vertical fashion. Also, we are not concerned about whether the C-program is syntactically correct or not. We know that $\sum^*$ is countably infinite, thus, number of C-programs is countably infinite.

Problem 11: Prove that the number of C-programs with exactly 3 statements is countably infinite ?
Solution:
Let program-1 be $x = x + 1$, program-2 be $x = x + 2$, $\ldots$, program-∞ be $x = x + \infty$. Clearly, the set of programs (Program-1,...) is infinite. We further know from the previous claim that the number of C-programs is countably infinite. Since this set is only a subset of all C-programs, implies that, the number of C-programs with exactly 3-statements is countably infinite.

Uncountable Sets

In earlier sections, we introduced infinite sets and techniques for showing a set is infinite. Further, we also presented an approach to count infinite sets (countably infinite). We now ask; is every set countable ? i.e., either countably finite or countably infinite. We answer this in negative and show that there are uncountable sets. We next introduce cantor's famous technique, diagonalization technique using which we show that the set $[0, 1]$, the set of real numbers between 0 and 1 is uncountable.

Problem 12: Show that $[0, 1]$ uncountable

Solution: We present a proof by contradiction. Suppose $[0, 1]$ is countable then there exists an enumeration, i.e., listing of elements in $[0, 1]$ in a systematic way; ENUM: $x_1, x_2, \ldots$. Further, there exists a bijection from N to ENUM. Let

$$\begin{aligned} x_1 &= 0.x_{11}x_{12}x_{13}x_{14}\ldots \\ x_2 &= 0.x_{21}x_{22}x_{23}x_{24}\ldots \\ x_0 &= 0.x_{31}x_{32}x_{33}x_{34}\ldots \\ &\ldots \end{aligned}$$

We now show that the above listing is incomplete by exhibiting an element $y \in [0, 1]$ and y is not listed in ENUM. Consider $y = 0.y_1y_2y_3y_4\ldots$, such that $y_i = 3$, if $x_{ii} = 2$ and $y_i = 2$, if $x_{ii} \neq 2$. Clearly, $y \in [0, 1]$ and any x_i and y will differ at one position (at least one). Therefore, y is not enumerated in $x_1, x_2, \ldots$. Thus, ENUM is incomplete and our assumption that $[0, 1]$ is countable is wrong. Therefore, $[0, 1]$ uncountable.

Note: Since $[0, 1]$ is uncountable, the set of real numbers R is uncountable.

Claim: Countable union of countable sets is countable.

Proof: Let $A_1, A_2, \ldots,$ be a set of countable sets. Since each set A_i is countable, then there exists an enumeration of A_i. Construct a matrix with the first row listing the elements of A_1, the second row listing the elements of A_2, and so on. Now, similar to the proof showing the set of rational numbers is countable, enumerate the elements of the constructed matrix to get a natural mapping to the set of natural numbers. Therefore, the claim follows.

Problem 13: Is irrational numbers countable ?.
Solution:
Assume that irrational numbers are countable. Since rational numbers are countable and by the above claim union of rational numbers and irrational numbers is countable, however, this is precisely the set of real numbers, which is a contradiction. Thus, the set of all irrational numbers are uncountable.

Problem 14: Given that $\sum^*$ is countably infinite. Is $P(\sum^*)$ countably infinite ?
Solution: Suppose $P(\sum^*)$ is countably infinite.
Since $\sum^*$ is countably infinite we can enumerate $\sum^*$ as $x_1, x_2, x_3, \ldots$. Since $P(\sum^*)$ is countably infinite, there exists an enumeration $A_1, A_2, A_3, \ldots$, where each A_i is subset of $\sum^*$. We now construct a matrix with row representing the sets (A_i's) and column representing $x \in \sum^*$. Table entries as illustrated in Figure are filled as follows; if you find x_i in A_j, place 1 in the corresponding cell, else place 0.
We now show that there is a subset in $\sum^*$ which is not listed as part of the enumeration. Choose

	x1	x2	x3	x4 ...
A1	1	0	1	0 ...
A2	0	1	1	0 ...
A3	1	1	0	1 ...
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

Fig. 4. Listing $P(\sum^*)$ and $\sum^*$ in a Matrix

$B = \{x_j \mid (A_j, x_j) = 0\}$. $B \in P(\sum^*)$ but not listed as part of the enumeration. Therefore, the enumeration is incomplete. Thus our assumption is wrong. Hence, $P(\sum^*)$ is uncountable.

Problem 15: How many computational problems are there? Is it countable/uncountable.

Solution: 1
Let problem-1 asks for printing $\{0\}$, problem-2 asks for printing $\{0, 1\}$, ..., problem-i asks for printing set containing i elements from N. i.e., each problem prints a subset of N. This problem collection is same as counting i element subset of $P(N)$, power set of N. Clearly, all are computational problems (well defined input and output) and hence the number of computational problems is strictly greater than $\mid P(N) \mid$. We have already shown that $P(N)$ is uncountable, therefore, the number of computational problems is uncountable.

Solution:2
In the earlier section, while showing the number of C-programs is countably infinite, we assumed that the alphabet is finite alphabet containing all ASCII characters. This assumption is true while counting the number of programs as program size is finite. However, this assumption need not be true for describing the problem. In other words, consider a computational problem, `Print the irrational number 0.524673...`, this description contains an infinite string as a substring. So, the problem description takes infinite characters, which is a $P(\sum^*)$. Thus, the number of computational problems is uncountable.

Remark on Solvability/Unsolvability:
Every problem is either solvable or unsolvable. A problem is said to be solvable if there exists an algorithm/program. A problem is said to be unsolvable if there does not exists an algorithm (Example: Print N, Print I).

Problem 16: How many solvable problems are there ?
Since each solvable problem has an algorithm or a program, this count is equivalent to the number of C-programs and therefore, the number of solvable problems is countably infinite.
Problem 17: How many unsolvable problems are there ?
Consider the set of programs `print` $[i, j]$ `where` $i, j \in R$, each program in this set is unsolvable problem as there is no algorithm to list all values of the closed interval $[0, 1]$ and this is true for all $[i, j]$. Since the size of this set is R, the number of unsolvable problems is uncountable.

Acknowledgements: Lecture contents presented in this module and subsequent modules are based on the text books mentioned at the reference and most importantly, lectures by discrete mathematics exponents affiliated to IIT Madras; Prof P.Sreenivasa Kumar, Prof Kamala Krithivasan, Prof N.S.Narayanaswamy, Prof S.A.Choudum, Prof Arindama Singh, and Prof R.Rama. Author sincerely acknowledges all of them. Special thanks to Teaching Assistants Mr.Renjith.P and Ms.Dhanalakshmi.S for their sincere and dedicated effort and making this scribe possible. This lecture scribe is based on the course 'Discrete Structures for Computing' offered to B.Tech COE 2014 batch during Aug-Nov 2015. The author greatly benefited by the class room interactions and wishes to appreciate the following students: Mr.Vignesh Sairaj, Ms.Kritika Prakash, and Ms.Lalitha. Finally, author expresses sincere gratitude to Mr.Sreeraj.R for thorough proof reading and valuable suggestions for improving the presentation of this article. His valuable comments have resulted in a better article.

References:

1. K.H.Rosen, Discrete Mathematics and its Applications, McGraw Hill, 6th Edition, 2007
2. D.F.Stanat and D.F.McAllister, Discrete Mathematics in Computer Science, Prentice Hall, 1977.
3. C.L.Liu, Elements of Discrete Mathematics, Tata McGraw Hill, 1995