Discrete Mathematics: Lectures 6 and 7
Sets, Relations, Functions and Counting

Instructor: Arijit Bishnu Date: August 4 and 6, 2009

Our main goal is here is to do counting using functions. For that, we need to have some basic understanding of sets, relations and functions. This notes is mainly based on [1, 2, 3, 4].

1 Sets

A set, as we all know by now, is a collection of elements. We are also familiar with the ways of writing or representing a set. For example, $\mathbb{N} = \{1, 2, \ldots\}$ denotes the set of natural numbers. We would use $\mathbb{N}$ to denote *natural numbers*, $\mathbb{Z}$ to denote the set of *integers*, $\mathbb{Q}$ to denote the set of *rational numbers*, $\mathbb{R}$ to denote the set of *real numbers* and $\mathbb{C}$ to denote the set of *complex numbers*. $\mathbb{N}_n$ denotes the set of *natural numbers* $1, 2, \ldots, n$.

The *cardinality* of a set A will be denoted by $|A|$. A set A is said to be a *finite set* if $|A|$ is finite, i.e. $|A| < \infty$. A set A is said to be a *subset* of B denoted as $A \subseteq B$ if every element of A is an element of B. The *power set* of A, denoted as $P(A)$, is the collection of all subsets of A. If $|A| = n$, $|P(A)| = 2^n$ (why?).

Funny things happen with sizes of infinite sets. Two sets are said to be *equinumerous*, if they have the same cardinality. Two infinite sets can also be equinumerous. Consider the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$. All these four are examples of infinite sets. We can also see the following: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. So, one should expect that $|\mathbb{N}| < |\mathbb{Z}| < |\mathbb{Q}| < |\mathbb{R}|$. But, strangely it so happens that $\mathbb{Q}$ and $\mathbb{Z}$ are equinumerous with $\mathbb{N}$. We would come back to the technique of proving two sets to be equinumerous after studying functions.

Countability of sets is very crucial to the study of computer science. This notion of countability (or its opposite, uncountability!) leads to the fact that computers cannot solve all problems. Just try solving the following *decision problem*: "Given a particular input to a particular computer program, the problem is to determine whether the program will terminate after a finite number of steps on the given input." This problem is known as the *halting problem* and is *undecidable*.

One might observe that we have not defined sets very formally and have relied on an intuitionistic notion. This might give rise to paradoxes like the famous Russell's paradox. To get rid of such paradoxes, set theory has been recast in formal terms where all properties of sets are built from some *axioms*. But, for the sets that we will be considering in this course, no such paradoxes will arise. So, we work with this intuitionistic notion of sets.

2 Cartesian product and relations

2.1 Ordered and unordered pairs

Let us first look at *unordered pairs* and *ordered pairs*. The symbol $\{a, b\}$ denotes the set that contains just the elements a and b. Also, $\{a, b\} = \{b, a\}$, i.e. the elements of the set $\{a, b\}$ can appear in any order. We call $\{a, b\}$ to be an *unordered pair* of a and b. In contrast, for *ordered pairs*, the order of the elements matters. We denote an ordered pair involving a and b as (a, b); $(a, b) \neq (b, a)$. $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. We can similarly have an *ordered n-tuple* involving $a_1, a_2, \ldots, a_n$, which is denoted as $(a_1, a_2, \ldots, a_n)$.

Definition 1 *The* Cartesian product *$A \times B$ of two sets A and B is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. In set-theoretic notations,*

$$A \times B = \{(a, b) |\ a \in A, b \in B\}.$$

If A and B are finite sets, the cardinality of $A \times B$ is $|A| \cdot |B|$. Is $A \times B = B \times A$? No, as the operation is not commutative.

2.2 Relation

Definition 2 *A* Relation *is a set of ordered pairs. Given two sets A and B, any subset of the Cartesian product $A \times B$ is called a* relation *between A and B. We denote a relation R from A to B as $R : A \to B$.*

If an ordered pair (a, b) belongs to a relation R, i.e. $(a, b) \in R$, we say that a and b are related by R. We also denote it as aRb. If $A = B$, then $R : A \to A$ is a relation from A to itself.

Example 1 *Let us consider equality (=). We can define equality as a relation $R : \mathbb{N} \to \mathbb{N}$. R contains $\{(1, 1), (2, 2), (3, 3), \ldots\}$. Similarly, we can define 'less than equal to' ($\leq$) as a relation, the set being $\{(2, 1), (3, 2), (3, 1), (4, 3), (4, 2), (4, 1), \ldots\}$.*

How many possible relations can there be? Any subset of a Cartesian product is a relation. Hence, the possible number of relations is $2^{|A| \cdot |B|}$.

Let A, B, C be sets with the following relations: $R : A \to B$, $S : B \to C$. The *composition* of relations R and S, denoted as $R \circ S$, is the relation $T : A \to C$ defined as follows: for given $a \in A$ and $c \in C$, aTc holds if and only if there exists some $b \in B$ such that aRb and bSc.

A relation can satifsy some conditions and based on that we can have special types of relations.

Definition 3 *We say that a relation R on a set A is*

reflexive *if $(a, a) \in R$, $\forall a \in A$,*

symmetric *if* $(a, b) \in R$ *implies* $(b, a) \in R$, $\forall a, b \in A$,

transitive *if* $(a, b) \in R$ *and* $(b, c) \in R$ *imply* $(a, c) \in R$, $\forall a, b, c \in A$.

antisymmetric *if* $(a, b) \in R$ *and* $(b, a) \in R$ *imply* $a = b$, $\forall a, b \in A$.

2.2.1 Equivalences

A special type of relation is known as *equivalence*.

Definition 4 *We say that a relation R on A is an equivalence on A if its reflexive, symmetric and transitive.*

Example 2 *Let T be the set of all triangles in the plane. We say that two triangles $t_1, t_2 \in T$ are related, i.e. $(t_1, t_2) \in R$ if and only if they are congruent. Two triangles are congruent if one can be transformed into the other by translation and rotation. Clearly, R is an equivalence relation.*

Example 3 *Let $T = \{(a, b) |\ a, b \in \mathbb{N},\ \text{and } a = b\}$. Clearly, T is an equivalence relation.*

Exercise 1 *Consider the following statement: Suppose R is a relation on X. If R is symmetric and transitive, then R is reflexive. As a proof of the above statement, consider the following. Let x be an arbitrary element in X. Let $y \in X$ such that $(x, y) \in R$. Since, R is symmetric, $(y, x) \in R$. Now, since $(x, y) \in R$ and $(y, x) \in R$, by transitivity, $(x, x) \in R$.*

If what has been proved is correct, then for equivalences, the reflexivity condition is redundant.

Solution: There is a fallacy in the argument. The basic fallacy is to assume that such a y exists. It is possible that there is an $x \in X$, that is not related to anything else by R. No such R will be reflexive. Consider the empty relation on any non-empty set X. It is symmetric and transitive but not reflexive.

Consider also an example. Let $R = \{(a, a), (a, b), (b, a), (b, b)\}$ on $X = \{a, b, c\}$. R is symmetric and transitive but $(c, c) \notin R$, so R is not reflexive. ■

The notion of *equivalence class* is related to equivalence. The equivalence classes form a *partition* of the set A. A *partition* of A is a collection of non-empty disjoint subsets of A whose union equals A.

Let R be an equivalence on a set A and let $a \in A$. Now, $R[a] = \{b |\ b \in A \text{ and } (a, b) \in R\}$. $R[a]$ denotes the equivalence class of R determined by a.

Exercise 2 *For any equivalence R on A, prove the following:*

(i) $R[a]$ *is non-empty* $\forall a \in A$.

(ii) For any two elements $a, b \in A$, *either* $R[a] = R[b]$ *or* $R[a] \cap R[b] = \emptyset$.

(ii) The equivalence classes determine the relation R uniquely, i.e. if R_1 and R_2 are two equivalences on A and if the equality $R_1[a] = R_2[a]$ holds for $\forall a \in A$, then $R_1 = R_2$.

Equivalence class induces a pairwise disjoint partition of A whose union is A. Conversely, any partition of A determines exactly one equivalence on A. That is, there exists a bijective mapping of the set of all equivalences on A onto the set of all partitions of A.

2.2.2 Ordered sets

Definition 5 *A partial order R on A is a reflexive, antisymmetric and transitive relation on A.*

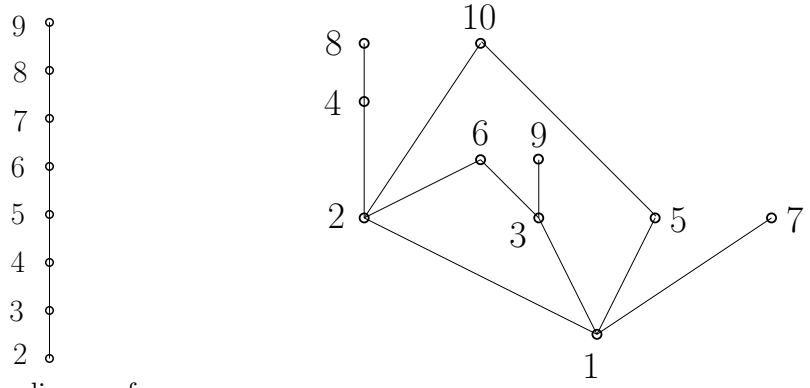
An ordered set is a pair (A, R), where A is a set and R is an ordering on A. This is also refered to as *partially ordered set*s or *poset*s. Examples of ordered sets are $(\mathbb{R}, \leq)$ and $(\mathbb{N}, \leq)$.

If for any two distinct elements $a, b \in A$, either $a \leq b$ or $b \leq a$ holds, then A is said to have a *linear ordering* or a *total ordering*. The sets $\mathbb{R}$ and $\mathbb{N}$ admit a linear ordering. Consider the following relation $R_|$ on $\mathbb{N}$:

$$R_| = \{(a, b)|\ a, b \in \mathbb{N} \text{ and } \exists \text{ a } c \in \mathbb{N}, \text{ such that } b = ac\}.$$

Exercise 3 *Verify whether $R_|$ is both a partial ordering and linear ordering on $\mathbb{N}$.*

Exercise 4 *Let A be a set and 2^A denotes the system of all subsets of the set A. Does the relation "$\subseteq$" define a partial ordering on 2^A?*



(a) Hasse diagram for $(\{2, 3, 4, 5, 6, 7, 8, 9\}, \leq)$.

(b) Hasse diagram for $\mathbb{N}_{10}$ ordered by divisibility.

Figure 1: Examples of Hasse diagram.

Hasse diagram: Partially ordered sets can be pictorially represented by *Hasse diagram*. Here the conditions can be represented by arrows. But, not all arrows are

to be drawn. If R is a partial order and $(a, b) \in R$ is represented as an arrow from a to b and $(b, c) \in R$ is also represented as an arrow b to c, then we may omit the arrow from a to c and take it as implicit. Similarly, we can forget about loops as we can assume they are always there. Also, if we always draw the ordering relation from top to bottom, we can get rid of the arrows and represent the relations using line segments. It can be proved that for finite posets, all the information is captured by the relation of *immediate predecessor*. The ordering can be reconstructed from the immediate predecessor relation. We omit the proof. One can go through [1] for the proof. The relation of *immediate predecessor* is the basis of drawing the Hasse diagram.

3 Function

We look at functions and its use in counting. Let us first define a *function*.

Definition 6 *A function f from the set A to B is a relation from A to B satisfying the following condition:*

- *for each $a \in A$, there exists a unique $b \in B$ with $(a, b) \in f$.*

The set A is the domain *of f and B is the* codomain *or* range *of f. A function f from A to B is denotes as $f : A \to B$.*

If $A = \emptyset$, then the only function from A to B is the empty set. On the other hand, if $A \neq \emptyset$ and $B = \emptyset$, then there are no functions. If both A and B are non-empty, then there are $|B|$ choices for each element of A. So, the total number of functions possible is $|B|^{|A|}$. Look at the following algebraic inequality. Is it true that $y^x \leq 2^{xy}$ for all positive integers x and y? Set $|A| = x$ and $|B| = y$ and use the fact that the number of functions has to be less than equal to the number of relations as function is a special type of relation.

Now, for some special types of functions.

Definition 7 *Let A and B be two non-empty sets. The function $f : A \to B$ is*

- *a one-to-one or injective function if no two elements of A are mapped to the same element of B, i.e. for $a, b \in A$ and $f(a), f(b) \in B$, $a \neq b$ implies $f(a) \neq f(b)$.*
- *a onto function or surjective function if for every $b \in B$ there exists $a \in A$ satisfying $f(a) = b$.*
- *a bijective function if f is both one-to-one and onto.*

If f is a bijection, then its converse denoted as f^{-1} is called the inverse *of f. The bijections are the only functions for which the 'converse relation' is also a function. Note that, if f is a bijection, then $f(a) = b$ if and only if $f^{-1}(b) = a$.*

Exercise 5 *Let $f : A \to B$ and $g : B \to C$ be two functions. Prove the following:*

(i) if f and g are one-to-one functions, then $g \circ f$ is also a one-to-one function.

(ii) if f and g are onto functions, then $g \circ f$ is also a function onto.

(iii) if f and g are bijective functions, then $g \circ f$ is also a bijective function.

(iv) Show that any function can be written as a composition of a one-to-one function and an onto function.

3.1 Functions and counting

We now look at the relations between the cardinalities of the sets satisfying a functional mapping and then explore what we promised at the very beginning: "counting is possible by transforming the problem to functions'.

Observation 1 *Let A and B be two sets such that $f : A \to B$ where f is a one-to-one function. Then, $|A| \leq |B|$.*

Observation 2 *Let A and B be two sets such that $f : A \to B$ where f is a function onto. Then, $|A| \geq |B|$.*

These two observations intuitively points to some relation about the cardinality of two sets having a bijection. In effect, there exists a theorem that says two sets are equinumerous if and only if there is a bijection between them. We state it without the proof. Interested students might look at [4].

Theorem 1 (Cantor-Schröder-Bernstein theorem) *Two sets A, B are equinumerous if and only if there exists a bijection $f : A \to B$ between them.*

Let us look at the following two problems that is already known to you from your high school days.

Problem 1 *How many 4-letter words can be formed using smaller case English alphabets?*

Problem 2 *How many 4-letter words can be formed using smaller case English alphabets where all letters are distinct?*

Well, you all know. The solution to Problem 1 is 26^4 as all four places can be filled up in 26 ways. The solution to Problem 2 is $26 \cdot 25 \cdot 24 \cdot 23$. Let us recast these problems in terms of functions. Let $A = \{w_1, w_2, w_3, w_4\}$ and $B = \{a, b, \ldots, z\}$. Here, $|B| = 26$ and $|A| = 4$. The solution to Problem 1 is nothing but counting the number of possible mappings of the function $f : A \to B$ which we know to be $|B|^{|A|}$. What about a formal proof?

Proposition 1 *Let A and B be two sets with $|B| \geq 1$. Then, the number of all possible mappings $f : A \to B$ is $|B|^{|A|}$.*

Proof: As the basis of induction, we have the function $f : \emptyset \to B$. Here, f will be the empty set as no ordered pairs are there. So, we have exactly 1 mapping. Under the assumption that A and B are non-empty sets, we could have proved the basis of the induction with $|A| = 1$ also. Then also there is only 1 mapping. The rest of the proof is left as an exercise. Sketch of the proof was discussed in the class. ■

Exercise 6 *How many boolean functions are possible with n boolean variables?*

Exercise 7 *How many subsets does a set A with $|A|$ have? Prove using the concept of functions.*

Solution: Consider any arbitrary set $A' \subseteq A$. Define a mapping $f_{A'} : A \to \{0, 1\}$ as follows. For, an element $a \in A$, we have

$$f_{A'}(a) = \begin{cases} 1 & \text{if } a \in A; \\ 0 & \text{if } a \notin A. \end{cases}$$

Distinct sets A' have distinct mappings $f_{A'}$. Conversely, any given mapping $f : A \to \{0, 1\}$ determines a subset $A' \subseteq A$ with $f = f_{A'}$. So, the number of mappings, which is $2^{|A|}$, is the same as all possible subsets of A. ■

What about the solution to Problem 2? Again, let $A = \{w_1, w_2, w_3, w_4\}$ and $B = \{a, b, \ldots, z\}$. The solution to Problem 2 is nothing but counting the number of possible injective mappings $f : A \to B$. Let us now count the number of possible injective maps from a set A, with cardinality $|A|$, to a set B, with cardinality $|B|$.

Proposition 2 *Let A and B be two non-empty sets with $|A|, |B| > 0$. Then, the number of all possible one-to-one or injective maps $f : A \to B$ is*

$$|B| \cdot (|B| - 1) \cdots (|B| - |A| + 1) = \prod_{i=0}^{|A|-1} (|B| - i).$$

Proof: We proceed by induction on $|A|$. First notice that, with $|A| > |B|$, there exists no (i.e. 0) injective map. The formula tallies with that. For the basis of the induction, with $|A| = 1$, there are $|B|$ choices for an element $a \in A$ to be mapped to an element in B. This also tallies with the formula.

Let, now $|A| \geq 1$ and $|B| \geq |A|$. The proof sketch is as follows. Fix $a \in A$ and choose $f(a) \in B$ arbitrarily in one of $|B|$ possible ways. To complete the injective function, next we need to find an injective map from $A \setminus a$ to $B \setminus f(a)$. The number of such inductive maps, by the induction hypothesis, is $(|B|-1)(|B|-2)\cdots((|B|-1)-(|A|-1)+1)$. Thus, the final result is the product of $(|B|-1)(|B|-2)\cdots(|B|-|A|+1)$ and $|B|$, i.e. $\prod_{i=0}^{|A|-1}(|B| - i)$. ■

Next, we introduce counting using bijections.

Example 4 *Let A be a set with cardinality $|A| = n \geq 1$. Show that A has exactly 2^{n-1} subsets of an odd size and exactly 2^{n-1} subsets of an even size.*

Solution: Fix an element $a \in A$. We know from Exercise 7, that the number of subsets of an n-element set is 2^n. So, the number of subsets of the set $A \setminus \{a\}$ will be $2^{(n-1)}$. Our idea is to set up a bijection between *all subsets of* $A \setminus \{a\}$ **AND** *all odd-sized subsets of* A.

Any subset $A' \subseteq A \setminus \{a\}$ can be extended to another subset $A'' \subseteq A$, such that A'' is odd-sized, as follows:

1. if $|A'|$ is odd, set $A'' = A'$;
2. if $|A'|$ is even, set $A'' = A' \cup \{a\}$.

One can easily verify that the above rule is a bijection between *all subsets of* $A \setminus \{a\}$ **AND** *all odd-sized subsets of* A. Hence, the result. ■

Exercise 8 *How many 8-digit sequences consisting of digits 0 to 9 are there? How many of them contain an even number of odd digits?*

References

[1] J. Matoušek and J. Nešetřil, *Invitation to Discrete Mathematics*, Oxford University Press, New York, 1998.

[2] C. L. Liu, *Elements of Discrete Mathematics*, Tata McGraw Hill, New Delhi, 2000.

[3] Martin J. Erickson, *Introduction to Combinatorics*, Wiley-Interscience Publication, John Wiley & Sons.

[4] Abhijit Das, *Sizes of sets*, Personal communication.