CS5130 : Mathematical Tools for Theoretical Computer Science

(Scribe Lecture Notes)

Lecturer : JAYALAL SARMA

Department of Computer Science and Engineering
Indian Institute of Technology Madras (IITM)
Chennai, India

Last updated on : September 30, 2020

Preface

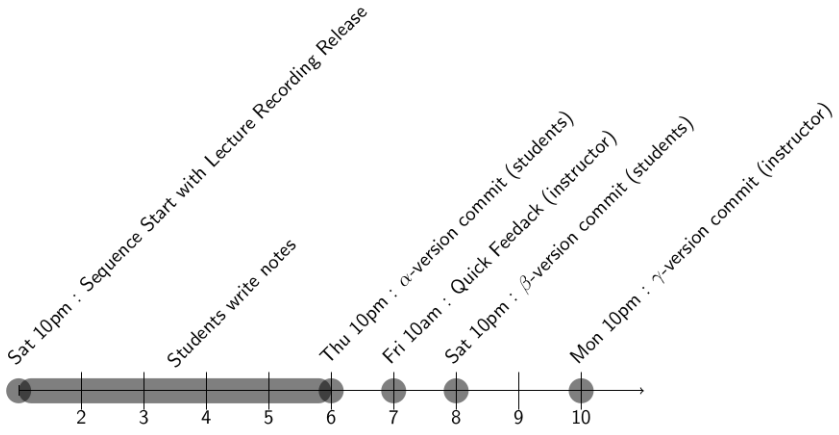
This lecture notes are produced as a part of the course CS5130: Mathematical Tools for Theoretical Computer Science which was a course offered (during the online semester Sep-Dec 2020) at the CSE Department of IIT Madras.

Acknowledgements

We acknowledge the efforts of the scribes and editors of this document.

Scribe status

Each lecture has a field called **status**. It tells which stage of the edit pipeline is the document currently. The scribe notes are due on Thursdays and Saturdays as per the following timeline.



Even after these edits, it is possible that there are still errors in the draft, which may not get noticed. If you find errors still, please report to the instructor.

List of Scribes

Table of Contents

Todo list

Instructor : Jayalal Sarma
Scribe : Jayalal Sarma (*TA:* JS)
Date : Sep 9, 2020
Status : α

Lecture
1

Pigeon Hole Principle and Basic Applications

We start course with the simplest but surprising powerful tool in combinatorial arugments which is the pigeon hole principle. Through this principle as an example, we will also quick review the methods of proof.

1.1 Quick Recap on Proof Techniques

A formal mathematical proof system in our context has axioms about various mathematical objects that we are using, like numbers, graphs which describes them through their properties. Then, there are rules of inferences such as modus ponens, modus tollens, resolution, syllogisms etc which helps us derive new statements from these axioms.

The peculiarity of these rules of inferences are that they "conduct truth" and forms building blocks for huge "truth conducting" structures called mathematical proofs. That is, if for any object[1], the premises of the rules of inference are true, then the conclusion is also true for them. Hence, suppose we derive a statement ϕ starting with the axioms, applying the rules of inferences in various combinations. Since the individual rules of inferences "conduct truth", the resulting structure also conducts truth and is called the mathematical proof of the statement ϕ from the axioms. Note that the truth of the statement ϕ for the object under consideration can be stated on relative to the truth of the axioms that we used. However, this is not a concern, since we are intending to use the mathematical proof systems to derive statements about objects which we know would satisfy the axioms (in fact, we wrote down axioms as properties of those objects.

Curiosity 1.1.1. It is an amusing question to ask, whether there are other objects, which we did not intend to, which also satisfies the axioms that we wrote, by accident. Say for example, we wrote the axioms for graphs, but "strings" also satisfies them. If so, the theorems that we prove for graphs using only those axioms will also be true for strings, automatically !!. Quite interestingly this is true for natural numbers. The mathematical theory of natural numbers is axiomatized by what are called the Peano's axioms. There are numbers that one can define which are different from natural numbers for which any theorem that we prove for natural numbers also are true

[1] a little more formally, the assignment in the propositional logic, and model in general first oder logic

(because they satisfy the Peano's axioms). Then one might ask, are we not trying to represent exactly natural numbers? So should we not augment Peano's axioms with more properties of natural numbers such that we remove such *unwanted* parallel models from satisfying the axioms we write. Even more interestingly, one can argue that this is not even possible. No matter, what extra formula we write the existence of such "parallel models" us inevitable. In fact, not just one "parallel model", there will be infintiely many of them. You should read about *Löwenheim–Skolem theorem*.

Writing down mathematical proofs explicitly by using rules of inference may seem to be a mechanical way of proving statements. While it avoids any chance of mistakes because of the mathematical precision and rigor it affects quick readability and communication of ideas. Hence, one would like to have more "human readable" ways of representing these proofs by writing some of the steps in English, while ensuring that we do not lose the mathematical rigor. This brings in some subjectivity about how "formal" a proof is - that is, how close is it to the formal mathematical framework of rules of inferences in terms of notations, presentation etc. Sometimes, very rigorous proofs tend to hide the intuitive idea behind the proof which one tends to (and sometimes need to) describe separately for easy communication. The more formal your proof is, the less chances of you making a logical error in the proof. It is a good idea to start writing proofs with the mindset of "rigor extremist" and once you are comfortable and see through the mathematically rigorous steps of a statement, you can rely more in English sentences. This course particularly would do it in the latter way, but ensuring that mathematical rigor is kept in tact. The beauty of the combinatorial proofs lies in the elegance and the combinatorial insight and intuition. Balancing the intuition with rigor in presentations and descriptions lies in the art of presentations.

Suppose that we have to prove a statement γ of the form $p \to q$. We quickly recall the different ways of proof in the above described form.

Direct Proof: Assume p and then derive q using the assumption and the axioms by applying the rules of inferences. The is considered as a proof of the statement $p \Rightarrow q$ since it can be associated with a valid argument form by itself.

Indirect Proof: Assume $\neg q$ and then derive $\neg p$. Again, this is also considered as a proof of the statement $p \Rightarrow q$ since it can be associated with a valid argument form by itself. This is also called proof by *contrapositive*.

Proof by Contradiction: A proof by contradiction, assumes the negation of the statement to be proven (that is, $\neg\gamma$) and then defined a statement r (this forms a part of creativitiy of the proof), and then derives $r \wedge (\neg r)$ from the assumption and axioms using the rules of inferences. By an associated valid argument form, this shows that γ must be true, again, by associating the definition of a valid argument form.

In addition, while proving quantified statements, there are a few additional ideas that are used which we quickly review below:

Proof by Exhaustive Cases: Suppose we want to derive a statement Γ of the form $\forall \alpha P(\alpha)$ where α comes from domain of discourse $\mathcal{D}$ (say, for example, α is a natural number, that is, $\mathcal{D} = \mathbb{N}$). We can partition $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2 \ldots \cup \mathcal{D}_k$ into several subdomains and prove the statement $\forall \alpha \in \mathcal{D}_i,\ P(\alpha)$ separately. Each part of the proof $\forall \alpha \in \mathcal{D}_i P(\alpha)$ is said to be a "case" of the proof. The fact that, $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_1 \ldots \cup \mathcal{D}_k$ is what is meant by the statement that the case analysis is *exhaustive*.

Proof by "Counter Example": Suppose we want to disprove statements of the form $\forall \alpha P(\alpha)$. That is, we want to derive $\neg (\forall \alpha P(\alpha))$ which is logically equivalent to $\exists \alpha \neg P(\alpha)$. Hence it suffices to demonstrate an α in the domain for which we can show $P(\alpha)$ is false.

Proof by Mathematical Induction: This is a technique to prove statements of the form $\forall \alpha P(\alpha)$ where the domain $\mathcal{D}$ is countably infinite. That is, the domain $\mathcal{D}$ can be put in bijection with the set of natural numbers. The technique forms part of the Peano's axioms that define the natural numbers and hence is a valid proof technique. If $\phi : \mathbb{N} \to \mathcal{D}$ is a bijection, in order to prove $\forall \alpha P(\alpha)$, we can equivalently prove $\forall n \in \mathbb{N}, P(\phi(n))$. In particular, it takes the following form: *If we can prove* $P(\phi(0))$ *and the implication* $[\forall n \in \mathbb{N}, P(\phi(n)) \Rightarrow P(\phi(n+1)]$ *then we can conclude* $\forall n\ P(\phi(n))$. There are versions of this proof techniques such as strong induction, structural induction, spiral induction, double induction etc which are adaptations of the above basic idea.

Most of the proofs that we do in the courses will follow one of the above frameworks. We will not do examples of these techniques since that is already covered in the basic discrete mathematics course.

1.2 The Pigeon Hole Principle (PHP)

With the quick recap done in the previous part, we now plunge into the actual business in this lecture. We first prove the following basic version of the Pigeon hole principle.

Theorem 1.2.1. *Let $n, k \in \mathbb{N}$, such that $n > k$. Suppose we place n identical balls in k identical bins, then there is a bin that has at least two balls in it.*

Proof. Let $n, k \in \mathbb{N}$ and $n > k$. Assume for the sake of contradiction that when we placed the balls into the bins as indicated in the theorem, there was no bin with at least two balls in it.

As such the bins are identical, but number them from 1 to k now. Using this notation, let us define b_i to be the number of balls that went into the bin number i. Clearly $\forall i, b_i \geq 0$. Since we did distribute all the balls into the bins, we have :

$$\mathcal{R} : \sum_{i=1}^{k} b_i = n$$

Using the assumption, we have that: $\forall i, 0 \leq b_i \leq 1$. Summing up for i: $\sum_{i=1}^{k} b_i \leq \sum_{i=1}^{k} 1 = k < n$. Hence we have derived the statement :

$$\neg\mathcal{R} : \sum_{i=1}^{k} b_i \neq n$$

Hence we have derived $\mathcal{R} \wedge \neg\mathcal{R}$. This is a contradiction and hence the original assumption that we started out with must be false and hence there has to exist a bin which has two balls in it. □

Curiosity 1.2.2. The formal proof of PHP as simple as it sounds is still a subject of substantial research in an area called *proof complexity*. To demonstrate this, let us write the principle itself in more rigorous notations. Let $n > k$, and $\{x_{ij} \mid i \in [n], j \in [k]\}$ be propositional variables (which can be called, say *pigeon hole variables*). Following our original notation, where there are n pigeons and k holes, the basic Pigeon Hole Principle is the following Disjunctive normal form formula :

$$\text{PHP}_k^n \stackrel{\text{def}}{=} \left(\bigvee_{i \in [n]} \bigwedge_{j \in [k]} \overline{x_{ij}} \right) \vee \left(\bigvee_{j \in [k]} \bigvee_{r \neq s \in [n]} (x_{rj} \wedge x_{sj}) \right)$$

To prove this, one possibility is to derive the contradiction from the negation of PHP_k^n. This is an expression in conjunctive normal form, with clauses:

$$\text{For } i \in [n] \text{ the clauses : } Q_i \stackrel{\text{def}}{=} \bigvee_{j=1}^{k} x_{ij}$$

$$\text{and for } s \neq t \in [n], j \in [k] \text{ the clauses } Q_{s,t,j} \stackrel{\text{def}}{=} \overline{x_{sj}} \vee \overline{x_{tj}}$$

Intuitively, these say that there is a function from $[n] \to [k]$ (which is represented by $x_{ij} = 1$ to mean that the function takes i to j) which is well defined (for every i, there exists a j such that $x_{ij} = 1$) and also injective (for two different s and t, it is not the case that x_{si} is 1 and x_{tj}). Since $n > k$, there cannot be an injection, and hence the negation of the conjunction of these clauses PHP_k^n must be true.

Suppose we ask, starting from these clauses as axioms, and applying rules of inferences (say the resolution principle) alone, how many steps of proof does one need to do to derive the contradiction ($r \wedge \neg r$ for some r). [2]. We measure this in terms of n and k which determines the number of variables in the system. The area which studies the complexity of proofs in the above is called *proof complexity theory*. It turns out the the basic PHP itself is one of the tautologies for which one requires exponentially long proofs if we are restricting ourselves to resolution? What if we relax this? The area has several interesting open questions related to this and they have close connections to computational complexity theory too.

[2]Notice that this sounds exactly like computation, how many steps of computation is required in order to certain tasks in terms of input parameters

1.2.1 A Quick Example:

We will now demonstrate the application of the principle itself by a quick example. This is meant to be a revision of the topic from the previous courses and hence it is very much possible that you have seen the application earlier.

Theorem 1.2.3. *If you consider any five points placed inside the unit square then there must necessarily exist two points are at most* 0.75 *unit away from each other.*

Proof. Firstly, to make it sound less magical, let us comment that theorem is actually true for 0.75 units replaced by 0.707 units which is actually $\frac{1}{\sqrt{2}}$. The application of PHP goes as follows. Consider four small squares which are obtained by the midpoint of the square as one of the corners. These small squares form the bins and the five points that we place forms the balls. By applying PHP, we conclude that there must be two points which falls into the same small square. Now the argument can be completed by the fact that the maximum distance between any two points which are in the same small square is at most $\frac{1}{\sqrt{2}}$ since the sides of the square are $\frac{1}{2}$ each. □

Remark 1.2.4 (Tightness). *Is the above theorem tight? Can it be improved? Improvement can be in terms of two parameters. Firstly, can we make the same claim for 4 points? Secondly, even for 5 points, can we make an improved claim about the minimum distance being, say 0.7 units? The answer to both these questions are no. For the first, we can demonstrate 4 points in which every pair is at least one distance away - the four corners themselves will serve as a counter example. For the second question, we can demonstrate 5 points which are actually only pairwise at least* $\frac{1}{\sqrt{2}}$ *distance away.*

Remark 1.2.5 (Glimpse of Extremals in Combinatorics). *The above example theorem, while is a classical application of Pigeon Hole Principle, it also demonstrates a curious phenomenon. In spirit it says that if there are large number of objects in a collection, then there must be some structure. Question is how large? And what is structure? The answers to these vary and forms the foundations of this area. We will see more of this when we see Ramsey Theory.*

1.3 Numbers and Remainders

It is customary to do an example of PHP from numbers and division under remainders. We will do a slightly unusual example.

Theorem 1.3.1. *Consider the infinite sequence* $7, 77, 777, \ldots, 7777777, \ldots$ *- there must necessarily exist a number in this sequence that is divisible by 2003.*

Proof. As weird as it sounds, one might wonder how does PHP play a role. There does not seem to be any place to apply PHP directly in the statement of the problem. Indeed, infinitude seems to indicate that we are allowed to take large numbers in the sequence. A usual trick is the division, and then consider the remainders.

As a start, consider first 2003 numbers in the sequence. Denote them by $n_1, n_2, \ldots n_{2003}$. Divide them by 2003 and collect the remainders that we see. Denote them by $a_1, a_2, \ldots, a_{2003}$. If any of the a_is are 0, then we are done since that Indeed, we have that $1 \leq a_i \leq 2002$. Clearly, now the pigeons and holes are visible now. The numbers n_is are the pigeons and the reminders are the holes. There are only 2002 holes but there are 2003 pigeons and hence by PHP, there must exists $1 \leq i < j \leq 2003$ such that $a_i = a_j$. This gives:

$$n_i \mod 2003 = n_j \mod 2003 \tag{1.1}$$

$$(n_i - n_j) \mod 2003 = 0 \tag{1.2}$$

$$2003 \text{ divides } (n_i - n_j) \tag{1.3}$$

$$\tag{1.4}$$

That is good progress. We managed to show 2003 divides $(n_i - n_j)$. However, $n_i - n_j$ unfortunately, will not be in the sequence at all. How will this number look like? By the structure of the numbers, subtracted, this difference will be a number of 7s and then several zeros. More precisely computing these number, we have that:

$$(n_i - n_j) = n_{j-i}10^{j-i}$$

So we have that 2003 divides the product of n_{j-1} and 10^{j-i}. However, 2003 being an odd number which is not a multiple of 5 will not have a common factor with any power of 10. Hence 2003 must necessarily divide n_{j-i} which should be there in the sequence. This completes the proof. □

1.4 Graphs

Our third application is related to problems that can be modelled as graphs.

Theorem 1.4.1. *In any chess tournament, where there are n participants, at any point of time there must be two participants who finished the same number of games in the tournament.*

It is natural to model this situation as a graph with n vertices where each vertex represents a participant and we put an edge between two vertices if player i and player j have played a game with each other. The number of games played by a player is exactly the degree of the vertex in this graph. Rewriting the above theorem in the new language now:

Theorem 1.4.2. *In any undirected graph G, there must be two vertices which are having the same degree.*

Proof. The proof is by an exhaustive case analysis. We need to argue the above for all graphs. We divide this domain into two based on whether there is an isolated vertex or not.

Case 1 : G has an isolated vertex - In this case, there is a vertex of degree 0, and hence there cannot be a vertex of degree $n - 1$. Thus we have n vertices, and only $n - 1$ possible degree values $\{10, , 2, \ldots n - 2\}$. By the PHP, we must see two vertices which has the same degree.

Case 2: G **does not have an isolated vertex** - In this case, there is no vertex of degree 0, and hence the degree values of vertices can only be in the set $\{1, 2, \ldots n-1\}$. Again we have n vertices whose degrees take only $n-1$ possible values. Again, by PHP, we must see two vertices having the same degree.

□

Exercise 1.5 (See Problem Set 1 (Problem 1))**.** A social network is said to be symmetric if the relation between users that is maintained as a part of the network, is symmetric. Consider a symmetric social network and let the symmetric relation maintained be that of "user A and B are *friends*" (like in the case of facebook). A user C is said to be a *mutual friend* of users A and B if, C is a friend of both A and B. Prove that - for any user A of the network who has at least two friends, there must exist two friends of A who has the same number of mutual friends with A.

Comment on whether symmetry is critical for your argument. Take the example of *instagram* where the symmetric relation of *friends* is replaced by *followers*. Generalize the definition of mutual friends to *mutual followers*. Comment on whether a similar statement for followers can be established in this case.

1.6 Discussion Session

Just to get started, we considered the following question - *how many people do we need to choose so that we can be assured that two among the set of people we have chosen will have their birthday on the same day?* The answer to this question is given by Pigeon Hole Principle immediately by considering the people to be pigeons and the day of the year on which their birthday falls to be the pigeonhole. Hence to be guaranteed that out of the 366 holes, at least one contains two pigeons (people), and hence having the same birthday, we need to choose 367 people. Just to test our understanding, we asked "is the theorem tight?" in terms of number of people. It is indeed is, since there is a set of 366 people whom you can choose all of whom have different birthdays. That is, 367, is the smallest number for which the above statement can be proposed. Hence the theorem is tight.

The first discussion point that was raised was a comparison with Birthday paradox. If we do not choose 367 people we are not given the guarantee that there are two people in the set with same birthday. What if we don't want this guarantee with certainty - but instead, we will need to get a probabilistic guarantee. To formalize this one has to imagine an experiment where the people are chosen uniformly at random. More rigorously, the property of the distribution is that for every date of the year, the probability that the chosen person has a birthday on that day is $\frac{1}{365}$. Let us say, we are talking about a non-leap-year. The questions is then of the form *what is the minimum number of people we need to choose, as per the above experiment, such that we are guaranteed at least 99.999% chance of getting two people with the same birthday in the set?*. A natural number to choose is 364 which is slightly less than 365. But what is the minimum? The answer beats our usual intuition and is surprisingly low - we need to choose only 70 people to achieve this !!. The

surprise goes even further if we ask for 50% success, then the number is just 23 !! - and hence this is called *the birthday paradox*.

1.6.1 Impossibility of Perfect Lossless Compression

PHP has a variety of applications. A first application outside discrete math course, that we usually encounter is in the automata theory where we use it to prove the pumping lemma. In fact, this one principle is pivotal in showing that there *cannot be* finite automaton accepting certain languages.

We then turned into a practically related application of PHP, in the context of file compression. We all have used file compression programs - say like zip or tar. They compress our files into smaller sizes and they usually provide compression ratio too. Here is a question out of curiosity. Can we give compression algorithm that is guaranteed provide compression for all the files? This is a natural requirement. Interestingly, the actual situation is worse, any compression algorithm, not only cannot reduce the size of all files, but also has to increase the size of some file. The argument uses PHP.

Compression algorithms are nothing but programs which translates files (which are interpreted as strings) to strings. That is, they are functions of the form $C : \Sigma^* \to \Sigma^*$. A compression algorithm is said to *lossless* if this function is injective. That is, given a compressed strings (element in the RHS) we have a unique file that we can decompress it to. Indeed, compression algorithms that are not lossless are practically useless since there cannot exist decompression algorithms which can recover the compressed file.

Theorem 1.6.1. *For any lossless data compression algorithm that makes at least one file smaller, there will be at least one file that it makes larger.*

Proof. Let C be the compression function from $\Sigma^* \to \Sigma^*$. Let us fix $\Sigma = \{0, 1\}$ without loss of generality. Suppose it makes at least one file smaller than its size as a result of the compression. In addition, for the sake of contradiction, suppose that the algorithm does not make any file larger than their respective sizes. Let $w \in \Sigma^*$ be the shortest string (say, $|w| = \ell$) which the algorithm makes smaller. That is, by the assumption, for $w' \in \Sigma^*$ such that $|w'| < |w|$, $|C(w')| = |w'|$. Thus, consider the following set :

$$\Gamma = \{w \in \Sigma^* \mid |C(w)| < \ell\}$$

From the above assumptions, we have that $|\Gamma| \geq 2^\ell + 1$, but then by definition $\Gamma \subseteq \{0, 1\}^{\ell-1}$. Hence by Pigeon Hole Principle, $\exists w, w' \in Gamma$ with $w \neq w'$, such that $C(w) = C(w')$. This contradicts the lossless property. ∎

Instructor : Jayalal Sarma
Scribe : Jayalal Sarma (*TA:* JS)
Date : Sep 9, 2020
Status : α

Lecture
2

More on PHP

2.1 Warm up and Generlizations of PHP

We start with a usual application of PHP to numbers to warm up in the lecture.

Theorem 2.1.1. *In any set of $n+1$ positive integers each at most $2n$, there must exist at least one number which divides the other.*

Proof. Let $S = \{a_1, a_2, \ldots, a_{n+1}\}$ be the set of $n+1$ positive integers such that $a_i \leq 2n$. Each number can be written in the form $a_i = 2^{k_i} q_i$ where k_i is the maximum power of 2 that divides a_i and q_i hence is an odd number.

Now consider the numbers $q_1, q_2, \ldots q_{n+1}$. Can they be distinct? Since they all are in the range $1 \leq q_i \leq 2n$, where there are only n odd numbers - By an application of PHP, we have that there must exist i, j such that $1 \leq i \neq j \leq n+1$ with $q_i = q_j$. Hence, we have that $k_i \neq k_j$. This gives the two exhaustive cases:

Case 1: $k_i > k_j$: Since 2^{k_j} divides 2^{k_i} and this gives $q_j 2^{k_j}$ divides $q_i 2^{k_i}$. Hence a_j divides a_i.

Case 2: $k_j > k_i$: Same as previous case, just swapping the role of i and j.

In either case, we have that there exists two numbers in the set where one divides the other. This concludes the proof. □

We now state a usual generalization of PHP as a recap.

Theorem 2.1.2 (Generalized of PHP). *Let n, m, r be positive integers and let $n > mr$. If we distribute n balls into m bins, then there must be a bin which has at least $r+1$ balls.*

Indeed, the generalization comes handy when the combinatorial statement that we want to explore is not about a "conflict" but about multiple elements getting to same bag. A simple recap example to demonstrate this is the following question - *how many students do we need to be in the course, such at the end of the semester, no matter how the performance of the students is, that at least five*

students get the same letter grade (out of the five grades S, A, B, C, D, E)? This is also an extremal question. Applying generalized PHP, with $r + 1 = 5$ and $m = 6$, it is sufficient to have 25 students in the class. And with 24 we cannot guarantee this since there is way to distributed 4 students each to each grade so that there are not 5 students having each grade.

2.2 Example 2 : Erdös-Szekeres Theorem

This is about a pattern that appears in sequence of distinct numbers first proved by Erdös and Szekeres in 1939. The theorem its has a geometric interpretation too. The theorem itself is a creative use of Pigeon Hole Principle and is a case of extremal combinatorics.

Theorem 2.2.1. *In any Sequence of $n^2 + 1$ distinct real numbers there must necessarily exist either a strictly increasing subsequence of $n + 1$ numbers or a strict decreasing subsequence of $n + 1$ numbers.*

Before we begin to prove this, let us play around with an example. $8, 11, 9, 1, 4, 6, 12, 10, 5, 7$. Here $n = 3$ and there are 10 numbers in the sequence. There must be at least one strictly increasing subsequence of length 4. Indeed, there is - the subsequence $1, 4, 6, 12$. In fact, there are more, $1, 4, 6, 10$ etc. But anyways there is at least one. In fact, in this case, it so happens that there is a strictly decreasing sequence also of length 4. This is the subsequence, $11, 9, 6, 5$. There are more subsequences.

Proof. The proof is an elegant and intuitive one. A perfect example of how such proofs are discovered. Suppose $a_1, a_2, \ldots a_{n^2+1}$ forms the given sequence of numbers.

Suppose we checked for the increasing subsequence of numbers of length $n + 1$ and for decreasing subsequence of length $n + 1$ but did not find it in the above sequence. How do we formally represent this data? Here is an idea, for each index k, let us associate a pair of numbers (i_k, d_k), which are defined as : the length of longest increasing (for i_k and respectively decreasing for d_k) subsequence of numbers starting from the number a_k in the given sequence. The reason we failed to find the subsequence indicates that these pairs must satisfy, for every k, $1 \leq i_k \leq n$ and $1 \leq d_k \leq n$.

Thus we have n^2+1 tuples in hand where value for each component can be only between 1 and n. Hence there are only n^2 different distinct such pairs possible. But now we have a scenario for PHP, which gives that there must exist $s, t \in [n^2 + 1]$ such that $s \neq t$ (say without loss of generality that $s > t$) such that the tuples for both these indices are the same. That is $i_s = i_t = i$ (say) and $d_s = d_t = d$ (say).

We know that the numbers are distinct in the sequence. Hence $a_s \neq a_t$. Thus we have the following two exhaustive cases:

Case 1: $a_s > a_t$: Let $(t_1, t_2, \ldots t_d)$ be the decreasing sequence of length i that starts from a_t with $t_1 = a_t$. But then $(a_s, t_1, t_2, \ldots t_d)$ is also decreasing and it starts with a_s and is of length $i+1$. This contradicts the fact that $d_s = d$.

Case 2: $a_s < a_t$: Same as the above case, where we replace decreasing with increasing and the final contradiction is for the fact that $i_s = i$, because we can demonstrate a length $i+1$ increasing subsequence of length $i+1$ in the given sequence.

Hence the proof. □

Remark 2.2.2. *The above theorem can also be generalized, and in fact is the original form of the Erdös-Szekeres theorem. For given natural numbers r, s they showed that any sequence of distinct real numbers with length at least $(r-1)(s-1)+1$ contains a monotonically increasing subsequence of length r or a monotonically decreasing subsequence of length s.*

2.3 Example 3: People at Party

If 6 people are invited to a party, something interesting happens. Let us say some pairs of them are friends and some pairs of them are strangers with each other. There will always be some set of three people who are pairwise strangers with each other or there will be a set of three people who are pairwise friends with each other. This phenomenon can be easily mistaken to be a sociological or behavioural psychological fact that humans seem to be behave this way. However, it turns out that it can be seen as a simple result of combinatorics and is a nice applciation of PHP in disguise. We demonstrate this now.

Theorem 2.3.1. *If 6 people are invited to a party, then there must exist three of them who are pairwise strangers each other, and there must be three of them who are pairwise friends with each other.*

There are many equivalent ways of formulating this. One can talk about graphs to model the facts stated above. We defer these to a later point when we get to Ramsey numbers. We now get to the proof of the above in the same language as we discussed above.

Proof. Let P be the set of people who joined the party. Let $\alpha \in P$ be one of the attendees. We do the following case analysis based on how many people does α are friends with in the party. We want to demonstrate a set $\Gamma \subseteq P$ such that $|\Gamma| = 3$ and the members of Γ are either pairwise friends or pairwise strangers.

Case 1: α has atleast three friends in P: Let β, γ, δ be the three friends. We ask the question, are β, γ, δ friends amongst themselves? The answer to this will give the following exhaustive subcases.

- **Case 1a:** β, γ, δ are pairwise strangers among each other: In this case we can simply set $\Gamma = \{\beta, \gamma, \delta\}$ which has the required property for Γ as desired.
- **Case 1b:** there is a pair among β, γ, and δ who are friends : Without loss of generality let us say β and γ are friends (the other cases are similar). In this case, define $\Gamma = \{\alpha, \beta, \gamma\}$ and it has the desired properties.

Case 2: α has at most two friends in P. In this case, there are three strangers for α in P, and let us name them $\beta, \gamma, and \delta$. We ask the question, are β, γ, δ friends amongst themselves? The answer to this will give the following exhaustive subcases.

Case 2a: β, γ, δ are pairwise friends among each other: In this case we can simply set $\Gamma = \{\beta, \gamma, \delta\}$ which has the required property for Γ as desired.

Case 2b: there is a pair among $\beta, \gamma,$ and δ who are strangers : Without loss of generality let us say β and γ are the strangers (the other cases are similar). In this case, define $\Gamma = \{\alpha, \beta, \gamma\}$ and it has the desired properties.

Since we argued in both the cases, this completes the proof of the theorem. □

Remark 2.3.2. *A more elegant way to handle case 2 is to reduce it to case 1 itself. Consider the complement of the friends/stranger relation. Note that the result required for the theorem does not change since we just need Γ to be either pairwise strangers or pairwise friends and they just get complemented. Now, if α has at most two friends in P, it has at least three friends in P in the complementary relation and hence we can reuse Case 1 in this case.*

Exercise 2.4. Is the above theorem tight? Indeed, one can construct 5 people going to a party and associate a friends/stranger relation among them such that there does not exist three people who are friends with each other and there does not exist three people who are strangers with each other. The exercise is to explicitly write down this counter example relation.

Exercise 2.5 (See Problem Set 1 (Problem 2))**.** The set M consists of nine positive integers, none of which has a prime divisor larger than six. Prove that M has two elements whose product is the square of an integer. Is the bound 9 in the above statement tight?

Instructor : Jayalal Sarma
Scribe : Jayalal Sarma (*TA:* JS)
Date : Sep 10, 2020
Status : α

Lecture
3

PHP for Dirichlet's Approximation Principle

We now discuss a very old and different application of PHP which predates the name PHP itself. This is to show the approximation principle of irrational numbers. This application got this principle the name as *Dirichlet Box Principle*.

3.1 Approximation of irrationals by rationals

The task we have at hand is about approximating irrational numbers using rationals to a given accuracy. As a concrete example, suppose we want to approximate $\sqrt{2}$ by $\frac{p}{q}$ up to a given accuracy ϵ such that

$$\left|\sqrt{2} - \frac{p}{q}\right| \leq \epsilon$$

the driving question for us, is how large should p and q be? In fact they are related and hence, we need to ask how large the denominator q should be? The larger the q is, the more the granularity of the representation is, and the larger the storage cost is for the number to be represented. Hence, for a fixed irrational number and a given ϵ we want the value of q to be as small as possible.

Indeed, if we want to do this for an arbitrary irrational number, here is a simple idea: let $q \in \mathbb{N}$ (which we will choose later). Divide the number line into intervals of length $\frac{1}{q}$ each. Consider the number α and see which interval it belongs to. Choose the nearest multiple of q to be the $\frac{p}{q}$ to be the approximation of α. A quick thought will convince you that the error introduced by this method is at most half of the interval size which is $\frac{1}{2q}$. That is, for any q that we choose, if we choose p also accordingly as above,

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q}$$

Thus, for a given ϵ, we should choose $\frac{1}{2q} < \epsilon$ to get the required accuracy. In other words, q linearly changes with $\frac{1}{\epsilon}$. Just to get a sense of this growth, if ϵ is given to be 0.0001, then we should choose q to be roughly 5000.

3.2 Dirichlet's Approximation Principle

Indeed, we would have probably preferred a smaller q, due to the above mentioned representation cost. Dirichlet approximation principle, exactly improves the above and is a nice application of the pigeon hole principle.

Theorem 3.2.1 (Dirichlet's Approximation Principle). *For every irrational number α, there is a $p, q \in \mathbb{Z}$ such that:*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

A few remarks about the improvement is due. Indeed, now q changes quadratically with ϵ. To check the numbers, suppose ϵ is given to e 0.0001, then we can afford to choose q to be just 100, as opposed to 5000. We will now prove the above theorem:

Proof. Let α be the irrational number that we are interested in approximating. First observation is that it is sufficient to prove that $\exists p, q \in \mathbb{Z}$,

$$|q\alpha - p| < \frac{1}{q}$$

In other words, we need to understand the nearest integer to the quantity $q\alpha$. Intuitively, the fractional part of $q\alpha$ plays a roles in this and which we will study now.

Fix a positive integer N (we will choose this later) and consider the numbers $0, \alpha, 2\alpha, \ldots N\alpha$. Ideally we will choose q to be less than N, hence one of these numbers is $q\alpha$. However, since we are interested in the fractional parts, let us distribute them into intervals as we did in the naive case.

Consider the interval from $[0, 1)$ divided into subintervals of the form:

$$\left[0, \frac{1}{N}\right), \left[\frac{1}{N}, \frac{2}{N}\right) \ldots, \left[\frac{N-1}{N}, 1\right)$$

There are N intervals in this list. If we distribute the fractional part of $N + 1$ numbers $0, \alpha, 2\alpha, \ldots N\alpha$ to this list, by PHP, we have that there must be two of the multiples of α which falls within the same interval. In other words, there exists $a, b \in \{0, 1, \ldots N\}$ such that:

$$\{a\alpha\} - \{b\alpha\} < \frac{1}{N}$$

Just to fast forward, the idea is to demonstrate that the choice of $q = a - b$ actually works for our purpose. To do this, we will show that the nearest integer to $a\alpha - b\alpha$ is at most $\frac{1}{a-b}$ away from it and that integer will be our p. Since $a - b$ is at most N, it is sufficient to show that there is an integer close to $a\alpha - b\alpha$ is at most $\{a\alpha\} - \{b\alpha\}$ away. By the above, we have that this is at most $\frac{1}{N}$ which in turn is at most $\frac{1}{a-b}$. This is in fact a general statement which we can prove as follows:

Lemma 3.2.2. *Let A and B be two real numbers, there is an integer p close to $|A - B|$ such that:*

$$d(p, |A - B|) \leq \{A\} - \{B\}$$

where $d(s, t)$ denotes $|s - t|$.

Proof. The idea is very simple, let us write: $A = A_1 + A_2$ and $B = B_1 + B_2$ where A_1 and A_2 are integral and fractional part respectively. If $A_2 > B_2$, then the distance to the integer $|A_1 - B_1|$ is at most $A_2 - B_2$. The other case works in a similar way. □

Applying Lemma 3.2.2 to the case when $A = a\alpha$ and $B = b\alpha$, gives us that there is an integer p such that

$$d(p, |a\alpha - b\alpha|) \leq |\{a\alpha\} - \{b\alpha\}| < \frac{1}{N} \leq \frac{1}{a - b} = \frac{1}{q}$$

Thus, there is p (as claimed by Lemma 3.2.2) and q (which is equal to $a - b$ which exists as per PHP application), such that:

$$|q\alpha - p| \leq \frac{1}{q}$$

This completes the proof of the theorem. □

Exercise 3.3 (See Problem Set 1 (Problem 3))**.** Let $\alpha_1, \alpha_2, \ldots \alpha_k$ be k rational numbers. Generalizing the Dirichlet's approximation principle argument that we did in class, using PHP again, prove that there must exist integers $p_1, p_2, \ldots p_k$ and q such that:

$$\forall i, \quad \left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{k}}}$$

Remark 3.3.1. *The proof of the theorem proves something stronger. That is, it actually can give a way to get many q's which acheive the error bound. Notice that the choice of N was free in the proof and q that we end up choosing is $a - b$ which is at most N. Hence suppose that we already have a p and q in hand, if we run the proof by choosing N to be large enough such that:*

$$\frac{1}{N} < |q\alpha - p|$$

then necessrily the new p and q that the proof gives will have to be different (and q needs to be larger). By repeating this, we can produce a new p and q and so on and so forth. This gives us a way to produce infinitely many p and q such that:

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

We were clearly motivated to improve the denominator of $2q$ in the naive attempt to q^2 in the denominator in the rational approximation principle. Can this be improved further? The following curiosity remark says otherwise.

Curiosity 3.3.2 (Tightness of Dirichlet's Approximation Principle - Roth's Theorem). Let α be any algebraic number (which can be expressed as the root of a polynomial with coefficients from $\mathbb{Q}$. For every ϵ the inequality,

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}$$

can hold true only for finitely many co-prime pairs (p, q). This says that the Dirichlet's approximation principle cannot be improved (for infinitely many p and q) with a larger order denominator.

The above remark says that we cannot improve in the exponent for Dirichlet's approximation principle. Can we improve by having a large multiplier for the q^2 in the denominator? Even this has a limit, and leads to classifying irrational numbers using what is called the *Lagrange measure* of the number.

Curiosity 3.3.3 (Hurwitz Theorem and Irrationality Measures). This is an improvement of the above principle. For every irrational number α, there are infinitely many relatively prime integers p and q such that:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{\sqrt{5}q^2}$$

The $\sqrt{5}$ in the denominator is the best possible. If we let it greater than $\sqrt{5}$, then there is a counter example - consider the irrational number $\frac{1+\sqrt{5}}{2}$ (the golden ratio). It can be shown that this can have only finitely many relatively prime integers p and q with the above formula holding (this is done through arguments about continued fraction representations). For example, if we avoid *golden ratio* and some similar irrational numbers, then we can improve the denominator to $\sqrt{8}$. If we avoid *silver ratio* $(1 + \sqrt{2})$ and associated irrational numbers, then we can improve this to $\frac{\sqrt{221}}{5}$. In general, the bound is of the form:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{L_n q^2}$$

where L_n (called the *Lagrange numbers*) steadily increases if some bad irrational numbers are included. These also are viewed as measures of "how much irrational the number is".

Instructor : Jayalal Sarma
Scribe : Jayalal Sarma (*TA:* JS)
Date : Sept 14, 2020
Status : α

Lecture
4

Counting by Bijections and Double Counting Principle

We now quickly review the basic tools from counting. Permutations and combinations forms the basics from discrete mathematics that we rely upon. We will stress on the aspects that are critical for the rest of the course. The first tool that we will demonstrate in detail is the power of counting by using bijections.

4.1 Basic Examples of Counting by Bijections

The cardinality of two sets is said to be the same if there is a bijection between the two. Indeed, for finite sets the notion of cardinality matches with that of size while it can be deceiving for infinite sets[3]. We will concentrate on finite sets for this part and use bijections to establish combinatorial counting.

We start with something that we are all familiar with, in order to bring out the nuances involved with proof by bijections. Notice that we know how to count this object even otherwise, by other means, but this is just as a starting example.

Proposition 4.1.1. *The number of subsets of a set is of n elements is exactly 2^n.*

Proof. Let S be the given set of n elements. Without loss of generality let us assume that $S = \{1, 2, \ldots, n\}$. The bijection is nothing but the well-known idea of characteristic vector of a set,

We establish a bijection between the following two sets.

$$\phi : \left\{ A : \begin{array}{c} A \text{ is a subset of} \\ \text{the set } S \end{array} : \right\} \to \left\{ x : \begin{array}{c} x \text{ is a string of length } n \\ \text{over alphabet } \{0,1\} \end{array} : \right\}$$

We first define the function as follows. Let A be any subset of S, define the string $w = \phi(x)$ as the n-bit string where for every $1 \leq i \leq n$:

$$w_i = \begin{cases} 0 & \text{if } i \notin A \\ 1 & \text{if } i \in A \end{cases}$$

[3]For infinte sets, there are notions of countability and uncountability of sets which we will not discuss here.

Notice that the function ϕ is well-defined (this may have to be checked explicitly in certain bijections when we define) since we are defining the bit w_i for every $i \in [n]$.

We now argue that it is an injection. Suppose that two sets $A, B \subseteq S$, but $A \neq B$. That is there is an $i \in S$ for which $i \in A$, but $i \notin B$. By the above definition, the i-th but of $\phi(A)$ will be 1 while the i-th bit of $\phi(B)$ will be 0. This implies $\phi(A) \neq \phi(B)$.

We also show that ϕ is a surjection. Given any $w \in \{0,1\}^n$, we can define a pre-image $A \subseteq S$ as $A = \{i \mid w_i = 1\}$. By definition, $\phi(A) = w$ and hence w has a pre-image. This shows ϕ is a surjection.

□

Let us argue a slight variant of the above example now. While there are other ways to establish this, we insist on using the method of counting by bijections.

Proposition 4.1.2. *The number of even sized subsets of $[n]$ is equal to the number of odd sized subsets, and both are equal to 2^{n-1}.*

Proof. by observing that the bijection that we defined in the previous proof has the additional feature that the number of 1s in $\phi(A)$ is exactly the cardinality of A, we can conclude that it is sufficient to establish a bijection between the following two sets:

$$\psi : \left\{ x : \begin{array}{c} x \in \{0,1\}^n \text{ having} \\ \text{even no. of 1s in it} \end{array} \right\} \to \left\{ w : \begin{array}{c} w \in \{0,1\}^n \text{ having} \\ \text{odd no. of 1s in it} \end{array} \right\}$$

Fix any $i \in [n]$, we define a bijection with respect i (this says there are actually n bijections between the two sets above, not just one !). Technically, we should be writing ψ_i but we drop the subscript since it is not critical for the representation.

Definition: We define the bijection as follows : let e_i denote the string which has 1 in the i-th position and 0 elsewhere.

$$\psi(x) = x \oplus e_i$$

where $\oplus$ denotes bitwise xor to produce an n bit string.

well-defined: We explicitly check whether the function is well-defined. Indeed, consider any $x \in \{0,1\}^n$ which has even number of 1s in it. By the operation $x \oplus e_i$ produces a string in $w \in \{0,1\}^n$. Since the i-th bit is flipped, w must necessarily have odd number of 1s in it.

injection: We show that ψ is an injection. Consider $x, x' \in \{0,1\}^n$ such that $x \neq x'$. There must exist an index j in which they differ. We have two cases:

Case 1: $j = i$: Indeed, since the i-th bit is flipped by the mapping, the images $w = \phi(x)$ and $w' = \phi(x')$ must also have their j-th bit to be different. Hence $\phi(x) \neq \phi(x')$.

Case 2: $j \neq i$: Since the operation does not change any other bit. The images $w = \phi(x)$ and $w' = \phi(x')$ must also have their j-th bit to be different. Hence $\phi(x) \neq \phi(x')$.

Hence, we conclude that ϕ is injective.

surjection: Given any $w \in \{0,1\}^n$ which has odd weight, we show $x \in \{0,1\}^n$ such that $\phi(x) = w$. Indeed, defining $x = w \oplus e_i$ will meet the requirement. Hence ϕ is surjective.

Hence we conclude that ϕ is a bijection and that the two sets must be of same cardinality. Since the two sets are disjoint and their union is of size 2^n, it must be that both of them are of size 2^{n-1}. This concludes the proof. □

Note that in the above proof, we wrote down the steps in proving the bijection explicitly. It is somewhat standard to skip over the one which are obvious from the definitions, but it is a good practice to write these down in a formal proof so that the argument is not prone to errors.

4.2 From Bijections to Double Counting

We will now introduce a new technique called *double counting* which has the method of bijections as its backbone.

Double Counting Method: The method can be presented as follows. There is one combinatorial (mostly counting) question that we will design which we will answer in two distinct (but provably correct) ways. Since the two answers are for the same counting problem, it is logical to equate them and such an equality gives relations that are otherwise no apparent.

The whole idea can be viewed as a method of bijection itself. In many situations, the double counting may also reveal an implicit bijection between the two different ways of answering the question. While this is not necessary for the double counting method, it is revealing to think about the underlying bijection.

This is a very elegant and powerful tool. The creativity in the proof is in designing the right question. Indeed, *asking the right question is mostly more than half way thorugh into constructing mathematical proofs* !!. We demonstrate this by a simple example first.

Proposition 4.2.1. *For any $k \leq n$,*

$$\binom{n}{k} = \binom{n}{n-k}$$

Proof. The combinatorial counting question in this case can be the following:

Q: In how many ways can we form a committee of size k from a set of n people.

A1: Directly choose the k committee members from n people. By definition, there are $\binom{n}{k}$ ways of doing this.

A2: Directly choose the $n-k$ non-members of the committee from n people and declare the remaining to be the committee members. There are $\binom{n}{n-k}$ ways of doing this too.

This completes the argument. Although not required for the proof, for the curious mind, the underlying bijection revealed is the complementation of the set. □

Note that there is an easy algebraic way of arguing the above identity. But as the expressions get more complicated, this proof technique is more revealing and elegant.

Proposition 4.2.2. *For any n and k,*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Proof. We can reuse the question itself from the proof of the earlier proposition.

Q: In how many ways can we form a committee of size k from a set of n people.

A1: Directly choose the k committee members from n people. By definition, there are $\binom{n}{k}$ ways of doing this.

A2: Let the potential members be $\{1, 2, \ldots n\}$. Classify the ways of choose k committee members into two. Ones that includes n and the ones that does not include n. Since these two kinds of committees are never the same, we can count both types and add them. More formally, this is expressed as, *condition on the fact whether n is in the committee or not*. If n is in the committee, then there are only $k-1$ remaining members of the committee needs to be chosen from the remaining $n-1$ members available to choose from - which gives $\binom{n-1}{k-1}$ ways of doing it. On the other hand, if n is not in the committee, then there are still k members to be chosen from $n-1$ potential members to choose from - this gives $\binom{n-1}{k}$ as the number of possible ways. Adding these two, gives the RHS as the second answer to the counting question.

This completes the argument. □

Proposition 4.2.3. *For $k \leq n$,*

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Proof. We can almost reuse the question itself from the proof of the earlier proposition.

Q: In how many ways can we form a committee of size k from a set of n people, and then choose a chair of the committee (who is also a part of the committee).

A1: Directly choose the k committee members from n people. By definition, there are $\binom{n}{k}$ ways of doing this. And then among the members chosen, choose a chair for the committee which can be done in k different ways. This gives $k\binom{n}{k}$ ways of completing the task which is equal to the LHS.

A2: First choose the chair from the potential members of the committee. This can be done in n ways. And then choose the remaining $k-1$ members of the committee from the remaining potential members of the committee. This can eb done in $\binom{n-1}{k-1}$ ways.

This completes the argument. □

Exercise 4.3. Prove the following identities using double counting method:

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1} \qquad \binom{m+n}{k} = \sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i} \qquad \binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$$

Proposition 4.3.1.

$$\sum_{m=k}^{n}\binom{m}{k} = \binom{n+1}{k+1}$$

Proof. We need to modify the question slightly here.

Q: In how many ways can we choose $k+1$ numbers from the set $\{1, 2, \ldots, n+1\}$?

A2: The RHS is immediate by definition.

A1: Count conditioning on the largest element to be chosen in the set. Note that a subset cannot be counted against two largest elements since largest element of a given set is uniquely defined. Now, for a fixed largest element $m+1$, the numeber of ways of choosing remaining elements is given by the number of ways of choosing k elements from the set $\{1, 2, \ldots m\}$ since $m+1$ is the largest. This gives $\binom{m}{k}$ ways of completing the task when the largest element is $m+1$. Since m has to be atleast k and can be at most n, this gives the number of ways of choosing a set of $k+1$ numbers from the set to be :

$$\sum_{m=k}^{n}\binom{m}{k}$$

which matches with the LHS.

This completes the argument. □

Use a similar argument to do the following:

Exercise 4.4 (See Problem Set 1 (Problem 4))**.** Use a double counting argument to establish the following identity :

$$\sum_{m=k}^{n-k}\binom{m}{k}\binom{n-m}{k} = \binom{n+1}{2k+1} \quad \text{where} \quad 0 \le k \le \frac{n}{2}$$

Generalize the idea to prove :

$$\sum_{j=r}^{n+r-k}\binom{j-1}{r-1}\binom{n-j}{k-r} = \binom{n}{k} \quad \text{where} \quad 1 \le r \le k$$

Instructor : Jayalal Sarma
Scribe : Narasimha Sai Vempati (*TA:* JS)
Date : Sept 19, 2020
Status : α

Lecture
5

Multichoosing

5.1 Introduction

Consider the definition of *set*. We know that it's a well defined collection of *distinct* objects. From a collection of n distinct symbols, the number of ways to form a *set* of length k is given by $\binom{n}{k}$. Now let's consider the definition of *multi-set*. It's similar to that of a *set*, except that it allows repetition of objects. Now it's natural ask the following question: From a collection of n distinct symbols, what is the number of ways to form a *multi-set* of length k. Multichoosing exactly answers this questions. In this lecture, we explore multichoosing in detail. We discuss several equivalent bijections to this problem and come-up with an algebraic expression for $\left(\binom{n}{k}\right)$ (spelled out as n *multi-choose* k).

5.2 Equivalent bijections

5.2.1 Non-negative solutions

Formally, $\left(\binom{n}{k}\right)$ is the number of ways of choosing k objects from a set of n objects where the order is not important but repetitions are allowed. For all $i = 1, 2, \cdots, n$, if we denote by x_i the number of copies of i^{th} object we choose, then we have the equation

$$x_1 + x_2 + \cdots + x_n = k \tag{5.5}$$

where each $x_i \geq 0$. Therefore, number of *non-negative* integral solutions to this equation gives us the required number of ways of choosing k objects from n objects with given conditions. Let's look at an equivalent problem and establish a bijection between these two.

5.2.2 Voting problem

If n candidates are contesting in an election and there are k voters, how many ways can votes of those k voters be distributed among n candidates?

If we denote by x_i, the number of votes received by i^{th} candidate and there are k voters, we have $x_1 + x_2 + \cdots + x_n = k$ and thus, the number of ways of dividing votes among candidates is the number of non-negative solutions to the equation 5.5. Formally, we can define a bijection f from set of solutions to the equation 5.5 to set of ways of dividing the votes among n candidates.

Definition: f takes the tuple $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and assign x_i number of votes to i^{th} candidate where $i = 1, 2, \cdots, n$.

Well defined: f is well defined because for every valid tuple $\mathbf{x} = (x_1, x_2, \cdots, x_n)$, we have $x_1 + \cdots + x_n = k$ and thus summing over votes received by i^{th} where $i = 1, 2, \cdots, n$ will be k votes in total.

Injective: f is an injection because for every valid way of dividing the votes among candidates, there's a unique solution tuple in which x_i = number of votes received by i^{th} candidate. In other words, for any two $\mathbf{x}_1 \neq \mathbf{x}_2$, there exists an $i \in [n]$ such that $x_{1_i} \neq x_{2_i}$ and i^{th} candidate gets different votes. Thus $f(\mathbf{x}_1) \neq f(\mathbf{x}_2)$.

Surjective: f is surjective because for every way of dividing k votes among n candidates, there is a pre-image $\mathbf{x} = (x_1, \cdots, x_n)$ which is a valid solution to the equation 5.5 (as there are a total of k voters, sum of number of votes received by each voter must sum up to k).

Thus f is a bijection from the set of non-negative solutions to $x_1 + \cdots + x_n = k$ to the set of ways of dividing k votes among n candidates.

5.2.3 Non-decreasing subsequences

Number of non-decreasing sequences of integers between 1 and n of length k. A non-decreasing sequence is of the form $\{a_1, a_2, \cdots, a_k\}$ where $1 \leq a_1 \leq a_2 \cdots \leq a_k \leq n$. Lets define a bijection f from set of non-negative integral solutions to Eqn. 5.5 to set of non-decreasing sequences between 1 and n of length k.

Definition: f takes $\mathbf{x} = (x_1, \cdots, x_n)$ as input and writes the number i x_i times for all $i = 1, 2, \cdots, n$ to obtain a sequence of length k.

Well defined: As f constructs the sequence in increasing order from 1 to n by writing i x_i times, the resulting sequence will be non-decreasing. Therefore, f is well defined.

Injective: For every $\mathbf{x}_1 \neq \mathbf{x}_2$, there exists an i such that $x_{1_i} \neq x_{2_i}$ and thus in the resulting sequences, number i is written different number of times. Therefore, f is injective.

Surjective: Every non-decreasing sequence of integers between 1 and n of length k has a pre-image $\mathbf{x} = (x_1, \cdots, x_n)$ which is a valid solution to equation 5.5 (where x_i is the number of times the number i is present in the sequence and as length of sequence is k, all x_i's where $i = 1, 2, \cdots, n$ sum up to k).

Thus f is a bijection.

5.2.4 Stars and bars problem

There are k stars placed horizontally. Find the number of ways to place $n-1$ bars in between those k stars. Lets define a bijection f from set of non-negative integral solutions to Eqn. 5.5 to set of ways of placing $n-1$ bars among k stars.

Definition: f takes $\mathbf{x} = (x_1, \cdots, x_n)$ as input and place x_i number of stars between $(i-1)^{th}$ bar and i^{th} bar. We leave it as an exercise to prove that f is well-defined, injective and surjective.

1: Jayalal says: Todo - Prove that f is a bijection

5.3 Algebraic expression

So far in Sec. 5.2, we have established bijections between *non-negatives integral* solutions of Eq. 5.5 and various other problems and argued that number of ways of solving any particular problem is equal to the number of non-negative integral solutions to Eq. 5.5. In this section, we are interested in coming up with a concrete expression for $\left(\binom{n}{k}\right)$ by solving it's equivalent bijection.

Method 1 Let's solve the *stars and bars* problem defined in Sec. 5.2.4. Let's use the fact that any placement of $n-1$ bars among k stars can be equivalently thought of as a string of length $n+k-1$ over the alphabet $\{\star, |\}$ with k $\star$'s. Therefore,

$$\begin{aligned}\text{number of ways of placing } n-1 \text{ bars among } k \text{ stars } &= \text{number of such strings} \\ &= \binom{n+k-1}{k}\end{aligned}$$

Method 2 Let's solve the *Non-decreasing subsequences* problem defined in Sec. 5.2.1. Let's establish a bijection f from set β of non-decreasing subsequences of integers between 1 and n of length k to a set Γ of strictly increasing subsequences of integers between 1 and $n+k-1$ of length k. A strictly increasing subsequence is of the form $1 \leq b_1 < b_2 < \cdots < b_k \leq n+k-1$

Definition: f takes as input a non-decreasing subsequence $(a_1, a_2, \cdots, a_k)$ between 1 and n and for all $i = 1, 2, \cdots, k$ set $b_i = a_i + i - 1$ and output the sequence $(b_1, b_2, \cdots, b_k)$

Well defined: For any $(a_1, a_2, \cdots, a_k) \in \beta$, we have for all $i = 1, 2, \cdots, k-1$,

$$\begin{aligned} a_i &\leq a_{i+1} \\ a_i + i &\leq a_{i+1} + i \\ a_i + i - 1 &< a_{i+1} + i \\ b_i &< b_{i+1} \end{aligned}$$

Therefore, the subsequence $(b_1, \cdots, b_k)$ is strictly increasing subsequence and thus f is well defined.

Injective: For every non-decreasing subsequence $(a_1, \cdots, a_k)$, there's a unique strictly increasing subsequence $(b_1, \cdots, b_k)$ where for all $i = 1, \cdots, k$, $b_i = a_i + i - 1$. Therefore f is injective.

Surjective: For every strictly increasing subsequence $(b_1, \cdots, b_k)$, there's a pre-image $(a_1, \cdots, a_k)$ which is non-decreasing where for all $i = 1, \cdots, k$, $a_i = b_i - i + 1$

Therefore, f is a bijection. The number of ways of choosing a strictly increasing subsequence $(b_1, \cdots, b_k)$ between integers 1 and $n+k-1$ is just choosing k integers from first $n+k-1$ integers and arrange them in one way(increasing order). Therefore number of ways = $\binom{n+k-1}{k}$. As f is a bijection, therefore, the number of non-decreasing subsequences between 1 and n of length k are $\binom{n+k-1}{k}$

Method 3 Let's solve the *Voting* problem defined in Sec. 5.2.2. Let's ask a slightly modified question.

Question: How many ways to distribute m votes among n candidates such that each candidate gets at least one vote.

Answer 1: As every candidate gets at least one vote, let's first distribute one vote each to each of the n candidate and the distribute the remaining $m - n$ votes among n candidates. By the bijection defined in Sec. 5.2.2, the number of ways of distributing $m - n$ votes among n candidates is $\left(\binom{n}{m-n}\right)$

Answer 2: Let's interpret votes as $\star$ s. Then the question essentially reduces to placing $n - 1$ bars (since there are n candidates, we divide by placing $n - 1$ bars) among m stars (since there are m voters). i^{th} candidate gets votes equal to number of stars between $(i-1)^{th}$ | and i^{th} |. However, there are two additional constraints

1. A bar cannot be placed in the beginning or in the end (if not then either the first candidate or the last candidate gets 0 votes)
2. We cannot place two | s between same two $\star$ s (if we place $(i-1)^{th}$ | and i^{th} | between same two $\star$ s, the i^{th} candidate gets 0 votes)

Hence, we have to choose $n - 1$ gaps among the $m - 1$ gaps (because we have $m + 1$ gaps and by cond. 1 we remove two) to place $n - 1$ | s without repetitions (because repeating violates cond. 2). Therefore, there are $\binom{m-1}{n-1}$ ways of doing it. Thus $\left(\binom{n}{m-n}\right)$=$\binom{m-1}{n-1}$ and by substituting $m = n + k$, we have

$$\left(\binom{n}{k}\right) = \binom{n+k-1}{n-1} = \binom{n+k-1}{k}$$

5.4 Identities

In this section, we discuss some identities on $\left(\binom{n}{k}\right)$ and argue their proofs using the idea of either double counting or bijections.

Identity 1

$$\left(\binom{n}{k}\right) = \left(\binom{k+1}{n-1}\right)$$

Proof. Let's use the bijection method to prove this. Formally, lets define sets S_1 and S_2 and count their cardinalities independently and then establish a bijection from S_1 to S_2 proving that $|S_1| = |S_2|$.

S_1: Configuration of k $\star$ s and $n-1$ | s as described in Sec. 5.2.4. By the bijection defined in it, $|S_1| = \left(\binom{n}{k}\right)$

S_2: Configuration of $n-1$ $\star$ s and k | s as described in Sec. 5.2.4. Again, by the bijection defined in it, $|S_2| = \left(\binom{k+1}{n-1}\right)$

Bijection: Let's define a bijection f from S_1 to S_2. f takes a configuration from S_1 as input and interpret $\star$ s as | s and | s as $\star$ s. Therefore it ends up with a configuration with $n-1$ $\star$ s and k | s which is a configuration is S_2. It's easy to observe that f is a bijection.

As f is a bijection from S_1 to S_2, we have $|S_1| = |S_2|$. This completes the proof ∎

Identity 2

$$k\left(\binom{n}{k}\right) = n\left(\binom{n+1}{k-1}\right)$$

Proof. Let's use the method of double counting to prove this.

Question: In how many ways can we construct a non-decreasing sequence $1 \leq a_1 \leq a_2 \cdots \leq a_k \leq n$ and mark one element?

Asnwer 1: By the bijection established in Sec. 5.2.3 we have $\left(\binom{n}{k}\right)$ number of non-decreasing subsequences and for every such subsequence, we can mark any one of the k elements choose. Thus the answer is $k\left(\binom{n}{k}\right)$

Answer 2: Firstly, determine the value in $[n]$ which is to be marked. Let r be this value. Now, consider a non-decreasing subsequence between 1 and $n+1$ with $k-1$ elements. Using r and the non-decreasing sequence chosen, we construct a unique non-decreasing sequence between 1 and n of length k with r as marked in the following way:

Let $(b_1, b_2, \cdots, b_{k-1})$ with $1 \leq b_1 \leq b_2 \leq \cdots \leq b_{k-1} \leq n+1$ be the chosen sequence,

- Insert marked-r in the right most position so that the resulting sequence is still sorted.

- As long as there's an $n+1$ in the sequence, remove it and add it as r to the right of marked-r in the sequence

Therefore, number of required sequences

$$\begin{aligned} &= \text{number of ways to choose } r \times \overset{\text{number of non-decreasing sequences of length } k-1 \text{ between 1 and } n+1}{\left(\!\binom{n+1}{k-1}\!\right)} \\ &= n \times \left(\!\binom{n+1}{k-1}\!\right) \end{aligned}$$

This completes the proof ∎

Exercise 5.5.

Prove the following by combinatorial arguments

$$\left(\!\binom{n}{k}\!\right) = \sum_{m=1}^{n} \left(\!\binom{m}{k-1}\!\right)$$

Hint: Look for bijection to number of non-decreasing subsequences

Prove the following by combinatorial arguments

$$\sum_{k=0}^{m} \left(\!\binom{n}{k}\!\right) = \left(\!\binom{n+1}{m}\!\right)$$

Hint: Look for bijection to Voting problem

Prove the following by combinatorial arguments

$$\left(\!\binom{n}{k}\!\right) = \sum_{m=0}^{n} \binom{n}{m} \left(\!\binom{m}{k-m}\!\right)$$

Instructor : Jayalal Sarma
Scribe : Anshu and Narasimha Sai (*TA:* JS)
Date : Sept 19, 2020
Status : α

Lecture
6

Catlan Bijections

6.1 Introduction

One of the classic examples to demonstrate the power of bijections is *Catlan numbers*. The Catlan numbers form a sequence of natural numbers that occur in various counting problems and occurs in several seemingly different contexts. Historically, *Euler* is the first person to study them. He was interested in counting the number of ways of dividing a polygon into triangles by drawing non-overlapping diagonals. Catlan numbers got their name from *Eugene Catlan* when he used them to answer the *Parenthesisation problem* which is the following: Consider a sequence $(a_1, a_2, \cdots, a_{n+1})$ of $n+1$ numbers, If we have to perform a binary operations $\odot$ n times among them, how many number of ways are there to parenthesise (or bracket) them using n parenthesis of single type (say $'()'$). In this lecture, we will see a few equivalent problems to this and then arrive at an explicit expression of Catlan numbers.

6.2 Equivalent Bijections

In this section, we see a few equivalent problems of the *parenthesisation* problem and argue that answer to each of them is also the *catlan number*

Full binary trees If we observe the Parenthesisation problem carefully, we notice that every valid parentesisation of those $n+1$ numbers form a *full binary tree* (a binary tree in which every node have either two children or no children) of $n+1$ leaves and n internal nodes where leaves represents the numbers $a_1, \cdots, a_{n+1}$ and each internal node corresponds to one operation. Therefore, there's an implicit bijection between the set of valid parenthesisations and full binary trees with n internal nodes. Therefore,

$$\begin{matrix}\text{number of valid parenthesisations of} \\ n+1 \text{ elements}\end{matrix} = \begin{matrix}\text{number of full binary trees with} \\ n \text{ internal nodes}\end{matrix} \tag{6.6}$$

Balanced parenthesised strings A balanced parenthesised string of length $2n$ is a string consists of n left brackets $'('$ and n right brackets $')'$ in which every prefix of the string has number of left brackets $'('$ $\geq$ number of right brackets $')'$. One can easily observe the bijection from set of balanced paranthesised string to valid parenthesisations of $n+1$ numbers

Euler's problem Find the number of ways of triangulating a polygon with $n+2$ edges

Handshaking problem Consider a scenario where $2n$ people are sitting around a table. How many ways they can shake hands with each other without crossing hands. We leave it as an exercise to establish bijections from *Euler's* problem to *Full binary tree* problem and *handshaking* problem to *balanced parenthesised strings* problem.

2: Jayalal says: Todo - Establish bijections from *Euler's* problem to *Full binary tree* problem and *handshaking* problem to *balanced parenthesised strings* problem

6.3 Algebraic Expression

In this section, we are interested in arriving at a concrete expression of the n^{th} *catlan number* (denoted by c_n). Let's solve another problem and then, by establishing a bijection to one of the above problems, we can arrive at an expression for c_n.

6.3.1 Monotone walk on $n \times n$ grid

Suppose we have a grid of size $n \times n$. How many ways are there to go from $(0,0)$ to (n,n) by using only downward edges or right edges. A sample path is represented in Fig. 6.1. We observe that each step can increment the value of exactly one of the co-ordinates by 1. Since we have to move from $(0,0)$ to (n,n), we have to increase the value of both the co-ordinates by n and n and thus irrespective of the path you take, the length of a path from $(0,0)$ to (n,n) must be of length $n+n=2n$.

If we represent each right move as R and each downward move as D, one can observe that there's a bijection f from the set of paths to set of strings of length $2n$ over the alphabet $\{D,R\}$ with number of D's = number of R's = n. Formally, if $(u_0,v_0),(u_1,v_1),\cdots,(u_{2n},v_{2n})$ represents the path where $(u_0,v_0)=(0,0)$ and $(u_{2n},v_{2n})=(n,n)$, and $b=b_1b_2\cdots b_{2n}$ represents the string where each b_i is either D or R, our bijection f takes a path as input and sets b_i as

$$b_i = \begin{cases} D & \text{if } u_i = u_{i-1}+1 \\ R & \text{if } v_i = v_{i-1}+1 \end{cases}$$

Well defined: As we have exactly n x co-ordinate increments and n y co-ordinate increments, we will have exactly n D's and n R's in our string and thus f is well defined.

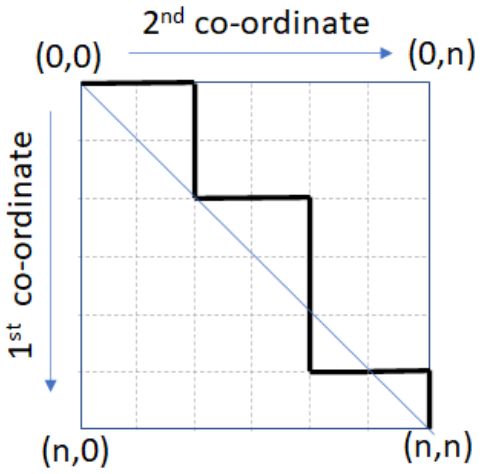


Figure 6.1: A path from $(0,0)$ to (n,n) using downward and right edges

Injective: Two different paths from $(0,0)$ to (n,n) will different in at least one (u_{i-1}, v_{i-1}) to (u_i, v_i) transition where $i = 1, 2, \cdots, 2n$, their corresponding strings under f will differ in at least i^{th} position and thus f is injective.

Surjective: Every string over $\{D, R\}$ of length $2n$ with equal number of D's and R's has a pre-image under f which is defined by $(u_0, v_0) = (0,0)$ and (u_i, v_i) is $(u_{i-1}+1, v_{i-1})$ if $b_i = R$ and $(u_{i-1}, v_{i-1}+1)$ if $b_i = D$. As there will be n D's and n R's, $(u_{2n}, v_{2n}) = (n,n)$ and thus f is surjective .

Thus f is bijection. As we have number of string over $\{D, R\}$ of length $2n$ with equal number of D's and R's equal to $\binom{2n}{n}$ (select n positions out of $2n$ available and fill them with D's and the rest with R's). Thus the number of paths from $(0,0)$ to (n,n) with only downward and rightward movements is $\binom{2n}{n}$.

Lets ask a slightly question. How many ways are there to go from $(0,0)$ to $(n+1, n-1)$ using only downward or right edges.Using a similar arguments as above, we can come up with a bijection to set of string over $\{D, R\}$ of length $2n$ with $n+1$ D's and $n-1$ R's. Therefore number of required paths are $\binom{2n}{n+1} = \binom{2n}{n-1}$

6.3.2 Diagonal avoiding paths and Catlan numbers

In this section we explore the connection between the above paths that we discussed and the Catalan number. Let us ask this question: How many paths are there in the grid from $(0,0)$ to (n,n) that avoids crossing the diagonal?

We first define what *crossing the diagonal* means. The diagonal consists of the points of the form (i,i), $i \in \{0, \ldots, n\}$. A path $((u_0, v_0), \ldots, (u_{2n}, v_{2n}))$ is said to be crossing the diagonal if it *intersects* through the diagonal and goes to some point below the diagonal. Mathematically, a path is a diagonal crossing path if $\exists\ i$ such that $u_i > v_i$. In particular, $\exists i : u_i = v_i + 1$ (refer fig.

6.2 for example. Any diagonal crossing path must necessarily pass through one of the red dots). Equivalently, in a diagonal avoiding path $\forall i \in \{0, \ldots, 2n\}, v_i \geq u_i$. A sample *diagonal-avoiding path* is shown in the fig. 6.3

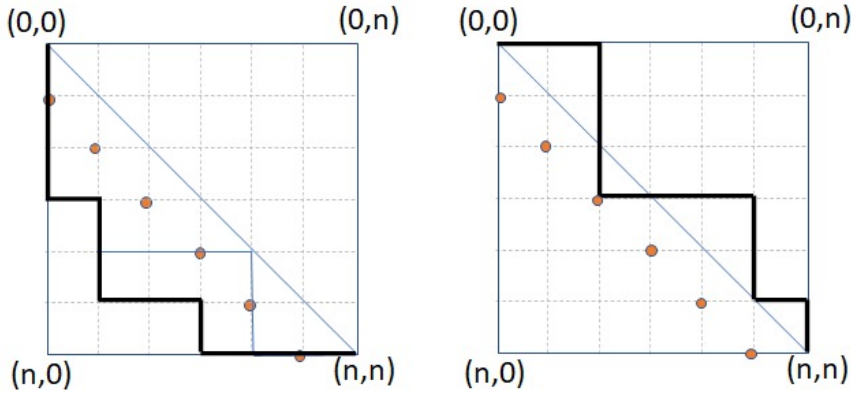


Figure 6.2: Diagonal crossing paths. Note that path in (a) is crossing the diagonal at $(0, 0)$

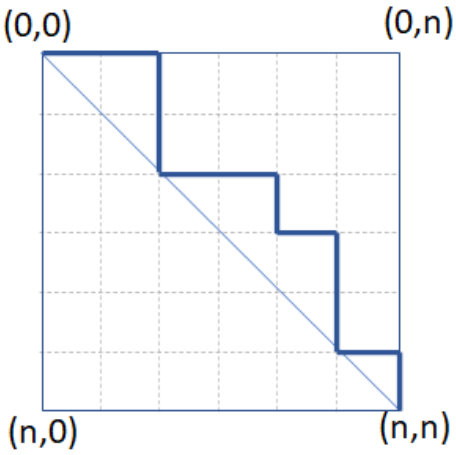


Figure 6.3: A diagonal avoiding path. Observe that it can still touch the diagonal

Before computing this number, an obvious question is what is the connection between such restricted paths and Catalan number. It turns out that the set of diagonal avoiding paths from $(0, 0)$ to (n, n) is in bijection with the set of balanced paranthesized strings of length $2n$. Hence, to count the number of balanced paranthesized strings of length $2n$, which is also the Catalan number, we only need to count the diagonal avoiding paths from $(0, 0)$ to (n, n). Let us first establish the bijection between the two.

6.3.3 Bijection from Diagonal avoiding paths to Balanced parenthesisation problem

Intuitively, the bijection can be defined as follows: for any given balanced parenthesized string $w = w_1 w_2 \ldots w_{2n}$, the corresponding path from $(0, 0)$ to (n, n) is obtained by starting from position

$(0,0)$, and scanning the string from left to right. Take right move whenever '(' is encountered and a down move for ')'. Formally we define the bijection as follows:

Defining the bijection: Let P be the set of diagonal avoiding paths from $(0,0)$ to (n,n) and B be the set of balanced paranthesized strings of length $2n$ over the alphabets $\{(,)\}$. Define the bijection $\phi : B \to P$ as follows:
For $w = w_1 w_2 \dots w_{2n} \in B$, $\phi(w) = (u_0, v_0), (u_1, v_1), \dots, (u_i, v_i), \dots, (u_{2n}, v_{2n})$, where

1. $(u_0, v_0) = (0,0)$
2. $\forall i \in \{1, 2, \dots, 2n\}$

$$(u_i, v_i) = \begin{cases} (u_{i-1} + 1, v_{i-1}) & \text{if } w_i =) \\ (u_{i-1}, v_{i-1} + 1) & \text{if } w_i = (\end{cases}$$

Proof of bijection

Well-defined: From the above description, given any string w, $\phi(w)$ is uniquely defined. Further, for any string $w \in B$, since the number of $'('$ is same as the number of $')' = n$, the corresponding path has n right and n down moves and hence it ends at (n,n). Also, since the number of left brackets is greater than or equal to the number of right brackets in any prefix of w, for all $i \in [2n]$, $v_i \geq u_i$. This shows that $\forall w \in B, \phi(w) \in P$. Hence, ϕ is well-defined.

Injective: Let w, w' be two different strings in set B. Then $\exists$ an index $i \in [2n]$ where $w_i \neq w'_i$. Hence $\phi(w)$ and $\phi(w')$ also differ at the ith step, where one of the paths takes one step right while the other takes one step down.

Surjective: Given any path $((0,0), (u_1, v_1), \dots, (u_{2n}, v_{2n}))$ the corresponding string $w \in B$ is defined as follows:
$\forall i \in [2n]$

$$w_i = \begin{cases} \text{`(`} & \text{if } (u_i, v_i) = (u_{i-1}, v_{i-1} + 1) \\ \text{`)`} & \text{if } (u_i, v_i) = (u_{i-1} + 1, v_{i-1}) \end{cases}$$

We can verify that the string w indeed is in set B, because firstly, for any path in P, $\forall i, v_i \geq u_i$ and hence by definition, number of left brackets '(' in w is greater than or equal to number of right brackets, '(' in any prefix of w. Secondly, for any path to reach from $(0,0)$ to (n,n) it must have n right moves (increase in 2nd coordinate) and n down moves (increase in 1st coordinate) and hence w must have n left brackets and n right brackets.

6.3.4 Counting the number of diagonal avoiding paths

Having established the bijection between Catalan number and diagonal avoiding paths, we get

$$C_n = \#\text{ of diagonal avoiding paths from } (0,0) to (n,n) \tag{6.7}$$

So, our next task is to count the number of diagonal avoiding paths from $(0,0)$ to (n,n). To count this, we take following approach. Let us call the diagonal avoiding paths as *good* paths and diagonal crossing paths as *bad* paths. Then,

$$\begin{array}{c}\text{\# of diagonal avoiding paths}\\ \text{from } (0,0) \text{ to } (n,n)\end{array} = \begin{array}{c}\text{\# of paths}\\ \text{from } (0,0) \text{ to } (n,n)\end{array} - \begin{array}{c}\text{\# of diagonal crossing paths}\\ \text{from } (0,0) \text{ to } (n,n)\end{array} \tag{6.8}$$

So, now our revised goal is to count the number of diagonal crossing paths from $(0,0)$ to (n,n). How do we do that? Here again bijection plays an important role. The idea is to translate diagonal crossing paths into different kind of paths which are easy to count.

Let us define the following path translation: Let $\pi = (0,0),(u_1,v_1),\ldots,(u_{2n},v_{2n})$ be a diagonal crossing path. Then there must exist i such that $u_i = v_i + 1$. There can be many such indices as the path can cross the diagonal multiple times. Choose i to be the least such index. Let $u_i = \ell$, then the first co-ordinate after crossing the diagonal is $(\ell, \ell-1)$. Let us call this point P (refer fig. 6.4(a)). Then to find the translated path we reflect the part of the path π after point P w.r.t. the main diagonal.

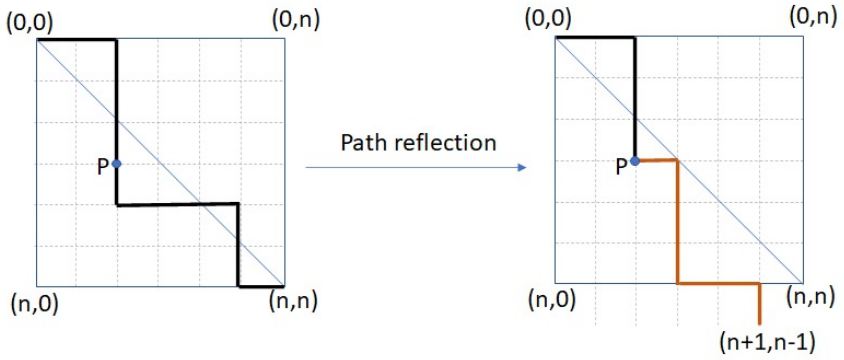


Figure 6.4: Point P in a diagonal crossing path and the reflected path after P

More precisely, we can divide the diagonal crossing path into two stretch S_1, S_2, where S_1 is the part of the path between $(0,0)$ to P and S_2 is the part of the path between P to (n,n). Then to translate π into a new path, replace S_2 with S_2' to get a new path $\pi' = S_1 S_2'$. The replacement S_2' is defined as follows:

- replace downward edges with right edges and
- replace right edges with downward edges.

Refer fig. 6.4(b) We can observe that the new path π' described in this way is always between $(0,0)$ to $(n+1, n-1)$. The argument for this goes as follows:

Originally (in S_2), $(\ell, \ell-1)$ goes to (n,n) which means it takes $(n-\ell)$ downward moves and $(n-\ell+1)$ right moves. Since, we are swapping the right and downward moves to get S_2' from S_2, there are $(n-\ell+1)$ downward moves and $(n-\ell)$ right moves from point $P = (\ell, \ell-1)$ in S_2'.

Thus, S'_2 goes from $(\ell, \ell-1)$ to $(\ell+n-\ell+1, \ell-1+n-\ell) = (n+1, n-1)$ and hence, $\pi' = S_1 S'_2$ is a path from $(0,0)$ to $(n+1, n-1)$.

Thus we have established that any diagonal crossing path from $(0,0)$ to (n,n) maps to a path from $(0,0)$ to $(n+1, n-1)$ after applying the transformation described above. The converse is also true, i.e., given any path from $(0,0)$ to $(n+1, n-1)$, we can translate it back to a diagonal crossing path from $(0,0)$ to (n,n) by using the same reflection technique. Thus, we get a bijection between the set of diagonal crossing paths from $(0,0)$ to (n,n) to the set of paths from $(0,0)$ to $(n+1, n-1)$. We formally define the translation and prove that it is indeed a bijection.

Bijection: Let A be the set of diagonal crossing paths from $(0,0)$ to (n,n) and B be the set of paths from $(0,0)$ to $(n+1, n-1)$. Then the mapping $\phi : A \to B$ is formally defined as follows:
Let $\pi = (0,0), (u_1, v_1), \ldots, (u_{2n}, v_{2n})$ and (u_i, v_i) be the first point when π crosses the diagonal. Then $\phi(\pi) = \pi' = (0,0), (u'_1, v'_1), \ldots, (u'_{2n}, v'_{2n})$ is given by:

1. $\forall 1 \leq j \leq i, (u'_j, v'_j) = (u_j, v_j)$
2. $\forall i+1 \leq j \leq 2n$,

$$(u'_j, v'_j) = \begin{cases} (u'_{j-1}+1, v'_{j-1}) & \text{if } (u_j, v_j) = (u_{j-1}, v'_{j-1}+1) \\ (u'_{j-1}, v'_{j-1}+1) & \text{if } (u_j, v_j) = (u_{j-1}+1, v'_{j-1}) \end{cases}$$

Well-defined: We already observed that any path $\pi \in A$ from $(0,0)$ to (n,n) maps to a path $(0,0)$ to $(n+1, n-1)$. Hence ϕ is well defined.

Injection: Consider two different diagonal crossing paths π_1 and π_2. Let $\pi_1 = S_{1,1} S_{1,2}$ and $\pi_2 = S_{2,1} S_{2,2}$, where the two components $S_{i,1}$ and $S_{i,2}$ for $i \in \{1,2\}$ are as defined before. Then following two cases are possible:

- Case1: $S_{11} \neq S_{21}$. Then $\pi'_1 \neq \pi'_2$, because the first component is copied as it is in the translation, i.e. $\pi'_1 = S_{1,1} S'_{1,2}$ and $\pi'_2 = S_{2,1} S'_{2,2}$.
- Case2: $S_{11} = S_{21}$, but $S_{12} \neq S_{22}$. In this case $S'_{12} \neq S'_{22}$ because of the way it is defined, i.e. for every right move there is a downwards move and vice-versa. Hence, $\pi'_i \neq \pi'_2$.

Surjective: Given any path π' from $(0,0)$ to $(n+1, n-1)$, we can construct the corresponding path π from $(0,0)$ to (n,n), such that $\phi(\pi) = \pi'$, as follows.
Let $\pi' = (0,0), (u'_1, v'_1), \ldots, (u'_{2n}, v'_{2n})$. Since π' goes to $(n+1, n-1)$ which is below the diagonal there must exist i such that (u'_i, v'_i) is below the diagonal. Again, there can be many such indices. Take i to be the first such index. Same as before, let $\pi' = S'_1 S'_2$, where S'_1 is the path from $(0,0)$ to (u'_i, v'_i) and S'_1 is the path from (u'_i, v'_i) to (u'_{2n}, v'_{2n}). Then $\pi = S'_1 S_2$ where S_2 is obtained from S'_2 by swapping the right and downwards moves. Mathematically, let $\pi = (0,0), (u_1, v_1), \ldots, (u_{2n}, v_{2n})$. Then

1. $\forall j \leq i$, $(u_j, v_j) = (u'_j, v'_j)$

2. $\forall\ i+1 \le j \le 2n$

$$(u_j, v_j) = \begin{cases} (u_{j-1}+1, v_{j-1}) & \text{if } (u'_j, v'_j) = (u'_{j-1}, v'_{j-1}+1) \\ (u_{j-1}, v_{j-1}+1) & \text{if } (u'_j, v'_j) = (u'_{j-1}+1, v'_{j-1}) \end{cases}$$

Again by the same argument as before it can be verified that π is a diagonal crossing path from $(0,0)$ to (n,n). We write it here for completeness. Let $(\ell, \ell-1)$ be the first point when π' crosses the diagonal. Then since the path from $(0,0)$ to $(\ell, \ell-1)$ remains as it is in π, it is a diagonal crossing path. Further since π' is path from $(0,0)$ to $(n+1, n-1)$, it takes $n+1-\ell$ downward steps and $n-\ell$ right steps from $(\ell, \ell-1)$. Hence, π takes $n+1-\ell$ right and $n-\ell$ downward steps from $(\ell, \ell-1)$. Thus, π ends at $(\ell+n-\ell, \ell-1+n+1-\ell) = (n,n)$.

Thus, we have established a bijection between the set of diagonal crossing paths from $(0,0)$ to (n,n) and the set of paths from $(0,0)$ to $(n+1, n-1)$. Hence,

$$\begin{aligned} \#\text{of diagonal crossing paths from } (0,0) \text{ to } (n,n) &= \#\text{of paths from } (0,0) \text{ to } (n+1, n-1) \\ &= \binom{2n}{n+1} \end{aligned}$$

Hence, from (6.7),(6.8),

$$\begin{aligned} C_n &= \#\text{of diagonal avoiding paths from} (0,0) \text{ to } (n,n) \\ &= \begin{matrix}\#\text{ of paths} \\ \text{from } (0,0) \text{ to } (n,n)\end{matrix} - \begin{matrix}\#\text{ of diagonal crossing paths} \\ \text{from } (0,0) \text{ to } (n,n)\end{matrix} \\ &= \binom{2n}{n} - \binom{2n}{n+1} \\ &= \binom{2n}{n} - \frac{n}{n+1}\binom{2n}{n} \\ &= \frac{1}{n+1}\binom{2n}{n} \end{aligned}$$

Here, in the second last line, we have used the identity:

$$\binom{2n}{n+1} = \frac{n}{n+1}\binom{2n}{n}.$$

Exercise 6.4.

Try to establish a bijection between the set of different possible polygon triangulation in a polygon of $n+2$ nodes and the set of binary trees with n internal nodes.

Hint: associate each internal node with a triangle in a triangulation. Then, each internal node will have degree three, which is the case for full binary tree, except for the leaves. Leaves will correspond to those triangles whose one of the edge is the boundary of the polygon.

Instructor : Jayalal Sarma
Scribe : Anshu Yadav (*TA:* JS)
Date : Sept 19, 2020
Status : α

Lecture 7

From Bijections to PIE

7.1 Introduction

In this lecture, we will continue with the use of bijections and use it in formally proving the two identities that we discussed in class and then see their relationship to the Principal of Inclusion and Exclusion.

7.2 The Identities

Recall that we proved following two identities in one of the discussion sessions

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0 \tag{7.9}$$

$$\sum_{k=0}^{m}(-1)^k\binom{n}{k} = (-1)^m\binom{n-1}{m} \tag{7.10}$$

In this section, we will see the proofs for the above equations is detail

7.2.1 Proof for Eqn. (7.9)

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$$

Proof. The LHS counts the number of even sized subsets of $[n]$ with positive sign and odd size subsets with negative sign. Then we proved the result using bijection between even sized and odd sized subsets of $[n]$. Hence, we get 0 on RHS. Let us formally define the bijection here.

Let E be the set of all even sized subsets of $[n]$ and O be the set of all odd sized subsets of $[n]$. Then the bijection $\phi_i : E \to O$ is defined with respect to an element $i \in [n]$ as follows.

Let $X \subseteq [n]$, such that $|X|$ is even. Then

$$\phi_i(X) = \begin{cases} X \setminus \{i\} & \text{if } i \in X \\ X \cup \{i\} & \text{if } i \notin X \end{cases}$$

Proof of bijection:

Well-defined: Given any even sized subset X, there are two possibilities: (i) $i \in X$, (ii) $i \notin X$. In first case, i is removed from X, hence its size reduces by one and becomes odd. In the second case, i is added, hence the size of the subset increases by one and becomes odd. Hence, ϕ is well defined.

Injective: Let X and X' be two distinct subsets of $[n]$. Then $\exists j \in [n]$ such that j is present in exactly one of the two subsets. Wlog, let $j \in X$ and $j \notin X'$. Now, if $j \neq i$, then $j \in \phi(X)$ and $j \notin \phi(X')$ and hence $\phi(X) \neq \phi(X')$. On the other hand, if $j = i$, then $j \notin \phi(X)$ and $j \in \phi(X')$. Hence, $\phi(X) \neq \phi(X')$.

Surjective: Let $Y \in O$ be an odd sized subset of $[n]$. From Y, we can recover X such that $\phi(X) = Y$ by the same operation as in ϕ. That is,

$$X = \begin{cases} Y \setminus \{i\} & \text{if } i \in Y \\ Y \cup \{i\} & \text{if } i \notin Y \end{cases}$$

It can easily be verified that in both the cases, X is an even sized subset of $[n]$.

This completes the proof. □

7.2.2 Proof for Eqn. (7.10)

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = \binom{n-1}{m}$$

Proof. Now we look at the second identity which is even more interesting. To prove this identity we use *almost bijection* where the bijection is between a set and subset of another set.

In words, the identity to prove, can be described as

$$\#\text{ of even sized subsets of } [n] \text{ of size atmost } m \;\_\; \#\text{ of odd sized subsets of } [n] \text{ of size atmost } m = (-1)^m \binom{n-1}{m}.$$

Clearly, there cannot be a bijection between the two sets (even sized subsets and odd sized subsets) in this case, since their difference is non-zero. This is where we use almost bijection.

We use following case analysis.

Case1: m is even: Then the identity to prove is:

$$\sum_{k=0}^{m}(-1)^k\binom{n}{k} = \binom{n-1}{m} \tag{7.11}$$

This can be interpreted as

$$\sum_{\substack{k=0,\\ k \text{ is even}}}^{m}\binom{n}{k} - \sum_{\substack{k=1,\\ k \text{ is odd}}}^{m-1}\binom{n}{k} = \binom{n-1}{m} \tag{7.12}$$

Let E be the set of all the even sized subsets of $[n]$ of size at most m and O be the set of odd sized subsets of $[n]$ having size at most $m-1$. Then, Eqn. (7.12) can intuitively interpreted as follows: there is a subset $E' \subseteq E$, such that E' is in bijection with O and $|E \setminus E'| = \binom{n-1}{m}$. Thus, we have three tasks at hand

- identify the set E', and
- define and prove the bijection between E' and O.
- prove that $|E \setminus E'| = \binom{n-1}{m}$

Defining the set E': Set E' is the union of two sets:

$$E' = \{X \subseteq [n] : |X| \text{ is even and } |X| \leq m-2\} \cup \{X \subseteq [n] : i \in X \text{ and } |X| = m\}$$

Defining the bijection: The bijection $\phi : E' \to B$ is defined in the same way as we defined it for first identity. That is, for $X \in E'$,

$$\phi(X) = \begin{cases} X \setminus \{i\} & \text{if } i \in X \\ X \cup \{i\} & \text{if } i \notin X \end{cases}$$

Proof of bijection

Well-defined: Let $X \in E'$, then (i) if $|X| \leq m-2$, then $|\phi(X)|$ is odd and $|\phi(X)| \leq m-1$, (ii) if $|X| = m$, then $i \in X$, hence $\phi(X) = X \setminus \{i\}$. This implies $|\phi(X)| = m-1$. Thus, in both the cases $\phi(X) \in O$.

Injective: Since, the function is same as in the previous case, the same argument for injectivity works.

Surjective: Let $Y \in O$ be an odd sized subset of $[n]$. From Y, we can recover $X \in E'$ such that $\phi(X) = Y$ by the same operation as in ϕ. That is,

$$X = \begin{cases} Y \setminus \{i\} & \text{if } i \in Y \\ Y \cup \{i\} & \text{if } i \notin Y \end{cases}$$

It can easily be verified that in both the cases, $|X|$ is even. In first case, since $|Y| \leq m-1, |X| \leq m-2$, hence $X \in E'$. In second case, since $i \notin Y$ and $|Y| \leq m-1$, $|X| \leq m$ and $i \in X$. Hence $X \in E'$, by definition.

This proves the bijection between E' and O.

Proof for: $|E \setminus E'| = \binom{n-1}{m}$

From the above definitions, $E \setminus E' = \{X \subseteq [n] : |X| = m, i \notin X\}$. This can be interpreted as $E \setminus E' = \{X \subseteq [n] \setminus \{i\} : |X| = m\}$. Hence, $|E \setminus E'| = \binom{n-1}{m}$.

Case2: m is odd: In this case the identity to prove is:

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = -\binom{n-1}{m} \tag{7.13}$$

This can be interpreted as

$$\sum_{\substack{k=0,\\ k \text{ is even}}}^{m-1} \binom{n}{k} - \sum_{\substack{k=1,\\ k \text{ is odd}}}^{m} \binom{n}{k} = -\binom{n-1}{m} \tag{7.14}$$

Equivalently,

$$\sum_{\substack{k=1,\\ k \text{ is odd}}}^{m} \binom{n}{k} - \sum_{\substack{k=0,\\ k \text{ is even}}}^{m-1} \binom{n}{k} = \binom{n-1}{m} \tag{7.15}$$

This time the set of odd sized subsets of $[n]$ of size at most m is bigger than the even sized subsets of $[n]$ of size at most m. The proof is same as that for the case of even m. Let E be the set of all the even sized subsets of $[n]$ of size at most $m-1$ (since m is odd) and O be the set of odd sized subsets of $[n]$ having size at most m. Then (7.15) can be interpreted as follows: there is a subset $O' \subseteq O$, such that E is in bijection with O' and $|O \setminus O'| = \binom{n-1}{m}$.

Thus, we have two task at hand

- identify the set O', and
- define and prove the bijection between E and O'.
- prove that $|O \setminus O'| = \binom{n-1}{m}$

Defining the set O': Set O' to be the union of two sets:

$$O' = \{Y \subseteq [n] : |Y| \text{ is odd and } |Y| \leq m-2\} \cup \{Y \subseteq [n] : i \in Y \text{ and } |Y| = m\}$$

Defining the bijection: The bijection $\phi : E \to O'$ is defined in the same way as we defined it

for first identity. That is, for $X \in E$,

$$\phi(X) = \begin{cases} X \setminus \{i\} & \text{if } i \in X \\ X \cup \{i\} & \text{if } i \notin X \end{cases}$$

Proof of bijection

Well-defined: Let $X \in E$, then $\phi(X)$ is of odd size because either an element is added or removed from X, which is of even size. Now, (i) if $i \in X$, then $\phi(X) = X \setminus \{i\}$. Hence, $|\phi(X)| \leq m - 2$ (because $|X| \leq m - 1$) which implies $\phi(X) \in O'$ (ii) if $i \notin X$, then, $\phi(X) = X \cup \{i\}$. This implies $|\phi(X)| \leq m$. But since, $i \in \phi(X)$, $\phi(X) \in O'$. This proves that ϕ is well- defined.

Injective: Since, the function is same as in sub section 7.2.1, the same argument for injectivity works.

Surjective: Let $Y \in O'$ be an odd sized subset of $[n]$. From Y, we can recover $X \in E$ such that $\phi(X) = Y$ by the same operation as in ϕ. That is,

$$X = \begin{cases} Y \setminus \{i\} & \text{if } i \in Y \\ Y \cup \{i\} & \text{if } i \notin Y \end{cases}$$

It can easily be verified that in both the cases, $|X|$ is even. In first case, $|Y| \leq m$ and hence $|X| \leq m - 1$. So, $X \in E$. In second case, since $i \notin Y$, $|Y| \leq m - 2$ (by definition) and hence $|X| \leq m - 1$. Hence $X \in E$.

This proves the bijection between E and O'.

Proof for: $|O \setminus O'| = \binom{n-1}{m}$

From the above definitions, $O \setminus O' = \{Y \subseteq [n] : |Y| = m, i \notin Y\}$. This can be interpreted as $O \setminus O' = \{Y \subseteq [n] \setminus \{i\} : |Y| = m\}$. Hence, $|O \setminus O'| = \binom{n-1}{m}$.

This completes the proof □

This proves both the identities.

7.3 Principle of Inclusion and Exclusion

Suppose we are given n sets $A_1, A_2, \ldots, A_n \subseteq G$, where G is some ground set. We are interested in finding the size of $A = A_1 \cup A_2 \cup \ldots \cup A_n$. This is very abstract scenario and we will see specific examples later, but here we are going to see classic use of the above identities in deriving this number.

So, we are interested in finding $|A| = |A_1 \cup A_2 \cup \ldots \cup A_n|$.

So, here is a thought process - Clearly, we can add the size of individual sets as $|A| = |A_1| + |A_2| + \ldots + |A_n|$, but this will over-count if there are some elements present in more than one sets. So, for that we need to subtract the double counting. For e.g. if $x \in A_1$ and $x \in A_2$, then it gets counted twice and to compensate for that we need to subtract $|A| = |A_1 \cap A_2|$ and we might attempt $|A| = |A_1| + |A_2| + \ldots + |A_n| - \sum_{1 \le i < j \le n} |A_i \cap A_j|$. But then, if x is present in A_1, A_2 and A_3, the it is under-counted (added thrice and subtracted thrice). So, again we need to compensate for that by adding $\sum_{1 \le i \le j \le k \le n} |A_i \cap A_j \cap A_k|$ in the above expression and this sequence goes on for any element being present in $k \le n$ sets and finally we get the expression for $|A|$ as follows

$$|A| = |A_1| + \cdots + |A_n| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n| \tag{7.16}$$

For $n = 2$, the above expression gives

$$|A| = |A_1| + |A_2| - |A_1 \cap A_2|$$

which we all must have seen before and can easily prove using Venn diagram.

In this section, we will formally prove the above expression for general n using the two identities we proved in previous section.

Proof. Consider any $x \in A_1 \cup A_2 \cup \cdots \cup A_n$. Let x appears in k of the A_i's. Then let us see how x gets counted

- $|A_1| + |A_2| + \cdots + |A_n|$: counts x k times (added)
- $\sum_{1 \le i < j \le n} |A_i \cap A_j|$: counts x $\binom{k}{2}$ times (subtracted)
- $\sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k|$: counts x $\binom{k}{3}$ times (added)
- and so on ...

Notice that in terms involving intersection of more than k sets, x never appears.

Thus,

$$\begin{aligned}
\substack{\#\text{of times } x \\ \text{gets counted}} &= k + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^{k+1} \binom{k}{k} \\
&= -\binom{k}{0} + \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^{k+1} \binom{k}{k} + \binom{k}{0} \\
&= -\sum_{i=0}^{k} (-1)^i \binom{k}{i} + \binom{k}{0} \\
&= \binom{k}{0} \qquad \text{from (7.9)} \\
&= 1
\end{aligned}$$

Thus, irrespective of the value of k, any element $x \in A_1 \cup A_2 \cup \cdots \cup A_n$ is counted exactly once. Hence, every $x \in A_1 \cup A_2 \cup \cdots \cup A_n$ is counted exactly once in RHS in (7.16).

This proves the PIE $\square$

Now let us look at the application of second identity that we derived. This identity is used in deriving a version of PIE which appears very naturally in several context. Let us look at one such example.

PIE says that if we want to derive $|A_1 \cup A_2 \cup \cdots \cup A_n|$, then the following expression does not give the correct count.

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

But we can ask, does this expression gives a lower or an upper bound? As we saw, this does over-counting, hence we can write

$$|A_1 \cup A_2 \cup \cdots \cup A_n| \leq |A_1| + |A_2| + \cdots + |A_n|$$

Now, suppose we include the next component, i.e.

$$|A_1| + |A_2| + \cdots + |A_n| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$$

Again from PIE we know that this also does not give the correct count. But we ask the same question again - does it give any lower or upper bound. And as we saw that this term can do some over-subtraction and hence we can say that this expression gives the lower bound. That is,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| \geq |A_1| + |A_2| + \cdots + |A_n| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$$

Similarly,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| \leq |A_1| + |A_2| + \cdots + |A_n| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k|$$

and we continue like this.

Let us now formally establish this observation. We use the same technique that we used in the proof of PIE.

Let x appears in k of the sets in $A_1, A_2, \ldots, A_n$. Suppose we cut off the PIE after $m \leq n$ sized

intersections. Then

$$\begin{aligned}
\begin{matrix}\#\text{of times } x \\ \text{gets counted}\end{matrix} &= \binom{k}{1} - \binom{k}{2} + \cdots + (-1)^{m+1}\binom{k}{m} \\
&= -\sum_{i=0}^{m}(-1)^i\binom{k}{i} + \binom{k}{0} \\
&= 1 + (-1)^{m+1}\binom{k-1}{m} \qquad \text{from (7.10)}
\end{aligned}$$

Thus, x is over counted or under counted depending on whether the second term on RHS is positive or negative. Let us analyze this for two cases.

Case1: $k \leq m$

Since, x appears in only $k \leq m$ sets and we are cutting down only after m, then this means that all possible intersections of this particular x are added and subtracted and x can not appear in any of the intersections of more than k sets. Hence, x is neither under counted nor over counted. In the expression, $\binom{k-1}{m} = 0$ Hence,

$$\#\text{of times } x \text{ is counted } = 1$$

Case2: $k > m$

In this case, x can be under counted or over counted depending upon whether m is even or odd. If m is odd then x is over counted.

If m is even then x is under counted.

Notice that either all $x \in A_1 \cup \mathsf{A}_2 \cup \cdots \cup A_n$ are correctly counted or under counted or all x are correctly counted or over counted based on the parity of m. Thus, whether a PIE cut down after m intersections gives lower bound or upper bound depends only on the parity of m. This principle is also called the *Bon Ferroni's inequality*.

Remark 7.3.1. *We used the equality in (7.11) to prove PIE. We can actually do the other way round as well, i.e. we can use PIE to prove this equality too.*

This completes this lecture. In the next lecture we will look at some applications of PIE.

7.4 Discussions

Bijection from Euler's problem to Binary Trees As we have already established a bijection from set of balanced parenthesisations to set of full binary trees and established that number of full binary trees with n internal nodes is the catlan number C_n, in this section, let's establish a bijection from the *Euler's Problem* to set of full binary trees to establish that the solution to *Euler's problem* is also catlan number C_n.

Lets recall *Euler's problem* first. Consider a convex polygon with $n+2$ edges. Euler's problem is the number of ways of triangulating it (partition the polygon into triangles) by drawing non-crossing diagonals. (Refer fig. 7.5). We know that number of non-crossing diagonals in a polygon of $n+2$ edges is $n-1$ (proof follows from a simple induction) and from those $n-1$ non-crossing diagonals, we have our polygon partitioned into n triangles. Let's associate each of the triangles with a vertex (green dots in the fig. 7.5). Observe that if two triangles share an edge, it must be one of the diagonals (no two triangles can share an edge because of non-crossing diagonals). Now, let's connect the vertices whose corresponding triangles share an edge. Any edge connecting two of these vertices crosses a diagonal. Now, consider a polygon edge e. For every polygon edge

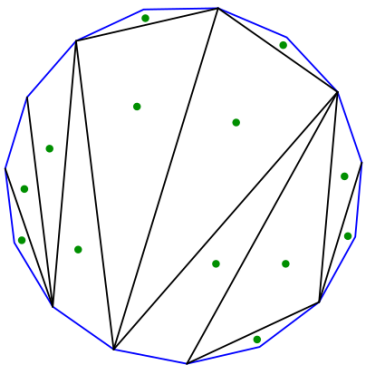


Figure 7.5: Partitioning a polygon into triangles by non-crossing diagonals. Observe that green dots in each triangle associates the triangle with a vertex

surrounding a vertex (other than e), add an open-edge originating from that vertex (see fig. 7.6). We arrive at the following claim.

Claim 7.4.1. *If we remove the underlying triangles (which are formed with polygon edges and diagonals), from fig. 7.6, the resulting graph obtained (see fig. 7.7) is a full binary tree with the vertices as internal nodes.*

Proof. We observe that degree of every vertex other than the vertex surrounded by edge e is 2. This vertex will act as root to our full binary tree. All other vertices have degree 3 because each vertex is surrounded by a triangle and if a side is a diagonal, it will be connected to vertex which is surrounded by triangle that shares the diagonal and if the side is a polygon edge, then there will be an open edge corresponding to it originating from the vertex. Therefore the resulting graph formed is a full binary tree with our vertices as n internal nodes and vertices corresponding to open edges are $n+1$ leaves (because there are $n+2$ edges and one edge is under consideration). This completes the description of bijection. □

We leave it as an exercise to the reader to prove that the mapping defined above is indeed a bijection.

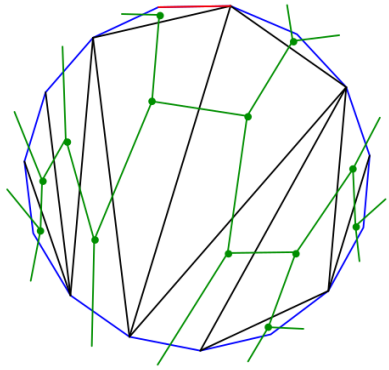


Figure 7.6: Polygon with vertices connected to form a tree

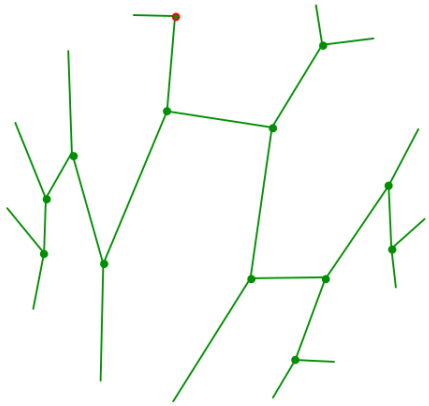


Figure 7.7: Tree formed by connecting vertices

Bijection from binary trees to full binary trees In this section we are interested in connection between binary and full binary trees. Recall that a full binary tree is one in which each node has either 0 or two children. On the other hand, when we say binary tree then it only means that each node can have at most two children. We want to find a bijection between set of binary trees with n internal nodes and set of full binary trees with certain number of internal nodes.

First of all lets try to see how to convert a given binary tree into a full binary tree so that we can reverse the process, i.e. recover the original (binary) tree back from the full binary tree without ambiguity.

Here is the first attempt:

Attempt 1: First natural approach can be to add a leaf node to all non-full (internal nodes having only one child) nodes, as shown in figure 7.8

But notice that this transformation is not injective. For example, it can be observed that both the trees in figure 7.9 map to same full binary tree.

Attempt 2(correct) Lets try a slightly different approach. Given a binary tree, do the following:

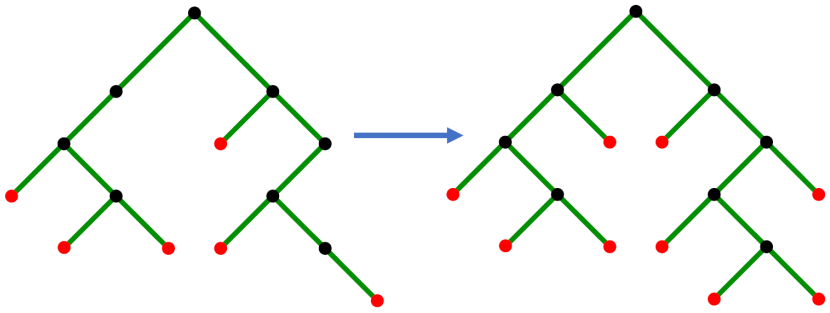


Figure 7.8: Binary to full binary tree attempt1: adding a child node to each non full node

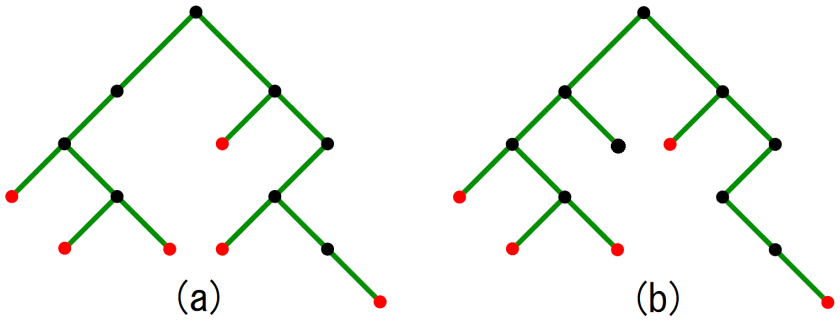


Figure 7.9: Two different binary trees that map to same full binary tree

- to each leaf node, add two children
- to each internal node having only one child, add another child

Figure 7.10 shows the full binary tree constructed in this way for the same binary tree as in Figure 7.8. We can see that this solution addresses the issue in the first attempt. Intuitively because of

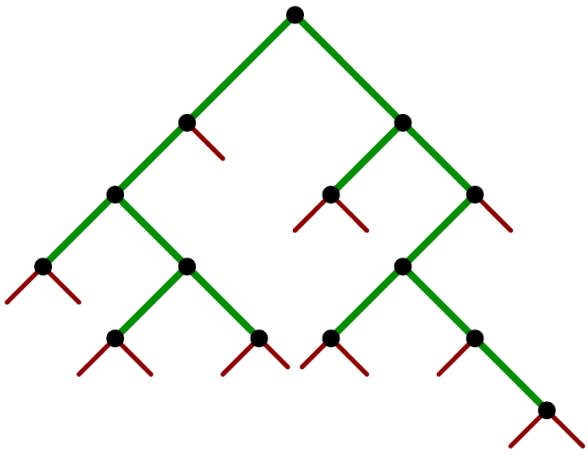


Figure 7.10: Full binary tree for the (non-full) binary tree given in fig 7.8. Notice that all the leaf nodes are added during transformation

following argument: in the previous attempt the problem was that given a full binary tree, it was hard to decide if a leaf node was originally present in the binary tree or added during transformation. Now, in the current solution, this issue does not arise, because for any leaf node originally present in the binary tree, we add two new leaves as its children. Thus, it can be observed that all the leaf nodes (and only these nodes) are added during transformation.

To see that this translation is well-defined, we can see that the transformed tree is full binary tree by construction itself. Surjectivity is also easy to prove. To recover a binary tree from any given full binary tree, simply remove all the leaf nodes. We discussed injection informally. To give a formal argument, we first need to identify how to characterize two different binary trees? One of the hint as given during the discussion is to assign address to the nodes in the form of binary string, where 0-1 represents left or right child.

Here we argued the bijection only intuitively and there are many things to be worked out formally. For example, proof for injection is not formally argued. Also, to argue surjection, we need to fix the number of nodes in full binary tree. Once we figure out this number, the argument for transformation being well-defined also need to take that into account.

Writing a complete formal proof of bijection is left as homework exercise.

Bijection between plane trees and full binary trees A plane tree is a rooted tree with an ordering among the children. A plane tree can have more than two children. Figure 7.11 shows a plane tree.

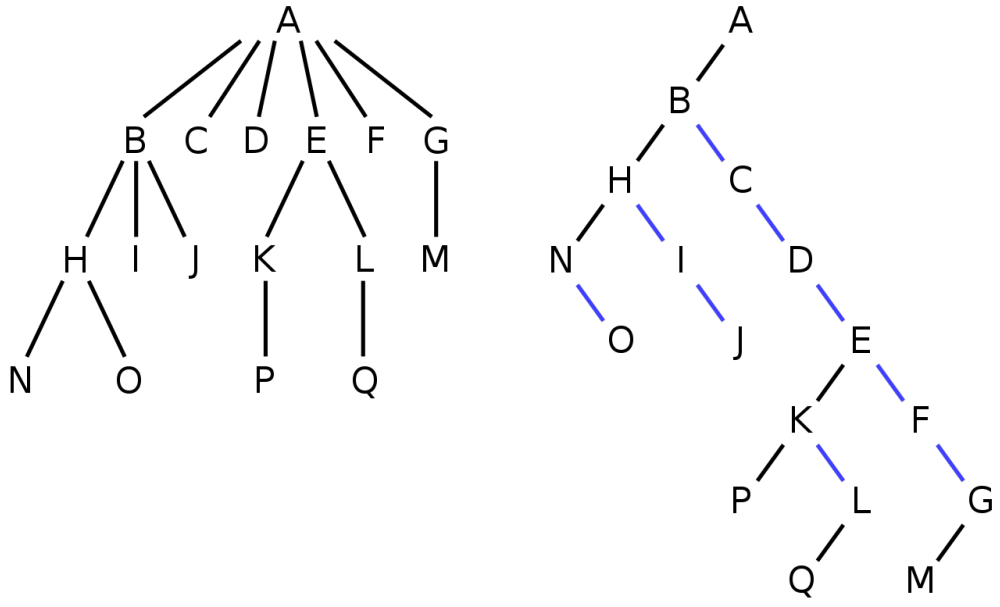


Figure 7.11: An example of plane trees and its transformation to a binary tree

We are interested in studying the connection between plane trees and binary trees. The number of plane trees with n nodes is equal to the number of binary trees with n nodes. Thus, there is bijection between set of plane trees with n nodes and the set of binary trees with n nodes.

Here we define the bijection function.

The Bijection: Given any plane tree, do the following

- For each node in the tree,
  - add its first child in plane tree as its left child in binary tree
  - add its immediate sibling on right as its right child in binary tree.

  child in the binary tree.

By following the above rule, we get a binary tree from given plane tree.

Observe that in the binary tree thus obtained, root node has only one child, while in general, in a binary tree the root can have both its children. Hence, we won't include the root as part of the binary tree.

Writing formal argument for all the properties is left as homework excercise.

Instructor : Jayalal Sarma
Scribe : Sumanth Naik (*TA:* JS)
Date : Sept 29, 2020
Status : α

Lecture
8

PIE and three applications

8.1 Introduction

The journey so far has been that we have been doing counting by bijections and established certain ideas regarding double counting and the bijections behind the scenes. Then we came to Principle of Inclusion-Exclusion(PIE) as a consequence of a bijection argument. In this lecture, we will look at another proof (an algebraic proof) for PIE and then 3 interesting applications of PIE.

8.2 Principle of Inclusion - Exclusion(PIE)

If there are n subsets of a ground set X; A_1, A_2, A_3, ..., $A_n \subseteq X$, then PIE helps us to estimate the size of the set of union of all n subsets of the ground set. Mathematically, PIE states that,

$$\begin{aligned}
|\bigcup_{i=1}^{n} A_i| &= \sum_{1\leq i\leq n} |A_i| \; - \sum_{1\leq i<j\leq n} |A_i \cap A_j| \\
&\quad + \sum_{1\leq i<j<k\leq n} |A_i \cap A_j \cap A_k| \; \ldots\ldots \\
|\bigcup_{i=1}^{n} A_i| &= \sum_{\emptyset\neq I\subseteq[n]} (-1)^{|I|+1} |\bigcap_{i\in I} A_i| \\
&= \sum_{\emptyset\neq I\subseteq[n]} (-1)^{|I|+1} |A_I|
\end{aligned}$$

where $[n] = \{1, 2, 3...n\}$ (short-hand notation for 1 to n elements) and $A_I = \bigcap_{i\in I} A_i$.

Note that the intuition behind understanding the formula in the second step from first is that, $\emptyset \neq I \subseteq [n]$ captures all the combinations of $1, 2, 3...n$ sized sets from n sized set of numbers, i.e., $1 \leq i \leq n$ (set of combinations of 1 sized set from n sized set), $1 \leq i < j \leq n$ (set of combinations of 2 sized set from n sized set) and so on up to set of combinations of n sized set from n sized set. The alternating sign in first equation's term is captured by $(-1)^{|I|+1}$ in second equation. And

finally, the intersection part of all the terms in first equation, i.e., $|A_i|, |A_i \cap A_j|, |A_i \cap A_j \cap A_j|$...., is captured in $\bigcap_{i \in I} A_i$ of the second equation.

Proof. This algebraic proof is using characteristic functions of A_1, A_2, A_3, ..., A_n (which are $f_1, f_2, f_3, ...f_n$).

$$f_i : X \longrightarrow \{0, 1\}$$

$$\forall x \in X, \quad f_i(x) = \begin{cases} 1 & \text{if } x \in A_i \\ 0 & otherwise \end{cases}$$

Note that $(1 - f_i(x))$ is the characteristic function for the compliment of A_i (i.e. $X \setminus A_i$ or $\overline{A}_i$). In other words; when you subtract the characteristic function of a set from 1, the difference is the characteristic function of the compliment of the same set. It is also to be noted that $f_i(x)f_j(x)$ is the characteristic function of $A_i \cap A_j$. In other words; when you multiply the characteristic functions of two sets with each other, the product is the characteristic function of the intersection of the two sets.

Consider a function defined as,

$$\begin{aligned} F(x) &= \prod_{i=1}^{n}(1 - f_i(x)) \\ &= (1 - f_1(x))(1 - f_2(x))....(1 - f_n(x)) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|}(\prod_{i \in I} f_i(x)) \end{aligned} \tag{8.17}$$

Note that the $F(x)$ represents the characteristic function of intersection of compliments (compliment of each f_i), hence by De-Morgan's Law, its mathematical equivalent is,

$$\overline{(\bigcup_{i=1}^{n} A_i)} = X \setminus \bigcup_{i=1}^{n} A_i$$

To get the size of the set in the RHS of previous equation (it has all the elements which are not present in any of the n subsets of X), we just need to count the number of x's in X for which $F(x)$ is 1 (as $F(x)$ will be 1 for any x only if every $f_i(x)$ is 0, i.e., $\forall i, x \notin A_i$). Hence,

$$|X \setminus \bigcup_{i=1}^{n} A_i| = \sum_{x \in X} F(x) \tag{8.18}$$

Also from (8.17),

$$\begin{aligned}\sum_{x\in X} F(x) &= \sum_{x}\sum_{I\subseteq[n]} (-1)^{|I|}(\prod_{i\in I} f_i(x)) \\ &= \sum_{I\subseteq[n]} (-1)^{|I|}(\sum_{x}(\prod_{i\in I} f_i(x))) \\ &= \sum_{I\subseteq[n]} (-1)^{|I|}|\bigcap_{i\in I} A_i| \end{aligned} \tag{8.19}$$

The last step is because $(\prod_{i\in I} f_i(x))$ is the characteristic function of intersection of n subsets, i.e., $\bigcap_{i\in I} A_i$. And its summation over x, $(\sum_x(\prod_{i\in I} f_i(x)))$ will give us the size of the intersection, $|\bigcap_{i\in I} A_i|$.
Also, note that the convention when $I = \emptyset$ is,

$$|\bigcap_{i\in I} A_i| = |X| \tag{8.20}$$

which can be reasoned as when I is empty, $(\prod_{i\in I} f_i(x))$ is 1 for any x. And its summation over x, $(\sum_x(\prod_{i\in I} f_i(x)))$ gives $|X|$.

By (8.18) and (8.19),

$$\begin{aligned} |X \setminus \bigcup_{i=1}^{n} A_i| &= \sum_{I\subseteq[n]} (-1)^{|I|}|\bigcap_{i\in I} A_i| \\ |X| - |\bigcup_{i=1}^{n} A_i| &= \sum_{I\subseteq[n]} (-1)^{|I|}|\bigcap_{i\in I} A_i| \\ |\bigcup_{i=1}^{n} A_i| &= |X| - \sum_{I\subseteq[n]} (-1)^{|I|}|\bigcap_{i\in I} A_i| \\ &= \sum_{\emptyset\neq I\subseteq[n]} (-1)^{|I|+1}|\bigcap_{i\in I} A_i| \qquad \text{(Using (8.20))} \end{aligned}$$

This completes the algebraic proof for PIE. □

8.3 Applications of PIE

8.3.1 Counting the number of derangements on n elements.

Consider a scenario where, n people go to a theatre to watch a movie, they keep their hats outside with the gatekeeper. On return, in a rush, the gatekeeper panicked and gave back the hats ran-

domly.
Question: What is the chance that nobody got their own hat for a very large n?
Answer (surprisingly): $1/e = 0.3678$.

Theorem 8.3.1. *Number of derangements on n elements is*

$$(\sum_{k=0}^{n} \frac{(-1)^k}{k!})n!$$

(We know that the total number of ways for the n people to pick n hats is $n!$ (factorial of n) and hence the chance of derangement is $(\sum_{k=0}^{n} \frac{(-1)^k}{k!})$. As $n \to \infty$, $(\sum_{k=0}^{n} \frac{(-1)^k}{k!}) \to 1/e \sim 0.3678$.)

Proof. Let S_n be the set of permutations on n elements. $\sigma \in S_n$ is a permutation function on n elements ($\sigma : [n] \to [n]$). $\forall_{i=1}^{n},\ \sigma(i)$ is defined as the person to whom i^{th} person's hat was given. If $\sigma(i) = i$, then it means that the i^{th} person got the correct hat - this is called a fix-point. What we are looking for is to count the number of fix-point free permutations in S_n.
The strategy is to count the number of non-derangements and subtract from $n!$. Mathematically, non-derangement is captured as

$$\exists i,\ \ \sigma(i) = i$$

Define A_i as,

$$\forall i \in \{1, 2, ...n\},\ \ A_i = \{\sigma \in S_n \mid \sigma(i) = i\}$$

So, A_i represents the set of n elements whose i^{th} element is fixed to i, other elements can be any non repeating value of 1 to n (except i as it is taken).
Set of non-derangement can be represented as

$$\bigcup_{i=1}^{n} A_i$$

Hence, we are interested in finding the number of non-derangements

$$|\bigcup_{i=1}^{n} A_i|$$

From PIE's statement,

$$A_I = \bigcap_{i \in I} A_i$$
$$|A_I| = (n - |I|)! \tag{8.21}$$

The previous step can be arrived at as follows : In A_I, $\forall i \in I$, $\sigma(i)$ is fixed to i by definition. For

the remaining $n-|I|$ values, σ can take any random permutation of the same $n-|I|$ values, hence $(n-|I|)!$.
Using PIE and using the idea of fixing size of I and sum over each size in next step,

$$\begin{aligned}
|\bigcup_{i=1}^{n} A_i| &= \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} |A_I| \\
&= \sum_{k=1}^{n} (-1)^{k+1} (\sum_{I \subseteq [n], |I|=k} |A_I|) \\
&= \sum_{k=1}^{n} (-1)^{k+1} (\sum_{I \subseteq [n], |I|=k} (n-k)!) \qquad \text{(By (8.21))} \\
&= \sum_{k=1}^{n} (-1)^{k+1} (n-k)! \binom{n}{k} \\
&= \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!} \\
&= (\sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!}) n! \qquad (8.22)
\end{aligned}$$

Now, to get number of derangements, subtract (8.22) from $n!$, which is

$$n! - (\sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!}) n! = (\sum_{k=0}^{n} \frac{(-1)^{k}}{k!}) n!$$

□

8.3.2 Euler's $\varnothing$ function.

Theorem 8.3.2. *Let $n \in N$, $\varnothing(n)$ = number of numbers $\leq n$, which are relatively prime to n. If*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

where p_i are distinct primes and $\forall i,\ \alpha_i \geq 1$, then

$$\varnothing(n) = n(\prod_{i=1}^{k} (1 - \frac{1}{p_i}))$$

Proof. Let $X = \{1, 2, 3, ..., n\}$. Then,

$$\forall 1 \leq i \leq k, A_i = \{m \in X \ \mid \ p_i \ divides \ m\}$$

So, A_i represents the set of multiples of p_i less than n.

Number of numbers which are not relatively prime to n is given by (as every number in any of A_i will have p_i as common factor)

$$(\bigcup_{i=1}^{k} A_i)$$

Hence,

$$\begin{aligned} \varnothing(n) &= n - |\bigcup_{i=1}^{k} A_i| && \text{(apply PIE)} \\ &= n - \sum_{I \subseteq [k], I \neq \emptyset} (-1)^{|I|+1} |A_I| && (8.23) \end{aligned}$$

Here,

$$|A_I| = |\bigcap_{i \in I} A_i| = \frac{n}{\prod_{i \in I} p_i} \tag{8.24}$$

The previous step can be reasoned as follows : In $\bigcap_{i \in I} A_i$, there will be those numbers which are multiples of all the p_i's. The same set can be obtained by including the product of every p_i, i.e., $\prod_{i \in I} p_i$, and all the numbers less than n which are multiples of that product. The number of such numbers can be captured by $\frac{n}{\prod_{i \in I} p_i}$.
By (8.23), (8.24) and using the convention of $\prod_{i \in I} p_i$ is 1 when $I = \emptyset$,

$$\begin{aligned} \varnothing(n) &= n - \sum_{I \subseteq [k], I \neq \emptyset} (-1)^{|I|+1} \frac{n}{(\prod_{i \in I} p_i)} \\ &= \sum_{I \subseteq [k]} (-1)^{|I|} \frac{n}{(\prod_{i \in I} p_i)} \\ &= n \sum_{I \subseteq [k]} (-1)^{|I|} \frac{1}{(\prod_{i \in I} p_i)} \\ &= n(\prod_{i=1}^{k} (1 - \frac{1}{p_i})) \end{aligned}$$

Note that the last step is done similar to (8.17) in PIE (section 8.2) derivation : f_i there is equivalent to $\frac{1}{p_i}$ here. This completes the proof for the theorem. □

Corollary 8.3.3. *$\varnothing$ is multiplicative when numbers are co-primes. i.e., if n_1, n_2 are co-primes, then $\varnothing(n_1 n_2) = \varnothing(n_1)\varnothing(n_2)$.*

Proof. Let A be the set of prime factors of $n_1 n_2$. Since $n_1 n_2$ is the product of two numbers n_1 and n_2, any prime $p \in A$ should divide at least one of n_1 and n_2. If n_1 and n_2 are co-primes, then the do not have any common prime factor. Therefore, any prime $p \in A$ should divide exactly one of n_1 and n_2. So, we can partition the set A into two sets X and Y where X is the set of prime factors

of n_1 and Y is that of n_2.

$$\begin{aligned}\varnothing(n_1n_2) &= n_1n_2(\prod_{p\in A}(1-\frac{1}{p})) \\ &= n_1(\prod_{p\in X}(1-\frac{1}{p})).n_2(\prod_{p\in Y}(1-\frac{1}{p})) \\ &= \varnothing(n_1)\varnothing(n_2)\end{aligned}$$

Thus, if n_1, n_2 are co-primes, then $\varnothing(n_1n_2) = \varnothing(n_1)\varnothing(n_2)$. □

8.3.3 Probability that two natural numbers are co-primes

For two randomly chosen natural numbers, what is the probability that they do not have a common factor (other than 1)?
Answer: $\sim 60\%$

Proof. Fix n; $S = \{(a,b)|a,b \in [n]\}$.
Consider two definitions, the good set G (represents set of pairs whose elements have $gcd = 1$) and the bad set B (represents set of pairs whose elements have $gcd > 1$),

$$G = \{(a,b)|\text{ no } d > 1 \text{ exist such that } d\ divides\ a \text{ and } d\ divides\ b\}$$

$$B = \{(a,b)|\exists d > 1 \text{ such that } d\ divides\ a \text{ and } d\ divides\ b\}$$

We want the upper bound of $|B|$ in terms of n^2.
Define X which has all the permutations of pairs possible as,

$$X = \{(a,b)|a,b \in [n]\}$$

And for prime $p \leq n$, define A_p as a set which contains pairs whose elements both have p as a prime factor and the pair belongs to X.

$$A_p = \{(a,b)|p\ divides\ a, p\ divides\ b, p\ is\ prime, (a,b) \in X\}$$

Clearly,

$$B = \bigcup_{p\leq n} A_p$$

By PIE,

$$|B| = \sum_{I\subseteq Q, I\neq\emptyset} (-1)^{|I|+1}|A_I| \text{ where, } Q = \{p|p \leq n, prime\} \tag{8.25}$$

Now, the aim is to estimate $|A_I|$ (as stated in PIE), we can write,

$$|A_I| = |\bigcap_{p_i \in I} A_{p_i}| \tag{8.26}$$

Here, $\bigcap_{p_i \in I} A_{p_i}$ denotes the set of pairs whose elements are both divisible by product of numbers (which are primes) in I. Note that the product need not be a prime. We can not write the resulting set ($\bigcap_{p_i \in I} A_{p_i}$) in terms of A_p as p is prime in the definition. So, lets create a new definition.
Let's define A_d, which denotes the set of pairs whose elements both have d as a factor and the pairs belongs to X (note that this definition is different from A_p as there p should be a prime, here d can be any number),

$$A_d = \{(a,b) | d \; divides \; a, d \; divides \; b, (a,b) \in X\}$$

Rewriting (8.26) using the definition of A_d,

$$|A_I| = |A_d| \;\; where, \quad d = \prod_{p_i \in I} p_i \tag{8.27}$$

Estimating $|A_d|$ separately, from definition, a can be any mutiple of d which is less than or equal to n, similarly b too can be any mutiple of d which is less than or equal to n. Hence,

$$\begin{aligned} |A_d| &= \lfloor \frac{n}{d} \rfloor \lfloor \frac{n}{d} \rfloor \\ &= (\lfloor \frac{n}{d} \rfloor)^2 \end{aligned} \tag{8.28}$$

From (8.25), splitting the summation by number of primes taking part,

$$\begin{aligned} |B| &= \sum_{k \geq 1} (\sum_{I \subseteq Q, I \neq \emptyset, |I| = k} (-1)^{|I|+1} |A_I|) && \text{(Apply (8.27) and (8.28))} \\ &= \sum_{k \geq 1} (\sum_{\substack{d \leq n, \\ \text{primes from } Q}} \sum_{\substack{d \text{ is a product} \\ \text{of } k \text{ distinct}}} (-1)^{k+1} (\lfloor \frac{n}{d} \rfloor)^2) && (8.29) \end{aligned}$$

Note that the value of k is used only to determine the sign of the terms in $|B|$. Usage of Mobius function gives a clever way to reduce the equation of $|B|$ to a single summation from double summation.
Mobius function $\mu(d)$ is given by

$$\mu(d) = \begin{cases} 0 & \text{if } p^2 \text{ divides } d, \; p \text{ is prime} \\ 1 & \text{if } d = 1 \\ (-1)^k & \text{if } d \text{ is a product of } k \text{ distinct primes} \end{cases}$$

Using $\mu(d)$ in (8.29),

$$|B| = \sum_{2 \le d \le n} (-\mu(d)((\lfloor \frac{n}{d} \rfloor)^2))$$

Now estimating $|G|$; since all of S can be either in G or B but not both and size of S is n^2,

$$\begin{aligned} |G| &= n^2 - |B| \\ &= n^2 + \sum_{2 \le d \le n} \mu(d)((\lfloor \frac{n}{d} \rfloor)^2) \\ &= \sum_{1 \le d \le n} \mu(d)((\lfloor \frac{n}{d} \rfloor)^2) \end{aligned} \tag{8.30}$$

Last step uses the fact that $\mu(1) = 1$ in the Mobius function.
Furthermore for any x,

$$\begin{aligned} (\lfloor x \rfloor)^2 - x^2 &= (x - \{x\})^2 - x^2 \\ &= x^2 - 2\{x\}x + \{x\}^2 - x^2 \\ &= -2x\{x\} + \{x\}^2 \\ &= O(x) \end{aligned}$$

Using this fact in (8.30),

$$\begin{aligned} |G| &= \sum_{1 \le d \le n} \mu(d)(\frac{n^2}{d^2} + O(\frac{n}{d})) \\ &= n^2 \sum_{1 \le d \le n} \frac{\mu(d)}{d^2} + O(n \sum_{1 \le d \le n} (\frac{\mu(d)}{d})) \end{aligned} \tag{8.31}$$

Estimating the second term in (8.31):

$$\begin{aligned} n \sum_{1 \le d \le n} (\frac{\mu(d)}{d}) &\le n(\sum_{1 \le d \le n} \frac{1}{d}) \\ &\le n \log n \end{aligned} \tag{8.32}$$

Last step is derived by the asymptotic estimate of the sequence of Harmonic series.

Estimating the first term in (8.31):
Using Euler's series, the following approximation can be done.

$$M = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \sim \frac{6}{\pi^2} \tag{8.33}$$

It can also be proven that

$$|M - \sum_{1 \leq d \leq n} \frac{\mu(d)}{d^2}| \leq \frac{1}{n} \tag{8.34}$$

Using (8.31), (8.32), (8.33) and (8.34),

$$\begin{aligned} |G| &= n^2(\frac{6}{\pi^2} + \frac{1}{n}) + O(n \log n) \\ |G| &= n^2 \frac{6}{\pi^2} + O(n \log n) \\ \frac{|G|}{n^2} &= \frac{6}{\pi^2} + O(1) \end{aligned}$$

Thus, as $n \to \infty$, the probability that two randomly chosen numbers do not have a common factor converges to $\frac{6}{\pi^2} \sim 60\%$. □

Instructor : Jayalal Sarma
Scribe : Raghul (*TA:* JS)
Date : Sept 29, 2020
Status : α

Lecture
9

Surjections and Stirling numbers

9.1 Introduction

In this lecture, we will look at another application of Principle of Inclusion-Exclusion(PIE) - counting number of surjections. Later, we will look at a concept related to that application - Stirling numbers of the second kind.

9.2 Applications of PIE

9.2.1 Number of surjections from $[m]$ to $[n]$

Consider $f : [m] \to [n]$. The total number of functions is n^m - each element in $[m]$ has n choices for its image. The number of injections is $\binom{n}{m}m!$ - the m different images required can be chosen from $[n]$ in $\binom{n}{m}$ ways and then these images can assigned their pre-images from $[m]$ in $m!$ ways. The number of surjections is not that obvious and can be derived using PIE.

Theorem 9.2.1. *The number of surjections from $[m]$ to $[n]$ is given by*

$$\sum_{k=0}^{n}(-1)^k(n-k)^m\binom{n}{k}$$

Proof. Let X be the set of all functions from $[m]$ to $[n]$. We know that

$$|X| = n^m \tag{9.35}$$

Let us define A_i ($\subseteq X$) for all $i \in [n]$ as follows.

$$A_i = \{f : [m] \to [n] \mid \forall j \in [m],\ f(j) \neq i\}$$

In other words, A_i is the set of functions in which the element i in $[n]$ does not have a pre-image and hence any element in A_i is a non-surjection. The union of all the A_i's will be the set of all non-surjections.
Clearly, $|A_i| = (n-1)^m$: since each element in $[m]$ has only $n-1$ choices for its image. Similarly, $\forall i < j,\ |A_i \cap A_j| = (n-2)^m$ and so on. Thus, for any $I \subseteq [n]$,

$$|A_I| = |\bigcap_{i \in I} A_i| = (n - |I|)^m \tag{9.36}$$

Using PIE to find the number of non-surjections,

$$\begin{aligned}
|\bigcup_{i=1}^{n} A_i| &= \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} |A_I| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{I \subseteq [n], |I|=k} |A_I| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{I \subseteq [n], |I|=k} (n-k)^m && \text{(By 9.36)} \\
&= \sum_{k=1}^{n} (-1)^{k+1} (n-k)^m \binom{n}{k} && (9.37)
\end{aligned}$$

Therefore, the number of surjections is given by

$$\begin{aligned}
|X \setminus \bigcup_{i=1}^{n} A_i| &= |X| - |\bigcup_{i=1}^{n} A_i| \\
&= n^m - \sum_{k=1}^{n} (-1)^{k+1} (n-k)^m \binom{n}{k} && \text{(using 9.35 and 9.37)} \\
&= (-1)^0 (n-0)^m \binom{n}{0} + \sum_{k=1}^{n} (-1)^k (n-k)^m \binom{n}{k} \\
&= \sum_{k=0}^{n} (-1)^k (n-k)^m \binom{n}{k}
\end{aligned}$$

This completes the proof. □

9.3 Stirling numbers of the second kind

Let us now look at another way of counting the number of surjections - in terms of Stirling numbers of the second kind. The number of ways of partitioning $[n]$ into k non-empty parts,

where neither the order of the parts nor the order of elements within a part matter, is denoted by $\left\{ {n \atop k} \right\}$ and is a Stirling number of the second kind.
For example; $\left\{ {4 \atop 1} \right\} = 1$ because [1,2,3,4] is the only way of partitioning, $\left\{ {4 \atop 2} \right\} = 7$ because $[1, 2, 3|4]$, $[1, 2, 4|3]$, $[1, 3, 4|2]$, $[2, 3, 4|1]$, $[1, 2|3, 4]$, $[1, 3|2, 4]$ and $[1, 4|2, 3]$ are the ways of partitioning, $\left\{ {4 \atop 3} \right\} = 6$ because $[1, 2|3|4]$, $[1, 3|2|4]$, $[1, 4|2|3]$, $[1|2, 3|4]$, $[1|2, 4|3]$ and $[1|2|3, 4]$ are the ways of partitioning and $\left\{ {4 \atop 4} \right\}$ = 1 because $[1|2|3|4]$ is the only way of partitioning.

Let us now count the number of surjections from $[m]$ to $[n]$ in terms of Stirling numbers of the second kind. We know that in a surjection, every element in the co-domain $[n]$ has at least one pre-image. So, we could partition the domain $[m]$ into n non-empty parts such that all the elements within a part have the same image in the co-domain. (For example; for $f : [5] \to 0, 1, 2$, $f(x) = x \ mod \ 3$, the partition of the domain is $[1, 4|2, 5|3]$.) Such a partition could be done in $\left\{ {m \atop n} \right\}$ ways and then each of these parts can be assigned to one element in $[n]$ in $n!$ ways. Thus the number of surjections from $[m]$ to $[n]$ in terms of Stirling numbers of the second kind is $\left\{ {m \atop n} \right\} n!$.

We have counted the number of surjections in 2 different ways (using PIE and in terms of $\left\{ {m \atop n} \right\}$). These two values should be equal and equating them would give us an expression for $\left\{ {m \atop n} \right\}$ as follows.

$$\left\{ {m \atop n} \right\} n! = \sum_{k=0}^{n} (-1)^k (n-k)^m \binom{n}{k}$$

$$\left\{ {m \atop n} \right\} = \frac{1}{n!} \sum_{k=0}^{n} (-1)^k (n-k)^m \binom{n}{k}$$

It is to be noted that by convention, $\left\{ {0 \atop 0} \right\} = 1$ and $\forall n > 0, \left\{ {n \atop 0} \right\} = \left\{ {0 \atop n} \right\} = 0$.

Theorem 9.3.1. *For any $n, k \in \mathbb{N}$;*

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}$$

Proof. We shall use double counting to prove this theorem. Let us count the number of ways of partitioning $[n]$ into k non-empty parts.
Clearly, the L.H.S. of the equation is the number of ways of partitioning $[n]$ into k non-empty parts. Consider the element n in $[n]$; in a partition, this element can either be in a part of size 1 or a part of size ≥ 2. The number of partitions in which n is in a part of size 1 is $\left\{ {n-1 \atop k-1} \right\}$: n is the only element in a part and then the remaining $n-1$ elements are to be partitioned into $k-1$ non-empty parts. The number of partitions in which n is in a part of size ≥ 2 is $k\left\{ {n-1 \atop k} \right\}$: the remaining $n-1$ elements are to be partitioned into k non-empty parts and then n is added to one of those parts in k ways. Thus, the total number of partitions is $\left\{ {n-1 \atop k-1} \right\} + k\left\{ {n-1 \atop k} \right\}$, which is the R.H.S. of the equation.

These two methods have counted the same value and hence should be equal. □

The equation stated in the theorem above is actually a very important property of Stirling numbers of the second kind. It is often used to connect any function or a set of numbers with the Stirling numbers of the second kind.

9.4 Instances of Stirling numbers of the second kind

Following are some of the instances where Stirling numbers of second kind appear.

9.4.1 n^{th} derivative of e^{e^x}

The n^{th} derivative of the function $f(x) = e^{e^x}$ is given by

$$f^{(n)}(x) = f(x) \sum_{k=0}^{\infty} \left\{ {n \atop k} \right\} e^{kx}$$

9.4.2 Falling factorials of x

We know that polynomials in one variable x (like $4x^2 + 3x + 2$, $10x^3 + 9x$, etc.) can be expressed as a linear combination of the powers of x i.e. $x^0, x^1, x^2, \ldots$. Thus, the powers of x are said to form a basis for such polynomials.
The falling factorials of x form another basis for polynomials in one variable x. The falling factorials are given by

$$(x)_0 = 1 \qquad (x)_1 = x$$
$$(x)_2 = x(x-1) \qquad for\ any\ k > 0,\ (x)_k = x(x-1)(x-2)\ldots(x-k+1)$$

One can easily prove that the falling factorials form a basis for polynomials if it can be proved that $\forall n$, x^n is a linear combination of falling factorials (for any polynomial, write the polynomial as a linear combination of x^n's and then replace x^n's with the corresponding linear combinations of $(x)_n$'s).

Theorem 9.4.1. *Powers of x can be written as the linear combination of falling factorials of x using the following equation.*

$$\forall n, x^n \equiv \sum_{k=0}^{n} \left\{ {n \atop k} \right\} (x)_k$$

Proof. (Note: This proof was done during the discussion session - not in the lecture video.)
Let the polynomial on the L.H.S. be $P(x)$ and that on the R.H.S. be $Q(x)$. In order to prove that $P(x) \equiv Q(x)$, it is sufficient to prove that $P(x) = Q(x)$ for sufficiently large number of distinct values of x. The reasoning for the same is as follows.

One can clearly see that the degree of both $P(x)$ and $Q(x)$ is n. So, the maximum degree of the polynomial $R(x) = P(x) - Q(x)$ is also n. This implies that the maximum number of roots for the equation $R(x) = 0$ is n. Therefore, if one can prove that $R(x) = 0$ for at least $n + 1$ distinct values of x, then it must be the case that $R(x) \equiv 0$ and hence $P(x) \equiv Q(x)$.
So, all we have to do now is to prove that $P(x) = Q(x)$ for at least $n + 1$ distinct x's where n is the degree of the polynomial $P(x)$. Let us use double counting to prove this.

Let x be any natural number. Let us count the number of different strings of length n over $\{1, 2, 3 \dots x\}$ in two different ways.

1. Each character in the string can be chosen in x ways and there are n characters in total. Therefore the count is x^n $(= P(x))$.

2. Let there be k distinct characters in our string. Clearly, $0 \leq k \leq n$ and different values of k would lead to different strings. So, we have to do summation over the value of k. Now, let us partition the n available spaces into k non-empty parts - so that spaces within the same part will get the same character and spaces in different parts get different characters. This partitioning can be done in $\left\{ {n \atop k} \right\}$ ways. There are k parts now and we have to assign one character each to these parts from $\{1, 2, 3 \dots x\}$. The character for the first part can be chosen in x ways, for the second part it is $(x - 1)$ ways, for the third part it is $(x - 2)$ ways and so on until $(x - k + 1)$ ways for the k^{th} part. Therefore, the count here is given by

$$\sum_{k=0}^{n} \left\{ {n \atop k} \right\} x(x-1)(x-2)\dots(x-k+1) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} (x)_k = Q(x)$$

These two methods count the same number and hence they should be equal. Therefore, $\forall x \in \mathbb{N},\ P(x) = Q(x)$, irrespective of the value of n. This means that for any n, we have proven that $P(x) = Q(x)$ for an infinite number of values of x. Hence, $\forall n,\ P(x) \equiv Q(x)$. □

9.5 Other interesting types of numbers

9.5.1 Bell numbers (B_n)

The number of ways of partitioning $[n]$ into non-empty parts is given by the Bell number B_n. It can clearly be seen that

$$B_n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\}$$

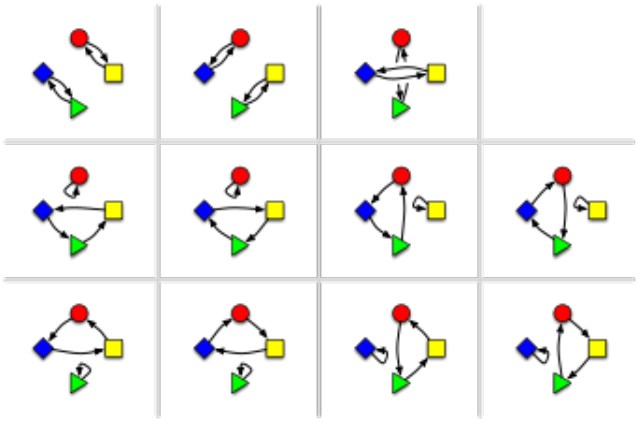


Figure 9.12: Permutations on 4 elements with 2 cycles

9.5.2 Stirling numbers of the first kind ($\begin{bmatrix} n \\ k \end{bmatrix}$)

The number of ways of permuting n elements such that the permutations have k cycles is given by the Stirling number of the first kind $\begin{bmatrix} n \\ k \end{bmatrix}$. Figure 9.12 shows all possible ways of permuting 4 elements with 2 cycles ($\begin{bmatrix} 4 \\ 2 \end{bmatrix} = 11$). From the definition of $\begin{bmatrix} n \\ k \end{bmatrix}$, it can clearly be seen that

$$n! = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix}$$

Instructor : Jayalal Sarma
Scribe : Raghul (*TA:* JS)
Date : Sept 29, 2020
Status : α

Lecture
10

Tutte's Matrix Tree Theorem and counting arborescences

10.1 Introduction

In this lecture, we will be looking at another application of the Principle of Inclusion-Exclusion(PIE) - Matrix Tree Theorem. We will understand the theorem and then we will cover all the bases required to prove the theorem. The proof of the theorem will be completed in the next lecture.

10.2 Kirchoff's Matrix Tree Theorem

The original theorem for undirected graphs was stated by Kirchoff in the 19th century and the generalised verion for directed graphs was stated by Tutte in the 20th century. This theorem is a classical bridge between combinatorial and algebraic quantities. Let us define few important terms before we jump into the theorems and proofs.

Definition 10.2.1. ***Laplacian Matrix for undirected graphs:*** *For any undirected graph $G(V, E)$ with n vertices, let us define a nxn matrix $L(G)$ called the Laplacian matrix of G as follows.*

$$L(G)_{ij} = \begin{cases} deg(v_i) & \text{if } i = j \\ -1 & \text{if } i \neq j \text{ and } (v_i, v_j) \in E \\ 0 & \text{otherwise} \end{cases}$$

It can also be noted that for a graph $G(V, E)$ without any self edges (i.e. $\forall i,\ (v_i, v_i) \notin E$), the Laplacian matrix can also be defined as $L(G) = D - A$ where D is a diagonal matrix with $D_{ii} = deg(v_i)$ and A is the adjacency matrix of G.

Theorem 10.2.2. *Matrix Tree Theorem for undirected graphs by Kirchoff:*
For any undirected graph $G(V, E)$, the number of different spanning trees rooted at v_i contained in G is

given by $det(L_G[i])$ where $L_G[i]$ refers to the matrix obtained by removing the i^{th} row and the i^{th} column from $L(G)$ (for any $i \in [n]$).

Note that the theorem has connected a combinatorial quantity to an algebraic one. It should also be noted that $det(L_G[i])$ is the same for every value of i (since the number of undirected spanning trees does not change with the root v_i). The usual proof of this theorem is done using induction on the number of vertices. Instead we will use PIE to prove the generalised version and this theorem will follow as a consequence. Before doing the proof, let us cover few other concepts required for the proof.

10.3 Determinant of a Matrix

From high school mathematics; we all know that for a 2x2 matrix A and a 3x3 matrix B, the determinants are given by

$$det(A) = a_{11}a_{22} - a_{12}a_{21}$$
$$det(B) = b_{11}b_{22}b_{33} - b_{11}b_{23}b_{32} - b_{12}b_{21}b_{33} + b_{12}b_{23}b_{31} + b_{13}b_{21}b_{32} - b_{13}b_{22}b_{31}$$

It is to be noticed that in the determinant expression of a nxn matrix, the subscripts in each term match with one of the $n!$ possible permutations on $[n]$ and there are $n!$ terms in the expression. For example; the first term in the expression for $|A|$ represents the permutation $[1 \to 1;\ 2 \to 2]$ and the other term represents $[1 \to 2;\ 2 \to 1]$. Similarly, the second term in the expression for $|B|$ represents $[1 \to 1;\ 2 \to 3;\ 3 \to 2]$ while the fifth term represents $[1 \to 3;\ 2 \to 1;\ 3 \to 2]$.
Thus, each term in determinant expression of a nxn matrix represents one of the permutations of $[n]$ and all the permutations are represented exactly once. In other words, given a permutation σ on $[n]$, the term $\prod_{i=1}^{n} a_{i\sigma(i)}$ appears exactly once in the expression of the determinant of a nxn matrix A.
Given any permutation σ on $[n]$, we can represent it in the point representation as a n-tuple as $(\sigma(1), \sigma(2), \sigma(3) \ldots \sigma(n))$. We can define the number of inversions of σ ($Inv(\sigma)$) as follows.

$$Inv(\sigma) = |\{(i,j) \mid i < j \text{ and } \sigma(i) > \sigma(j)\}|$$

For example; for the permutation $\sigma_1 = (1,3,2)$, $Inv(\sigma_1) = 1$ (since (2,3) is the only such (i,j) pair); for $\sigma_2 = (3,1,2)$, $Inv(\sigma_2) = 2$ (since (1,2) and (1,3) are the (i,j) pairs) and for $\sigma_3 = (3,2,1)$, $Inv(\sigma_3) = 3$ (since (1,2), (2,3) and (1,3) are the (i,j) pairs).
It can be noticed that the sign of a term representing the permutation σ in the determinant expression is given by

$$Sign(\sigma) = (-1)^{Inv(\sigma)}$$

From the inferences done above, one can logically guess the determinant expression for a nxn matrix A in terms of $Sign(\sigma)$ and $\prod_{i=1}^{n} a_{i\sigma(i)}$. However, until proven mathematically, this remains

nothing more than a logical guess. So, let us state this as a theorem and prove it.

Theorem 10.3.1. *For any $n \in \mathbb{N}$, the determinant of the n^{th} order square matrix A is given by*

$$det(A) = \sum_{\sigma \in S_n} Sign(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$$

where S_n is the set of all permutations on $[n]$.

Proof. We know that the determinant of any matrix A follows the following four properties.

1. If all the elements in a row of A are 0, then $det(A) = 0$
2. If two rows of A are identical, then $det(A) = 0$
3. If a row of A is a multiple of another row, then $det(A) = 0$
4. Adding the multiple of a row of A to another row, does not change the value of $det(A)$

Though not done as part of the lecture, it can be proven that there is only one expression in terms of a_{ij}'s that satisfies all the four properties. Therefore, it is sufficient to prove that the expression given in the theorem satisfies all the four properties stated above to prove the whole theorem.
Let us now prove the first property : Let all the elements in row k be 0 i.e. $\forall_{j \in [n]}\ a_{kj} = 0$. It can clearly be seen that each term in the determinant expression stated in the theorem has some $a_{k\sigma(k)}$ in it. So each term will be 0 and hence $det(A) = 0$.
Proving that the expression stated in the theorem satisfies the other three properties is left as an exercise for the students. □

10.4 Applications of PIE

10.4.1 Tutte's Matrix Tree Theorem

Now, let us continue our journey towards stating and proving Tutte's Matrix Tree Theorem. Firstly, let us define Spanning Arborescences - the directed graphs equivalent for spanning trees and Laplacian matrix for directed graphs.

Definition 10.4.1. ***Spanning Arborescences:*** *An Arborescence is a directed graph in which a vertex u is called the root and for every other vertex v in the graph, there is exactly one directed path from u to v. In simpler terms, an arborescence is an directed tree in which all the edges are directed away from the root. A Spanning Arborescence $S(V, E)$ of a directed graph $G(V', E')$ is an arborescence such that $V = V'$ and $E \subseteq E'$.*

Definition 10.4.2. ***Laplacian matrix for directed graphs:*** *For any directed graph $G(V, E)$ with n vertices, let us define a nxn matrix $L(G)$ called the Laplacian matrix of G as follows.*

$$L(G)_{ij} = \begin{cases} indeg(v_i) & \text{if } i = j \\ -1 & \text{if } i \neq j \text{ and } (v_i, v_j) \in E \\ 0 & \text{otherwise} \end{cases}$$

Theorem 10.4.3. *Tutte's Matrix Tree Theorem for directed graphs*
For any directed graph $G(V, E)$, the number of different spanning arborescences rooted at v_i contained in G is given by $det(L_G[i])$ where $L_G[i]$ refers to the matrix obtained by removing the i^{th} row and the i^{th} column from $L(G)$ (for any $i \in [n]$).

Note that since spanning arborescences are directed, the number of spanning arborecences depend on the chosen root. Hence, unlike the undirected case, $det(L_G[i])$ here depends on the value of i. Without loss of generality, we can choose $i = n$ for our proof. Therefore, all we should prove is the number of spanning arborescences rooted at v_n for the directed graph G is given by

$$det(L_G[n]) = \sum_{\sigma \in S_{n-1}} Sign(\sigma) \prod_{i=1}^{n-1} l_{i\sigma(i)} \tag{10.38}$$

The R.H.S. of the equation is the determinant expression for the $(n-1)$x$(n-1)$ matrix $(L_G[n])$. Now let us define another type of directed graphs called Spregs to help with our proof process.

Definition 10.4.4. ***Spregs:*** *Single prdecessor graphs or Spregs with distinguished vertex v of a directed graph $G(V, E)$ is a subgraph $T(V, E')$, $E' \subseteq E$, such that each vertex in T except the vertex v has exactly one predecessor and the vertex v has no predecessors. In other words; in the spreg T, $indeg(v) = 0$ and for every $u \neq v$, $indeg(u) = 1$.*

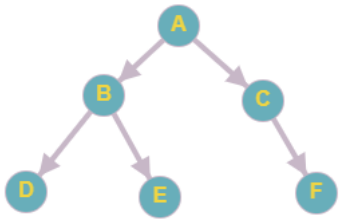


Figure 10.13: Both spreg and arborescence

It is important to distinguish between spregs and spanning arborescences : spregs may contain

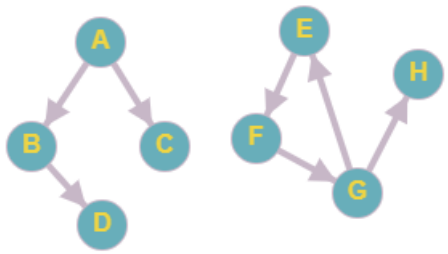


Figure 10.14: Spreg but not arborescence

disconnected components and cycles in them. On the other hand, spanning arborescences are directed spanning trees and hence are single connected components and do not have cycles in them. The directed graph in figure 10.13 is a spreg with distinguished vertex A and an arborescence rooted at A. On the other hand, the graph in figure 10.14 is a spreg with distinguished vertex A but not an arborescence. Now let us consider the following lemma and prove it.

Lemma 10.4.5. *If $T(V, E)$ is a spanning arborescence rooted at v, then T is a spreg with distinguished vertex v.*

Proof. Let $T(V, E)$ is a spanning arborescence rooted at v. We know from the definition that for every other vertex u in T, there is a unique directed path from v to u. The underlying undirected graph of T is a tree and does not have any cycles and hence there should not be any cycles (directed/undirected) in T.
Let us now assume that $indeg(v) \neq 0$. This means that there exists a vertex u in T such that the edge $e = (u, v) \in E$. We know that there is a unique path in T from v to u - let that path be P. Now the path $P + e$ is a directed cycle in T. A contradiction. Therefore, $indeg(v) = 0$.
Let us now assume that for some $u \neq v$ in T, $indeg(u) = 0$. This implies that T is not a spanning arborescence. A contradiction. Therefore, $indeg(u) > 0$.
Let us now assume that for some $u \neq v$ in T, $indeg(u) \geq 2$. This implies $\exists u_1 \neq u_2$ such that $e_1 = (u_1, u) \in E$ and $e_2 = (u_2, u) \in E$. We know that there exists a unique path P_1 from v to u_1 and another path P_2 from v to u_2. Since $u_1 \neq u_2$, $P_1 \neq P_2$. Now, $P_1 + e_1$ and $P_2 + e_2$ are two distinct paths from v to u. A contradiction. Therefore, $indeg(u) = 1$.
Therefore, $indeg(v) = 0$ and for every other vertex u, $indeg(u) = 1$. In other words, T is a spreg with distinguished vertex v. □

It is important to note that the converse of the above stated lemma is not true because spregs may contain discconnected components and cycles in them. Now, we will look at another lemma.

Lemma 10.4.6. *If $T(V, E)$ is a spreg with distinguished vertex v, then the spreg consists of an arborescence rooted at v and zero or more weakly connected components (the underlying undirected component is connected). Each of these weakly connected components have exactly one directed cycle in them.*

Proof. The proof of this lemma is left as an exercise for the students to complete. □

Thus; (a spreg with distinguished vertex v) = (an arborescence rooted at v) + k (weakly connected components with one directed cycle each); where $k \geq 0$.

For proving Tutte's theorem; the idea to count the number of arborescences rooted at v_n is that we would count the number of spregs with distinguished vertex v_n and then remove the number of spregs that are not arborescences - the terms in such a expression would exactly match with that of the R.H.S. of 10.38.

In the R.H.S. of 10.38, consider the term for σ = identity permutation i.e. $\forall i,\ \sigma(i) = i$. Clearly, $Sign(\sigma) = 1$ since $Inv(\sigma) = 0$. The term would be $+\prod_{i=1}^{n-1} l_{ii}$. This is exactly equal to the total number of spregs with distinguished vertex v_n - the reasoning is as follows.
Since v_n is the distinguished vertex, ignore all the edges whose end vertex is v_n. For every other vertex u, choose exactly one of the edges whose end vertex is u ($\prod_{i=1}^{n-1} indeg(v_i)$ ways). Clearly, such a subgraph is a spreg - by definition of spregs. Therefore, the number of distinct spregs is $\prod_{i=1}^{n-1} indeg(v_i) = \prod_{i=1}^{n-1} l_{ii}$ (by the definition of Laplacian matrix).

We have counted all the spregs; now, spregs with cycles have to be removed from the count. This part of the proof involves PIE and will be done in the next lecture.

Chapter 11

Supplementary Material

11.1 Curiosity Collection

Here we list down all the "out of curious" questions that we discussed (sometimes even not discussed) in the class (and hence in this document).

Curiosity 11.1.1. It is an amusing question to ask, whether there are other objects, which we did not intend to, which also satisfies the axioms that we wrote, by accident. Say for example, we wrote the axioms for graphs, but "strings" also satisfies them. If so, the theorems that we prove for graphs using only those axioms will also be true for strings, automatically !!. Quite interestingly this is true for natural numbers. The mathematical theory of natural numbers is axiomatized by what are called the Peano's axioms. There are numbers that one can define which are different from natural numbers for which any theorem that we prove for natural numbers also are true (because they satisfy the Peano's axioms). Then one might ask, are we not trying to represent exactly natural numbers? So should we not augment Peano's axioms with more properties of natural numbers such that we remove such *unwanted* parallel models from satisfying the axioms we write. Even more interestingly, one can argue that this is not even possible. No matter, what extra formula we write the existence of such "parallel models" us inevitable. In fact, not just one "parallel model", there will be infintiely many of them. You should read about *Löwenheim–Skolem theorem*.

Curiosity 11.1.2. The formal proof of PHP as simple as it sounds is still a subject of substantial research in an area called *proof complexity*. To demonstrate this, let us write the principle itself in more rigorous notations. Let $n > k$, and $\{x_{ij} \mid i \in [n], j \in [k]\}$ be propositional variables (which can be called, say *pigeon hole variables*). Following our original notation, where there are n pigeons and k holes, the basic Pigeon Hole Principle is the following Disjunctive normal form formula :

$$\text{PHP}_k^n \stackrel{\text{def}}{=} \left(\bigvee_{i \in [n]} \bigwedge_{j \in [k]} \overline{x_{ij}} \right) \vee \left(\bigvee_{j \in [k]} \bigvee_{r \neq s \in [n]} (x_{rj} \wedge x_{sj}) \right)$$

To prove this, one possibility is to derive the contradiction from the negation of PHP_k^n. This is an expression in conjunctive normal form, with clauses:

$$\text{For } i \in [n] \text{ the clauses : } Q_i \stackrel{\text{def}}{=} \bigvee_{j=1}^{k} x_{ij}$$

$$\text{and for } s \neq t \in [n], j \in [k] \text{ the clauses } Q_{s,t,j} \stackrel{\text{def}}{=} \overline{x_{sj}} \vee \overline{x_{tj}}$$

Intuitively, these say that there is a function from $[n] \to [k]$ (which is represented by $x_{ij} = 1$ to mean that the function takes i to j) which is well defined (for every i, there exists a j such that $x_{ij} = 1$) and also injective (for two different s and t, it is not the case that x_{si} is 1 and x_{tj}). Since $n > k$, there cannot be an injection, and hence the negation of the conjunction of these clauses PHP_k^n must be true.

Suppose we ask, starting from these clauses as axioms, and applying rules of inferences (say the resolution principle) alone, how many steps of proof does one need to do to derive the contradiction ($r \wedge \neg r$ for some r). [1]. We measure this in terms of n and k which determines the number of variables in the system. The area which studies the complexity of proofs in the above is called *proof complexity theory*. It turns out the the basic PHP itself is one of the tautologies for which one requires exponentially long proofs if we are restricting ourselves to resolution? What if we relax this? The area has several interesting open questions related to this and they have close connections to computational complexity theory too.

Curiosity 11.1.3 (Tightness of Dirichlet's Approximation Principle - Roth's Theorem). Let α be any algebraic number (which can be expressed as the root of a polynomial with coefficients from $\mathbb{Q}$. For every ϵ the inequality,

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}$$

can hold true only for finitely many co-prime pairs (p, q). This says that the Dirichlet's approximation principle cannot be improved (for infinitely many p and q) with a larger order denominator.

Curiosity 11.1.4 (Hurwitz Theorem and Irrationality Measures). This is an improvement of the above principle. For every irrational number α, there are infinitely many relatively prime integers p and q such that:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{\sqrt{5}q^2}$$

The $\sqrt{5}$ in the denominator is the best possible. If we let it greater than $\sqrt{5}$, then there is a counter example - consider the irrational number $\frac{1+\sqrt{5}}{2}$ (the golden ratio). It can be shown that this can have only finitely many relatively prime integers p and q with the above formula holding (this is done through arguments about continued fraction representations). For example, if we avoid *golden ratio* and some similar irrational numbers, then we can improve the denominator to $\sqrt{8}$. If

[1] Notice that this sounds exactly like computation, how many steps of computation is required in order to certain tasks in terms of input parameters

we avoid *silver ratio* $(1+\sqrt{2})$ and associated irrational numbers, then we can improve this to $\frac{\sqrt{221}}{5}$. In general, the bound is of the form:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{L_n q^2}$$

where L_n (called the *Lagrange numbers*) steadily increases if some bad irrational numbers are included. These also are viewed as measures of "how much irrational the number is".

11.2 Exercises

Exercise 11.3. Is the above theorem tight? Indeed, one can construct 5 people going to a party and associate a friends/stranger relation among them such that there does not exist three people who are friends with each other and there does not exist three people who are strangers with each other. The exercise is to explicitly write down this counter example relation.

Exercise 11.4. Prove the following identities using double counting method:

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1} \qquad \binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i}\binom{n}{k-i} \qquad \binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$$

11.5 Problem Sets

11.5.1 Problem Set #1

(1) (See Exercise 1) A social network is said to be symmetric if the relation between users that is maintained as a part of the network, is symmetric. Consider a symmetric social network and let the symmetric relation maintained be that of "user A and B are *friends*" (like in the case of facebook). A user C is said to be a *mutual friend* of users A and B if, C is a friend of both A and B. Prove that - for any user A of the network who has at least two friends, there must exist two friends of A who has the same number of mutual friends with A.

Comment on whether symmetry is critical for your argument. Take the example of *instagram* where the symmetric relation of *friends* is replaced by *followers*. Generalize the definition of mutual friends to *mutual followers*. Comment on whether a similar statement for followers can be established in this case.

(2) (See Exercise 2) The set M consists of nine positive integers, none of which has a prime divisor larger than six. Prove that M has two elements whose product is the square of an integer. Is the bound 9 in the above statement tight?

(3) (See Exercise 3) Let $\alpha_1, \alpha_2, \ldots \alpha_k$ be k rational numbers. Generalizing the Dirichlet's approximation principle argument that we did in class, using PHP again, prove that there must exist integers $p_1, p_2, \ldots p_k$ and q such that:

$$\forall i, \ \left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{k}}}$$

(4) (See Exercise 4) Use a double counting argument to establish the following identity :

$$\sum_{m=k}^{n-k} \binom{m}{k}\binom{n-m}{k} = \binom{n+1}{2k+1} \quad \text{where} \quad 0 \leq k \leq \frac{n}{2}$$

Generalize the idea to prove :

$$\sum_{j=r}^{n+r-k} \binom{j-1}{r-1}\binom{n-j}{k-r} = \binom{n}{k} \quad \text{where} \quad 1 \leq r \leq k$$