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 : November 30, 2020

Preface

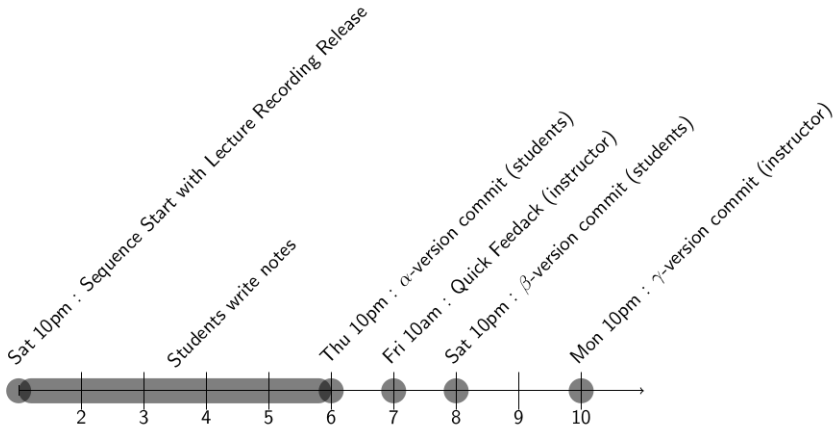
This lecture notes are produced as a part of the course CS5130: Mathematical Tools for Theoretical Computer Science which was a course offered (during the online semester Sep-Dec 2020) at the CSE Department of IIT Madras.

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 : γ

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 : γ

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 : γ

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 : γ

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.

4.1.1 Discussion Session - Counting Cyclic Triplets

We considered the following counting question in the discussion session to demonstrate that simple bijection and the idea of associating combinatorial objects is a very powerful combinatorial technique.

Problem 4.1.3. *Imagine there are $2n+1$ players in a round-robin tournament. That is, each player plays against every other player. Assume that there are no ties in any match. We say that players $\{a, b, c\}$ forms a cyclic triplet if a beats b, b beats c, and c beats a (note that the order does not matter). We want to count the maximum number of cyclic triplets that is possible in the tournament.*

Proof. It is natural to model the above using graphs where each vertex is a player and two vertices (i, j) is a directed edge if the player i beats player j. This gives a directed graph with $2n+1$ vertices whose underlying undirected graph is a complete graph on $2n+1$ vertices. It is also called a tournament. Cyclic triplets can naturally be associated with triangles in these directed graphs. So the statement we are address is also equivalently stated as *in any tournament on $2n+1$ vertices, what is the number of triangles?*.

The idea is to look at associated objects called "corners" of the triangles. There are $\binom{2n+1}{3}$ triangles, and hence there are $3\binom{2n+1}{3}$ many corners. The corners can be classified into three types.

Type 1: A corner where both edges are incoming edges.

Type 2: A corner where both edges are outgoing edges.

Type 3: A corner where one edge is incoming and the other is outgoing.

What happens in a cyclic triplet? It forms a triangle, hence the three corners has to be of Type 3. A non-cyclic triplet will have one corner of each Type. This also establishes a bijection between the Type 1 and Type 2 corners as follows.

$$\psi : \left\{ \begin{array}{c} \text{Type 1} \\ \text{Corners} \end{array} \right\} \to \left\{ \begin{array}{c} \text{Type 2} \\ \text{Corners} \end{array} \right\}$$

defined as follows: given any corner c of type 1, define $\psi(c)$ as the type 2 corner that appears in the (undirected) triangle that this corner appears in. This is well defined because (1) c cannot appear in a triangle corresponding to the cyclic triplet (2) exactly only type 2 triplet can appear in a triangle corresponding to non-cyclic triplet. This uniquely assigns a type 2 corner with c and makes the function, well-defined, injective and surjective (since the process can be reversed too). In fact, the same bijection also proves that the number of non-cyclic triplets is exactly the number of Type 1 corners and also exactly equalt to the number of Type 2 corners. Hence it sufficient to count the number of Type 1 corners.

So now the strategy is clearer. To obtain an upper bound on the number of cyclic triplets, we express it $\binom{2n+1}{3}$ minus the number of non-cyclic triplets. The it suffices to obtain a lower bound for the number of non-cyclic triplets. Hence it suffices to obtain a lower bound on the number of type 1 corners (or equivalently the number of type 2) corners.

One natural attempt is to aim to count type 1 corners alone. If d_i is the in-degree of the i-th vertex, then the number of type 1 corners can be estimated as :

$$t_1 = \sum_{i=1}^{2n+1} \binom{d_i}{3}$$

However, it is unclear how to get a reasonably tight lower bound for this quantity. Instead, the trick is to count the type 1 and type 2 simultaneously as :

$$t = t_1 + t_2 = \sum_{i=1}^{2n+1} \left[\binom{d_i}{2} + \binom{2n - d_i}{2} \right]$$

Since we know that $t_1 = t_2 = t$, we have the number of non-cyclic triplets is:

$$\frac{1}{2} \sum_{i=1}^{2n+1} \left[\binom{d_i}{2} + \binom{2n - d_i}{2} \right]$$

Since we need a lower bound for this, we can use the fact that the summation is minimised when d_i is equal in both the terms in the multiplication. Hence number of non-cyclic triplets is at least:

$$\begin{aligned} \frac{1}{2} \sum_{i=1}^{2n+1} \left[\binom{n}{2} + \binom{n}{2} \right] &\geq \frac{n(n-1)(2n+1)}{2} \\ \text{\# of Cyclic Triplets} &\leq \binom{2n+1}{3} - \frac{n(n-1)(2n+1)}{2} \\ &\leq \frac{n(n+1)(2n+1)}{6} \end{aligned}$$

A natural question is whether this is tight? Or did we have any slackness in the counting? The count will be tight if the $d_i = n$ can be achieved for all vertices. This can be done by the following explicit graph for which the number of cyclic triplets will be hence exactly equal to $\frac{n(n+1)(2n+1)}{6}$ and shows that the above bound is tight.

The construction is as follows. Consider the sequence $1, 2, \ldots, 2n+1$. Define $(i, j) \in E$ if $i - j \mod 2n+1$ is in $[n]$. This ensures that the in-degree and the out-degree of all the vertices is exactly n and hence the graph will achieve the above bound. □

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 $\{1, 2, \dots n\}$. 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 :

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

Generalize the idea to prove :

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

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

Lecture
5

Multichoosing

Recall the definition of a set as 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 $\binom{n}{k}$. As a generalization of this - a *multi-set* allows repetition of objects. The size of a multi-set is the number of elements (counting multiple occurrences separately) in the set. Given that, here is a natural combinatorial question : *from a collection of n distinct symbols, what is the number of ways to form a* multi-set *of size k.* This is also called *multichoosing*. 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).

5.1 Multichoosing via Equivalent Counting Problems

We first state several, seemingly different, yet, to-be-proved-to-be equivalent counting problems.

Problem 5.1.1 (Non-negative Integral Solutions). *Let $n, k \geq 0$ be natural numbers. How many non-negative integral solutions exist for the equation:*

$$x_1 + x_2 + \ldots + x_n = k$$

We can relate this to the multi-choosing problem straightaway. 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.

The Bijection: Consider any outcome of the multichoosing - that is a multi-set S of k objects from the set of n objects where order is not important and objects may repeat. For all $i = 1, 2, \cdots, n$, if we denote by x_i the number of times i^{th} object we chose (or equivalently, is the multiplicity of the i-th object in the multiset S), then we have the equation

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

where each $x_i \geq 0$. Since the multiplicity of different objects in S uniquely characterizes the multi-set S by definition, conversely, any non-negative integral solution to the equation of the above form, uniquely defines a multi-set associated with it. Hence, it follows that this function is a bijection.

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. We look at an equivalent problem and establish a bijection between these two.

Problem 5.1.2 (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?*

Again, we immediately relate it to multi-choosing. But this time we do it by the non-negative integral solution problem. 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. 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 $i = 1, 2, \cdots, n$. The function 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 $\mathbf{x}_{1_i} \neq \mathbf{x}_{2_i}$ 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.

Problem 5.1.3 (Non-decreasing subsequences). *A non-decreasing sequence is a sequence of the form $\{a_1, a_2, \cdots, a_k\}$ where $1 \leq a_1 \leq a_2 \cdots \leq a_k \leq n$. How many non-decreasing sequences of integers of length k can be formed using numbers between 1 and n?.*

Let us quickly 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. 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. 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.

Problem 5.1.4 (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.*

Let us 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. 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.

5.2 Algebraic expression for Multi-choosing - Three Methods

In the previous section, 5.1, we have established bijections between *non-negatives integral* solutions of Equation 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 Equation 5.5. In this section, we are interested in coming up with a concrete algebraic expression for $\left(\binom{n}{k}\right)$ by solving the corresponding problems. Naturally, there are different methods to do this based on the counting problem that we try to use. We give them as the three different methods below.

Method 1 : via the Stars-and-Bars Problem: We solve the *stars and bars* problem defined in Problem 5.1.4. We will 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 : Non-decreasing Subsequences : We solve the *Non-decreasing subsequences* problem defined in Problem 5.1.1. We 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 $i = 1, 2, \cdots, k-1$, $a_i \leq a_{i+1}$. This gives, $a_i + i \leq a_{i+1} + i$. Hence, $a_i + i - 1 < a_{i+1} + i$ and hence the resulting b_is satisfy, $b_i < b_{i+1}$. 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 We solve the *Voting* problem defined in Problem 5.1.2. We first ask a slightly modified question and use the method of double counting.

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, we 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. 5.1.2, the number of ways of distributing $m - n$ votes among n candidates is $\left(\binom{n}{m-n}\right)$

Answer 2: We 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

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

5.3 Identities for Multichoosing

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. We use the bijection method to prove this. Formally, we 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 Problem 5.1.4. 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 Problem 5.1.4. Again, by the bijection defined in it, $|S_2| = \left(\binom{k+1}{n-1}\right)$

Bijection: We 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:

$$\textbf{Identity 2:} \qquad k\left(\binom{n}{k}\right) = n\left(\binom{n+1}{k-1}\right)$$

Proof. We 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. 5.1.3 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

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

This completes the proof □

Exercise 5.4. 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

Exercise 5.5. 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.

Exercise 5.6. 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 : γ

Lecture
6

Catalan Numbers and Bijections

One of the classic examples to demonstrate the power of bijections is *Catalan numbers*. The Catalan 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. Catalan numbers got their name from *Eugene Catalan* 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 Catalan numbers.

6.1 Four Counting Problems

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,

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

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. It is non-trivial to see that this is equal to Catalan number. We discuss this in the discussion session later. See Section 6.4.

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.

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

6.2 Algebraic Expression

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

6.2.1 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 $n + n = 2n$.

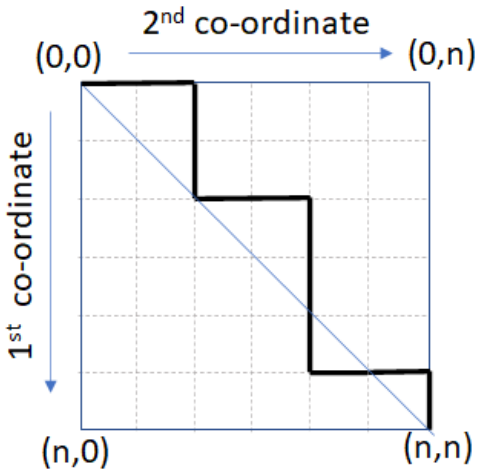


Figure 6.1: A path from $(0, 0)$ to (n, n) using downward and right edges

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 $b = b_1 b_2 \cdots b_{2n}$ 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.

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 $\binom{2n}{n+1} = \binom{2n}{n-1}$

6.2.2 Diagonal avoiding paths and Catalan 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

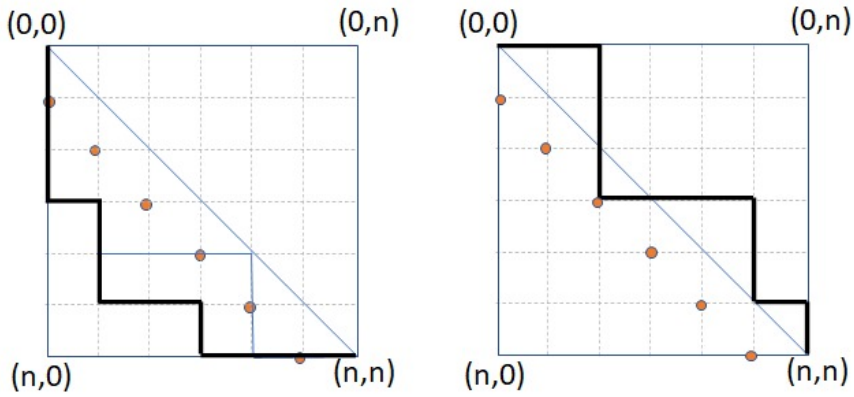


Figure 6.2: Diagonal crossing paths. Note that path in (a) is crossing the diagonal at $(0, 0)$

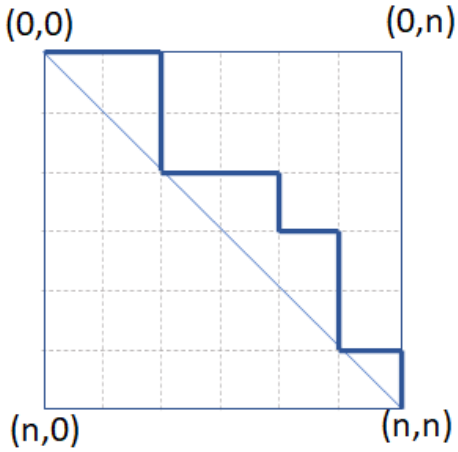


Figure 6.3: A diagonal avoiding path. Observe that it can still touch the diagonal

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.

6.2.3 Bijection from Diagonal avoiding paths to Balanced parenthesisation problem

Intuitively, the bijection can be defined as follows: for any given balanced parenthesized string $w = w_1 w_2 \dots w_{2n}$, 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.

6.2.4 Counting the number of diagonal avoiding paths

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

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

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 diag-

onal 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.

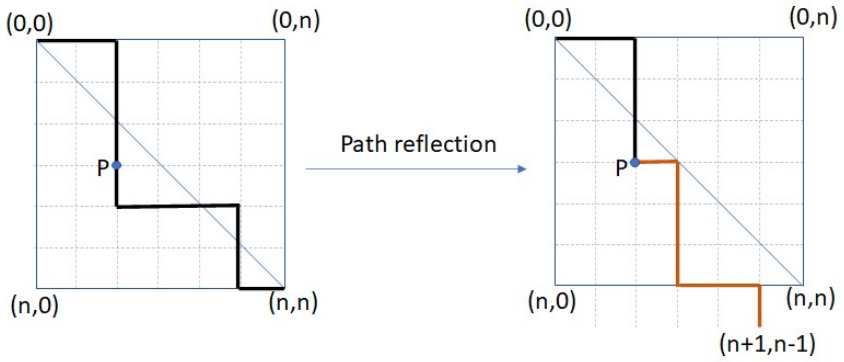


Figure 6.4: Point P in a diagonal crossing path and the reflected path after P

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

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

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 $\pi' = S'_1S'_2$, 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 $\pi = S'_1S_2$ 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. $\forall j \le i$, $(u_j,v_j) = (u'_j,v'_j)$

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 6.3.

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.

6.4 Catalan Bijections

6.4.1 Bijection from Triangulations 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, we 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.

We 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. 6.5). 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. We associate each of the triangles with a vertex (green dots in the fig. 6.5). 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, we 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

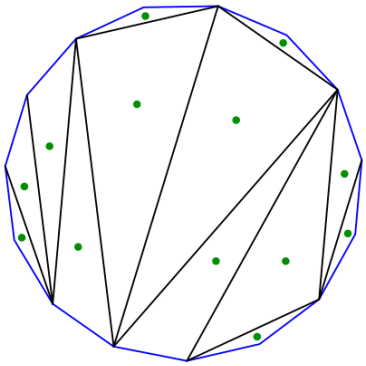


Figure 6.5: Partitioning a polygon into triangles by non-crossing diagonals. Observe that green dots in each triangle associates the triangle with a vertex

surrounding a vertex (other than e), add an open-edge originating from that vertex (see fig. 6.6). We arrive at the following claim.

Claim 6.4.1. *If we remove the underlying triangles (which are formed with polygon edges and diagonals), from fig. 6.6, the resulting graph obtained (see fig. 6.7) 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

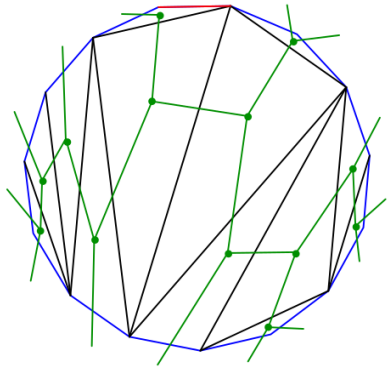


Figure 6.6: Polygon with vertices connected to form a tree

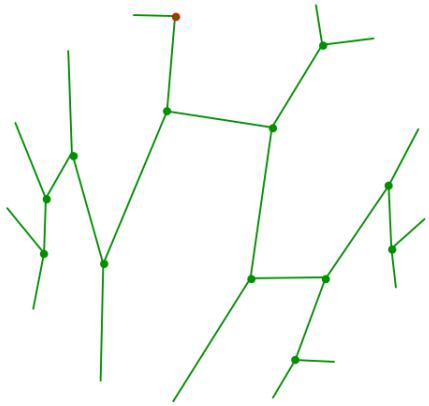


Figure 6.7: Tree formed by connecting vertices

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.

6.4.2 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 we 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: (flawed) 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 6.8

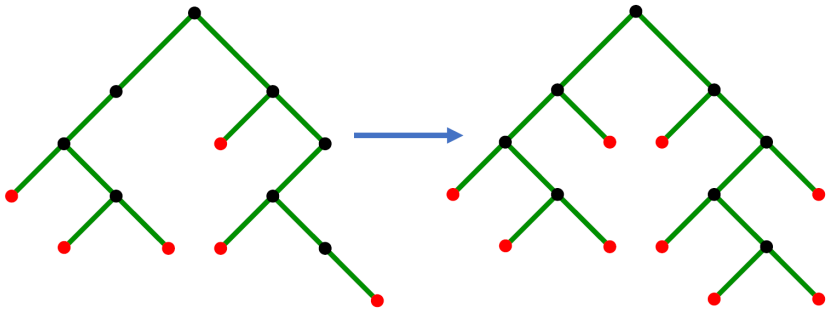


Figure 6.8: Binary to full binary tree attempt1: adding a child node to each non full node

But notice that this transformation is not injective. For example, it can be observed that both the trees in figure 6.9 map to same full binary tree.

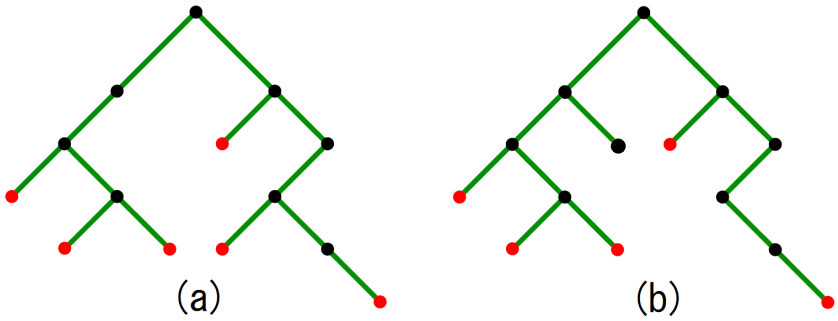


Figure 6.9: Two different binary trees that map to same full binary tree

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

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

Figure 6.10 shows the full binary tree constructed in this way for the same binary tree as in Figure 6.8. We can see that this solution addresses the issue in the first attempt. Intuitively because of 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

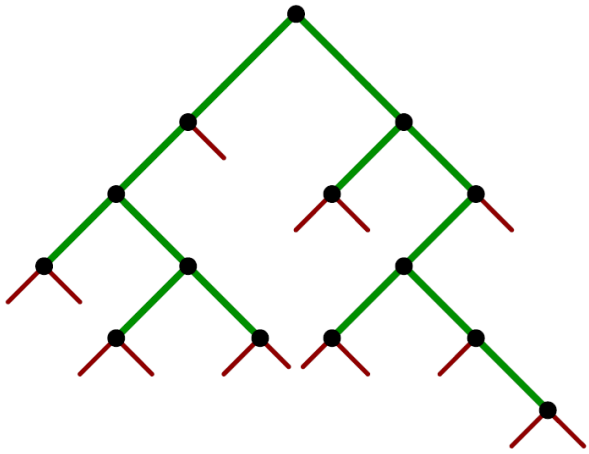


Figure 6.10: Full binary tree for the (non-full) binary tree given in fig 6.8. Notice that all the leaf nodes are added during transformation

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.

6.4.3 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 6.11 shows a plane 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,

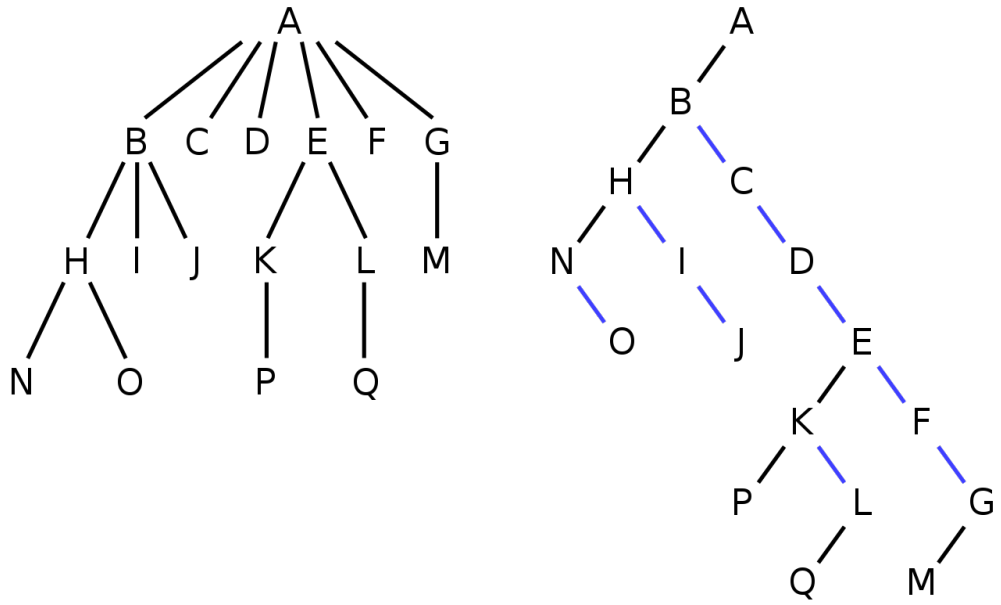


Figure 6.11: An example of plane trees and its transformation to a binary tree

- 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 : Anshu Yadav (*TA:* JS)
Date : Sept 19, 2020
Status : γ

Lecture 7

From Bijections to PIE

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.

7.1 Two Useful Binomial Identities and Proof by Bijections

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

7.1.1 Signed Binomial Sum : 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. □

7.1.2 Lower-cut Sum : Proof for Eqn. (7.10)

The equation we set out to prove is:

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

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

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

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.

Case 1: 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, $|E \setminus E'| = \binom{n-1}{m}$.

Case 2: 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 7.1.1, 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.

7.2 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 $|A| = |A_1| + |A_2| + \ldots + |A_n| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|$. 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,

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

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 ∎

7.2.1 Using the Lower-cut Sum : Bonferroni Inequality

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.

Case 1: $k \leq m$**:** 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,

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

Case 2: $k > m$**:** 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 7.2.1. *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.

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

Lecture
8

PIE and three applications

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.

8.1 Principle of Inclusion Exclusion (PIE) - An Algebraic Proof

If there are n subsets of a ground set X; A_1, A_2, $A_3, \ldots A_n \subseteq X$, 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,

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

where $[n] = \{1, 2, 3, \ldots, n\}$ (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 $1, 2, 3, \ldots, n$ 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., $|A_i|, |A_i \cap A_j|, |A_i \cap A_j \cap A_j| \ldots$ is captured in $\bigcap_{i\in I} A_i$ of the second equation.

Proof. Define the characterestic function of the set A_i as f_i described as : $f_i : X \longrightarrow \{0, 1\}$, where the images are defined as

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

By definition, $(1 - f_i(x))$ 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,

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

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,

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

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),

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

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, $\left|\bigcap_{i\in I} A_i\right|$. Also, note that the convention when $I = \emptyset$ is, $\left|\bigcap_{i\in I} A_i\right| = |X|$. which can be reasoned as when I is empty, $\left(\prod_{i\in I} f_i(x)\right)$ is 1 for any x. And its summation over x, $\sum_x \left(\prod_{i\in I} f_i(x)\right)$ gives $|X|$.

By (8.18) and (8.19),

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

This completes the algebraic proof for PIE. □

8.2 Applications of PIE

We now see three different applications of PIE which exposes some interesting features of the tool.

8.2.1 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 randomly.

Question: What is the chance that nobody got their own hat for a very large n?
Answer (surprisingly high): roughly 36% ! (more precisely, the probability is $1/e = 0.3678$).

Formally, if we view the rearrangement as a permutation on n elements, the property that we are looking for can be expressed mathematically as follows : A permutation $\sigma \in S_n$ is said to be a derangement if $\forall i \in [n], \sigma(i) \neq i$. Now we prove the following theorem.

Theorem 8.2.1. *Number of derangements on n elements is*

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

Before we proceed, let us demonstrate why this implies our surprising answer. 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 $\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right)$. As $n \to \infty$, $\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right) \to 1/e \sim 0.3678$.). We now proceed with the proof of the above theorem, which is a nice application of PIE.

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 - in terms of formal language of permutations, this is called a *fix-point* of the permutation. 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 $\exists i,\ \ \sigma(i) = i$. Now we set up the application of PIE in this context, by defining the A_is first. 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).

The set that we want to estimate the size of - the 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 $|\bigcup_{i=1}^{n} A_i|$.

We want to apply PIE - which is about intersection of these A_i. Can A_i and A_j really intersect? Indeed, they can, and we can even estimate the size of the intersection: indeed, for a permutation to be in the intersection it has to be fixing the element i and j and it has the freedom to choose any permutation for the remaining values. Hence,

$$|A_i \cap A_j| = (n-2)!$$

Now we generalize this estimate to arbitrary size intersections since they appear in the RHS of PIE. For a shorthand notation, define, $A_I = \bigcap_{i \in I} A_i$. Now, from the statement of PIE, we need to

estimate sizes of $|A_I|$ for different $I \subseteq [n]$. Observe that,

$$|A_I| = (n - |I|)! \tag{8.20}$$

Indeed, 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 arbitrary permutation of the same $n - |I|$ values, hence $(n - |I|)!$ gives the number of possibilities.

Using PIE and using the idea of fixing size of I and sum over each size in next step,

$$\begin{aligned}
|\bigcup_{i=1}^{n} A_i| &= \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} |A_I| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{I \subseteq [n], |I|=k} |A_I| \right) \\
&= \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{I \subseteq [n], |I|=k} (n-k)! \right) && \text{(By (8.20))} \\
&= \sum_{k=1}^{n} (-1)^{k+1} (n-k)! \binom{n}{k} \\
&= \sum_{k=1}^{n} (-1)^{k+1} \frac{n!}{k!} \\
&= \left(\sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!} \right) n! && (8.21)
\end{aligned}$$

Now, to get number of derangements, subtract (8.21) from $n!$, which is

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

□

8.2.2 Euler's Φ function.

Theorem 8.2.2. *Let $n \in N$, $\Phi(n)$ = 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

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

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

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

Thus, 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) - is given by exactly the set : $\bigcup_{i=1}^{k} A_i$. Thus we have the ground set for application for PIE. We need to be able to estimate the sizes of the intersections. More precisely:

$$\begin{aligned}\Phi(n) &= n - |\bigcup_{i=1}^{k} A_i| && \text{(apply PIE)}\\ &= n - \sum_{I\subseteq[k], I\neq\emptyset} (-1)^{|I|+1}|A_I| && (8.22)\end{aligned}$$

where To esteimate $|A_I|$. We claim that $|A_I| = |\bigcap_{i\in I} A_i| = \frac{n}{\prod_{i\in I} p_i}$. This 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 Equation 8.22 and using the convention of $\prod_{i\in I} p_i$ is 1 when $I = \emptyset$,

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

Note that the last step is done similar to (8.17) in PIE (section 8.1) derivation : f_i there is equivalent to $\frac{1}{p_i}$ here. This completes the proof for the theorem. □

Corollary 8.2.3. *Φ is multiplicative when numbers are co-primes. i.e., if n_1, n_2 are co-primes, then $\Phi(n_1 n_2) = \Phi(n_1)\Phi(n_2)$.*

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.

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

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

8.2.3 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,

$$|B| = \sum_{I \subseteq Q, I \neq \emptyset} (-1)^{|I|+1} |A_I| \text{ where, } Q = \{p | p \leq n, prime\} \tag{8.23}$$

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

$$|A_I| = |\bigcap_{p_i \in I} A_{p_i}| \tag{8.24}$$

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 (8.24) using the definition of A_d,

$$|A_I| = |A_d| \;\; where, \quad d = \prod_{p_i \in I} p_i \tag{8.25}$$

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,

$$\begin{aligned} |A_d| &= \lfloor \frac{n}{d} \rfloor \lfloor \frac{n}{d} \rfloor \\ &= (\lfloor \frac{n}{d} \rfloor)^2 \end{aligned} \tag{8.26}$$

From (8.23), splitting the summation by number of primes taking part,

$$\begin{aligned} |B| &= \sum_{k \geq 1} (\sum_{I \subseteq Q, I \neq \emptyset, |I| = k} (-1)^{|I|+1} |A_I|) && \text{(Apply (8.25) and (8.26))} \\ &= \sum_{k \geq 1} (\sum_{\substack{d \leq n, \\ d \text{ is a product} \\ \text{of } k \text{ distinct} \\ \text{primes from } Q}} (-1)^{k+1} (\lfloor \frac{n}{d} \rfloor)^2) && (8.27) \end{aligned}$$

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 (8.27),

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

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

$$\begin{aligned} |G| &= n^2 - |B| \\ &= n^2 + \sum_{2 \le d \le n} \mu(d)((\lfloor \frac{n}{d} \rfloor)^2) \\ &= \sum_{1 \le d \le n} \mu(d)((\lfloor \frac{n}{d} \rfloor)^2) \end{aligned} \tag{8.28}$$

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 (8.28),

$$\begin{aligned} |G| &= \sum_{1 \le d \le n} \mu(d)(\frac{n^2}{d^2} + O(\frac{n}{d})) \\ &= n^2 \sum_{1 \le d \le n} \frac{\mu(d)}{d^2} + O(n \sum_{1 \le d \le n} (\frac{\mu(d)}{d})) \end{aligned} \tag{8.29}$$

Estimating the second term in (8.29):

$$\begin{aligned} n \sum_{1 \le d \le n} (\frac{\mu(d)}{d}) &\le n(\sum_{1 \le d \le n} \frac{1}{d}) \\ &\le n \log n \end{aligned} \tag{8.30}$$

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

Estimating the first term in (8.29):
Using Euler's series, the following approximation can be done.

$$M = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \sim \frac{6}{\pi^2} \tag{8.31}$$

It can also be proven that

$$|M - \sum_{1 \leq d \leq n} \frac{\mu(d)}{d^2}| \leq \frac{1}{n} \tag{8.32}$$

Using (8.29), (8.30), (8.31) and (8.32),

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

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

$$|X| = n^m \tag{9.33}$$

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 $I \subseteq [n]$,

$$|A_I| = |\bigcap_{i \in I} A_i| = (n - |I|)^m \tag{9.34}$$

Using PIE to find the number of non-surjections,

$$\begin{aligned}
|\bigcup_{i=1}^{n} A_i| &= \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} |A_I| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{I \subseteq [n], |I|=k} |A_I| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{I \subseteq [n], |I|=k} (n-k)^m && \text{(By 9.34)} \\
&= \sum_{k=1}^{n} (-1)^{k+1} (n-k)^m \binom{n}{k} && (9.35)
\end{aligned}$$

Therefore, the number of surjections is given by

$$\begin{aligned}
|X \setminus \bigcup_{i=1}^{n} A_i| &= |X| - |\bigcup_{i=1}^{n} A_i| \\
&= n^m - \sum_{k=1}^{n} (-1)^{k+1} (n-k)^m \binom{n}{k} && \text{(using 9.33 and 9.35)} \\
&= (-1)^0 (n-0)^m \binom{n}{0} + \sum_{k=1}^{n} (-1)^k (n-k)^m \binom{n}{k} \\
&= \sum_{k=0}^{n} (-1)^k (n-k)^m \binom{n}{k}
\end{aligned}$$

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

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

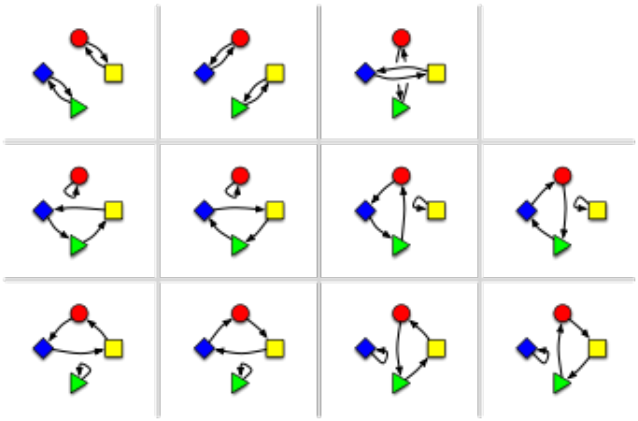


Figure 9.12: Permutations on 4 elements with 2 cycles

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

$$det(L_G[n]) = \sum_{\sigma \in S_{n-1}} Sign(\sigma) \prod_{i=1}^{n-1} l_{i\sigma(i)} \tag{10.36}$$

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 $u \neq v$, $indeg(u) = 1$.*

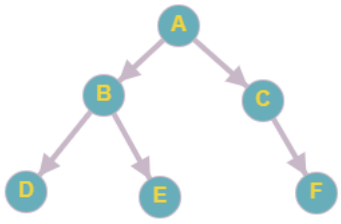


Figure 10.13: Both spreg and arborescence

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

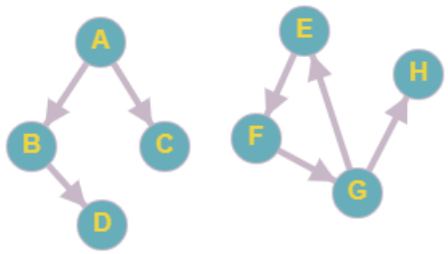


Figure 10.14: Spreg but not arborescence

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 11.37.

In the R.H.S. of 11.37, 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.

Instructor : Jayalal Sarma
Scribe : Shrinidhi Bajpayee (*TA:* JS)
Date : 2 october, 2020
Status : α

Lecture
11

More on PIE, PIE -Tuttes-Matrix-Tree-Theorem-Part2

11.1 Introduction

We finished Tutte's Matrix Tree Theorem in non trivial way.Let's just recall Tutte's Theorem.We have directed graph $G(V, E)$.We have $V = v_1, v_2, ...v_n$.
A $n \times n$ matrix $L(G)$ called the *Laplacian matrix* of G as follows.

$$L(G)_{ij} = \begin{cases} indeg(v_i) & \text{if } i = j \\ -1 & \text{if } i \neq j \text{ and } (v_i, v_j) \in E \\ 0 & \text{otherwise (When there is no edge)} \end{cases}$$

What theorem says,the number of spanning arborescences rooted at some vertex n is given by exactly equal to $det(L_G[i])$ Here i=n.
Quickly Recap Definition of 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 $E \subseteq E'$.
One condition is that there is a directed path from V to every vertex in G within E′.
Second condition is underlying undirected graph should be a tree.

Recall the following from the last lecture.

$$det(L_G[n]) = \sum_{\sigma \in S_{n-1}} Sign(\sigma) \prod_{i=1}^{n-1} L_{i\sigma(i)} \tag{11.37}$$

$S(n-1)$ is notation for permutation of $n-1$. This is expression of determinant that we have seen in last lecture. So we want to show it is equal to spanning arborescence we introduce concept called Spreg.So what is Spreg ?. We quickly define Spreg.

Definition 11.1.1. ***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 $u \neq v$, $indeg(u) = 1$.*

Every vertex other than distinguished vertex must be indegree 1.Subgraph of G is called Spregs.So there are several spregs are possible similar to several spanning arborescence possible.
We want to count spanning arborescence using spregs.That will be very nice combinatorial interpretation of this topic,that is plan.

2.We want to count the number of spregs distinguished vertex Vn.
We associated with last lecture that every spanning arborescence corresponds to spregs .It turns out there are more spregs.There is some structure,Spregs looks like are of the form arborescence + weekly connected component 1 + weekly connected component 2.....
V can not be part of cycle.V can be vertex in component.Weekly connecetd component has exactly 1 cycle.
So what we want to count spregs in inner circle with distinguished vertex Vn.Ok so already know what we have to count.Basic strategy is as follows:
Strategy is that count the number of spregs with distinguished vertex Vn which does not have any cycle.So this is what we want to count.We want to use Inclusion Exclusion.In fact we will not only count through Inclusion exclusion but we will go through each term of the determinant expression corresponds to our counting terms.
Let's demonstrate by writing down Inclusion exclusion.
In order to define Inclusion Exclusion formulation we need to define the

1.Universe (Called as X).
2.Component A_i.
To define that Let's consider,notice that we want to count spregs without any cycle.
We need to be set of all spregs with distinguished vertex V_n.
Let $C_1, C_2, C_3, \ldots, C_n$ be the set of cycles in graph G.We looking at simple cycle.
A_i define as spregs which contain the cycle C_1.The number of spregs which does not contain any cycle.This what we want to count.So,

$|X| - |\bigcup_{i=1}^{n} A_i|$ It is same as,

$$|X| - \sum_{I \subseteq [n], I \neq \emptyset} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|$$

So already applied Inclusion Exclusion,Now write it as

$$|X| + \sum_{I \subseteq [n], I \neq \emptyset} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|$$

So basically we need to count this.We can say that each term in these expression are exactly same as term used in determinant expression.As number of Spregs are equal to number of spanning arborescence,hence theorem is called.This is strategy.Hence each term is associated with terms of determinant theorem.

Observation: Let's consider C1,C2 be two cycles.

What can say about

$$A1 \bigcap A2 = \emptyset iff C1 \bigcap C2 \neq \emptyset.$$

Every spregs looks like arborescence + uniquely weekly connected component 1 +uniquely weekly connected component 2.

$$If C1 \bigcap C2 \neq \emptyset then |A1 \bigcap A2| = 0.$$

Using the observation,

The number of spregs with distinguished vertex Vn which is acyclic is nothing but

$$|X| + \sum_{I \subseteq [n], I \neq \emptyset, for J,K \in I, J \neq K, cj \bigcap ck = \emptyset} (-1)^{|I|+1} |\bigcap_{i \in I} A_i|$$

Recall: We counted —X— =Total number of spregs

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

This is determinant expression. term corresponds to

$$\sigma = id$$

$$\prod_{i=1}^{n-1} (L_i) = \prod_{i=1}^{n-1} deg_i n(L_i)$$

Now we count the singleton sized I. Spregs that contain exactly one cycle. Fix,I=1,We are counting spregs which contain only C1. Let CI be (Vi1,Vi2,Vi3,....Vin)

$$\sigma(i1) = i2$$

$$\sigma(i2) = i3$$

$$\sigma(ik-1) = ik$$

$$\sigma(ik) = iI$$

$$\sigma \in S_n - 1$$

$$\forall otheri \in 1...n$$

$$\sigma(i) = i$$

This is permutation which contain one cycle. Now we just able to do following
Claim: Term in the determinant expression for

$$LG[n]correspondsto\sigma = numberofspregswhichcontainC1$$

Right now we are talking about one circle. Let's see proof of this. Proof of this is very natural.

$$sign(\sigma)\prod_{i=1}^{n-1} L_i, \sigma(i$$

sign of permutation is exactly equal to $(-1)^{(l-1)}$.Here length is l.

Second term is

$$(-1)^{(l-1)}(\prod_i, |\sigma(i)| = iL_i, i)(\prod_i, |\sigma(i)| \neq iL_i, \sigma(i))$$

$$L_i, \sigma(i) = -1, ifV_i, V_\sigma(i)isedgeingraph \in Eotherwise$$

If corresponding edge is present then this term is non zero otherwise zero.

$$(-1)^{(l-1)}(\prod_i, |\sigma(i)|deg_in(v_i)) * (-1)^l$$

$$= (-1)^{(2l-1)}|numberofspregswhichcontainC1|$$

$$= -|numberofspregswhichcontainC1|$$

Proposition for

$$\sigma \in S_n - 1comsistingofsinglecycle.$$

$$\sigma = (i1, i2, ...il)$$

Associate$C\sigma$ as a cycle corresponds to vertex sequence (Vi1,Vi2,Vi3.....Vil,Vii)
Then the term in the determinant corresponds to σ satisfies following.

$$sgn(\sigma)(\prod_{i=1}^{n-1} L_i, \sigma(i))$$

$$-(\prod_{i,\sigma(i)=i} deg_i n(v_i))C_\sigma \subseteq G(V,E)$$

$$0 if C\sigma \nsubseteq G(V,E)$$

$$-1 if C\sigma \subseteq G(V,E) if \forall i \sigma(i) \neq i$$

Corollary:

$$For \sigma, C\sigma as above$$

$$|\prod_{i=1}^{n-1} L_i, \sigma(i)| = number of spregs which contain C_\sigma$$

Now this is case for single cycle.
Now we will generalise case for multiple cycle.
So it is very natural.

Question: Suppose $\sigma \in S_{n-1}$ is the product of $k > 0$ disjoint cycle.

$$\sigma = (i11, i12, i13.....iil)(i21, i22, i23....(ikl, ik2, ik3...ikl)$$

k is number of cycles. So now we are associate

$$C_\sigma = \cup j = 1^k C_j where C_j is (V_i j1....V_i jLj.....Vij I)$$

Then the term corresponds to σ in $det(L_G[n])$

$$sgn(\sigma) = (-1)^K \prod_{i|\sigma(i)|} deg_i n(V_i) if C_\sigma \subseteq G$$

$$o if C\sigma \nsubseteq G$$

Corollary: If we look at

$$|\prod_{i=1}^{n} L_i, \sigma(i)| = number of spregs which contain C_\sigma = \bigcup_{j=1}^{k} C_j$$

$$det(L_G[n]) = \sum_{\sigma \in S_n - 1} sig(\sigma) \prod_{i=1}^{n} L_i \sigma$$

This is how determinant expression looks like.
Number of spanning arborescence rooted at Vn as distinguished vertex and not containing cycle.
This is strategy. This lecture is combinatorial application of PIE.

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

Lecture
12

Algorithmic Application of PIE

12.1 Introduction

We talk about counting problem.Its about given a $n * n$ bipartite graph,We want to count the number of perfect matching in it?
subset of edges such that every vertex has exactly one edge incident on it from the subset.
Bipartite adjacency matrix is different from adjacency matrix.

Trivial Algorithm: Run through all n sized subsets of E.

$$\binom{n^2}{n} \sim \binom{n^2}{n}^n \sim n^n \sim 2^{nlogn}$$

$$\binom{n}{k}^k \leq \binom{n}{k} \leq \binom{n_e}{k}^k$$

e=natural log base

12.2 Decision Problem:

Binpacking Problem: Given a positive integer (bin capacity B),positive integer k
We have n item with weight S1,S2,S3.....,Sn
partition the items into u1,u2,u3.....,uk
Capacity is such that sum of weights of items in each ui is almost B.
This is binpacking problem.
It is NP-problem.

By PIE Time complexity is $O(nB2^n)$
n=number of items
B=capacity
Now we will reformulate PIE.

Given a collection of N combinatorial objects
Let p(1),p(2),p(3)...p(n) be properties.
p_i is essential function

$$N \to 0, 1$$

It is possible that some object doesn't have properties of that.

$$N_i \to Numberofobjectsamong Nwithproperty P(i).$$

$$i_1, i_2, ...i_r \subseteq 1, 2, 3, ...N$$

$$N_{i_1,i_2,i_3....i_r} = Numberofobjectswithpropertiesp(i_1)p(i_2)....p(i_r)$$

N(0)=Number of objects not having any of the property.

$$N(0) = N - \sum_{i=1}^{n} N_{i_1} + \sum_{i_1<i_2} N_{i_1,i_2} - \sum_{i_1<i_2<i_3} .....(-1)^j \sum_{i_1<i_2<...i_j} N_{i_1,i_2...i_j}(-1)^x N_1...r$$

Restatement (Complementary term)(For the discussion)

$$N \to Numberofobjects.$$

$$Q(1), Q(2), ...Q(n)$$

be properties that some of these objects have.

$$W \subseteq 1, 2, ...n$$

Let N(W) be the number of objects having none of the properties Q(i).

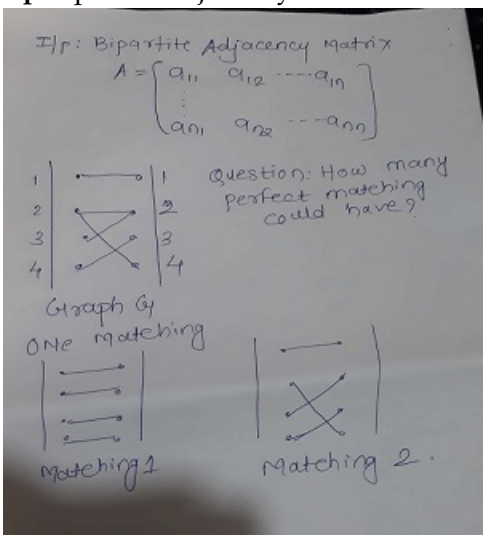
$$i \in W$$

Now what we want to count the other set.

$$X \to number of objects which has all the properties.$$

$$X = \sum_{W \subseteq [n]} (-1)^{|W|} N(W)$$

Pf:$Define P(i) iff \neg Q(i)$
Now the above restatement is applicable.
Given a bipartite graph $G(u, v, E)$
$|u| = |v| = n$
count the number of perfect matching.
I/p: Bipartite adjacency matrix.



There are 2 perfect matching is in these graph.
Matching 1: There is bijection.
There are 4!=24 permutation.But matching 1 and matching 2 are two permutation for perfect matching.
How's the algebric way of writing itself.
Let's write $\sigma \in S_n$
Consider,

$$\prod_{i=1} na_i\sigma(i)$$

When $a_i\sigma_i$ is non zero value. When $i\sigma_i$ is true.

$$\prod a_i i = a11.a22.a33.a44$$

1

What will be product of

$$\prod_{i=1} na_i\sigma(i)$$

$$a12.a21.a33.a44$$

0

If corresponding edge is there in graph then value will be 1 otherwise 0.
a12=0 since no edge from 1 to 2.
Let's write,
Permanant of A=

$$\sum_{\sigma \in S_n} = Numberofperfectmatchinginthegraph.$$

Given a matrix A,
Its two types are:
!)permutataion (A) that is per(A): It is number of perfect matching in graph.
2)Determinant (A) that is det(A)

Problem: Given a matrix A o/p the value of per(A)
Trivial Algorithm: Run over all $\sigma \in S_n$ compute the product

$$\prod_{i=1} na_i\sigma(i)$$

and add.

$$O(n!) \sim O(n^n) \sim 2^{nlogn}$$

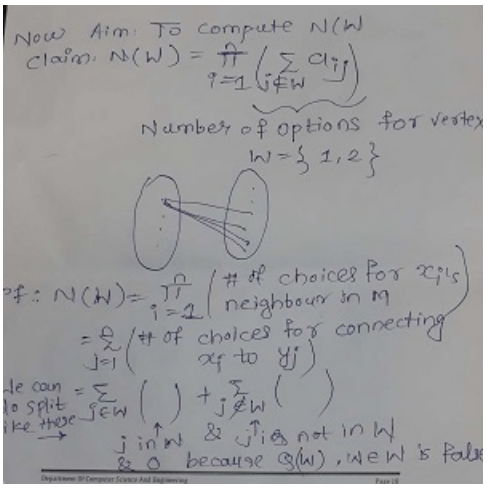
Lemma:A is bipartite adjacency matrix of a bipartite graph G

$$Per(A) = \sum_{W \in 1...n} (-1)^{|W|} \prod_{i=1}^{n} (\sum_{j \notin W} a_i j)$$

Applying Lemma, 2^n W's and $n^2 = remainingComputation$
$2^n n^2$ time algorithm.
PF: To apply complementary form PIE.
Define N objects: $M \in N$
$M \subseteq E$ such that for every
$\forall i \in 1...n$ the vertex X_i is the endpoint of some vertex in M.
$\forall j \in [n]Q(j)$: Vertex Y_j is the endpoint of some vertex in M.
We want to count number of objects from underlined part which satisfies Q(1) .....Q(n)
The number of perfect matching=per(A)=number of objects which satisfies all of Q(1) Q(2)....Q(n)
Q(1) says first one is matched.
Q(2) says second one is matched.
Like this etc etc.
When all vertex are matched from both side.

$$\sum_{W \in 1...n} (-1)^{|W|}$$

N(W)=Number of objects which satisfies none of property in W.



Per(A)=Number of perfect matching.

$$\sum_{W \subseteq 1...n} (-1)^{|W|} (\prod_{i=1}^{n} (\sum_{j \in w} aij))$$

This completes the proof of the Lemma.
This lemma gives $O(2^n n^2)$ algorithm for computing number of perfect matching in a given bipartite graph.

Quickly Recap:
Binpacking problem:
$BincapacityB, WehavenumberofbinsK, WehavenitemsS1....Snaresizes.$ Question is Can we partition items to $u1....uk[n]$ such that We want to count this.
Algorithm:
Trivial Algorithm: Run through partition.

$$\binom{n}{k}$$

$O(nB2^n)$ time space.
A partition of [n] into u1....uk is said to be feasible if the sum of the sizes of item $\leq$ B in uj.
Relax: Items can appear more than once.
observation:A feasible solution with relaxation will remain feasible without relaxation.
Relaxed Solution:ordered set of K lists of items from $1...n$.
1.Each of the elements in $1...n$ appears atleast in one list.
2.For each list $a1, a2....ap$

$$\sum_{h=1} pS_a k \leq B$$

To apply PIE,we need to define objects $Q1$....

Objects: Ordered sets of K list of elements from 1...n such that for each list (a1...ap)

$$\sum_{h=1} pS_a n \leq B$$

Q(1):=The ordered list of k lists contain 1 in atleast one list in it.

.

.

.

Q(W):=W is contained in atleast one of the lists in the ordered set of list.

.

.

.

Q(n)

X=Set of objects which satisfy all of the properties Q(1)....Q(n)

$$X = \sum_{w \subseteq [n]} (-1)^{|w|} N(W)$$

Aim: To compute N(W)

A(W):=Number of list a1....ap of elements list in W.

$$\sum_{h=1} pS(an) \leq B$$

$$N(W) = (A(W))^k$$

Aim: Compute A(W)

$P_w(j)$ =number of list a1....ap of which element not in w such that

$$\sum_{h=1} pS(ak) = j$$

$$A(w) = \sum_{j=0} BP_w(j)$$

$$P_w(j) = \sum_{i \notin w} P_W(j - s(w))$$

$$p_W(j) = 0, j < 0$$

$$P_w(0) = 1$$

Time taken is $O(nB2^n)$

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

Lecture
13

From Principle of Inclusion-Exclusions to Mobius Inversion

The journey so far has been that we have started with pigeon hole principle and its applications then we used double counting and bijections to establish different identities then we moved to PIE and its different applications. In this lecture, we will look at a more generalized version of PIE and move gradually towards the Mobius Inversion.

13.0.1 PIE Revisited

Previously we have used PIE to compute $|\bigcup_{i=n}^{n} A_i|$ as follows,

$$\left|\bigcup_{i=n}^{n} A_i\right| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|$$

Now, we are interested to compute $\left|\bigcap_{i=1}^{n} \overline{A_i}\right|$, which can be rewritten as,

$$\begin{aligned}
\left|\bigcap_{i=1}^{n} \overline{A_i}\right| &= \left|\overline{\bigcup_{i=1}^{n} A_i}\right| && \text{(using De-morgan's law)} \\
&= |X| - \left|\bigcup_{i=n}^{n} A_i\right| \\
&= |X| - \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right| \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \left|\bigcap_{i \in I} A_i\right| && (13.38)
\end{aligned}$$

Note that $\bigcap_{i \in \emptyset} A_i = X$. This thing can also be stated in the following way.

Theorem 13.0.1. *Let X be a finite set and $P_1, \ldots, P_m$ properties. Further define for $S \subseteq [m]$ the set $N(S) = \{x \in X \mid \forall i \in S : x \text{ has property } P_i\}$ then, number of elements in X satisfying none of the properties $P_1, \ldots, P_m$ is given by,*

$$\sum_{S \subseteq [m]} (-1)^{|S|} |N(S)|$$

13.0.2 Stronger version of PIE

The Inclusion-Exclusion Principle has a stronger version which is as follows.

Theorem 13.0.2 (Stronger PIE). *Let $f, g : 2^{[n]} \longrightarrow \mathbb{R}$ are functions assigning real numbers to subsets of $[n]$ with the property that for any $A \subseteq [n]$*

$$g(A) = \sum_{S \subseteq A} f(S)$$

Then,

$$f(A) = \sum_{S \subseteq A} (-1)^{|A|-|S|} g(S)$$

Proof. Let f and g are functions from the powerset of $[n]$ to real numbers and for all $A \subseteq [n]$

$$g(A) = \sum_{S \subseteq A} f(S)$$

$$\begin{aligned} \sum_{s \subseteq A} (-1)^{|A|-|S|} g(S) &= \sum_{s \subseteq A} (-1)^{|A|-|S|} \left(\sum_{T \subseteq A} f(T) \right) \\ &= \sum_{T \subseteq A} C_T f(T) \end{aligned} \tag{13.39}$$

Where C_T is appropriate signed number. Our aim is now to find C_T for different T

Case 1: ($T = A$) $C_T = 1$, since $f(A)$ is only encountered for $T = S = A$.

Case 2: ($T \neq A$) choosing a set between T and A is equivalent of choosing a set from $A \setminus T$

$$C_T = \sum_{T \subseteq S \subseteq A} (-1)^{|A|-|S|} = \sum_{i=0}^{k} (-1)^{k-1} \binom{k}{i} = 0$$

This proves the claim.

$$\boxed{\therefore f(A) = \sum_{S \subseteq A} (-1)^{|A|-|S|} g(S)}$$

□

Why it is strong version? it implies PIE. Assume the strong version, we can derive PIE.

Proof. Properties $P_1, \ldots, P_m$ of elements of X . $X_1, \ldots, X_m$ are the subsets of X satisfying the respective property i.e. $X_i = \{x \in X \mid x \text{ satisfy } P_i\}$. then for $S \subseteq [m]$ we define $f(S)$ to be the

number of elements in X having all properties P_i such that $i \notin S$ and none of the properties P_j such that $j \in S$ i.e.

$$f(S) = \left| \bigcap_{i \in [m] \setminus S} X_i \setminus \bigcup_{i \in S} X_i \right|$$

We are interested in counting the number of elements in X which does not satisfy any property in $P_1, \ldots, P_m$ i.e. $f([m])$. We define,

$$\begin{aligned} g(A) &= \sum_{S \subseteq A} f(S) \\ &= \left| \bigcap_{i \in [m] \setminus A} X_i \right| \\ &= N([m] \setminus A) \end{aligned}$$

$g(A)$ counts $x \in X$ if the property that x does not satisfy forms a subset of A. By 32.1.1

$$\begin{aligned} f([m]) &= \sum_{S \subseteq [m]} (-1)^{m-|S|} g(S) \\ &= \sum_{\substack{S' \subseteq [m] \setminus S \\ S \subseteq [m]}} (-1)^{|S'|} N(S') \\ &= \sum_{S \subseteq [m]} (-1)^{|S|} N(S) \end{aligned}$$

This concludes the proof. □

Instructor : Jayalal Sarma
Scribe : K Sampreeth Prem (*TA:* JS)
Date : Oct 5, 2020
Status : α

Lecture 14

Mobius Inversion and applications

14.1 Introduction

The focus on this lecture will be if we have two funtions f and g such that g can be expressed as a function of f by a peculiar relation then how can we express f in terms of g. We have already seen one such inversion during the discussion of stronger version of PIE where we have two fuctions mapping from sets to numbers. In this lecture we will look at a different setup where we have two functions $f : \{\mathbb{N}\} \to \{\mathbb{N}\}$ and $g : \{\mathbb{N}\} \to \{\mathbb{N}\}$ and if g can be expressed in a peculiar way w.r.t f then we want to invert to express f in terms of g.This is called **Möbius Inversion**. Before we formally state the theorem and prove it, we will look at two functions namely Euler's function and Möbius function and derive some of their properties.We will then establish a relation between these two functions to prove the Möbius Inversion and then look at an application of the theorem.

14.2 Euler's Function

Euler's function, also known as phi-function $\Phi(n)$, counts the number of integers between 1 and n inclusive, which are coprime to n.

$$\Phi(n) = |\{k \in \mathbb{N} | 1 \leq k \leq n, gcd(n,k) = 1\}|$$

We have already derived the formula for $\Phi(n)$ in 8.2.2 which is

$$\Phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}) \quad \text{where} \quad n = \prod_{i=1}^{k} (p_i)^{a_i} \tag{14.40}$$

14.2.1 Properties of $\Phi(n)$

Property 14.2.1. *If* $gcd(n1, n2) = 1 \Rightarrow \Phi(n_1)\Phi(n_2) = \Phi(n_1 n_2)$

Proof. We have derived this in 8.2.2 □

Property 14.2.2. $\sum_{d|n} \Phi(d) = n$

Proof. Fix d as a divisor of n. Consider the following sets $A = \{x \in \{1, 2, ..n\} | gcd(x, n) = d\}$ and $B = \{y \in [\frac{n}{d}] | gcd(y, \frac{n}{d}) = 1\}$. Now we will establish a bijection between these two sets. The cardinality of the second set is $\Phi(\frac{n}{d})$ (by definition of Φ) but instead of counting explicitly we will establish a bijection between A and B. Consider the mapping $x \mapsto \frac{x}{d}$,this mapping is well defined because $gcd(x, n) = d$ so $d|x$ and $\frac{x}{d}$ is an integer whose value is at most $\frac{n}{d}$ so it is in the range of B.The mapping is injective because division is injective. Now take any element from 1 to $\frac{n}{d}$, multiply it with d then we will get a number p such that $gcd(p, n) = d$ because d is the divisor of both n and p. So the mapping is also surjective and hence a bijection. Observe that the property can be rewritten as,

$$\sum_{k=\frac{n}{d}} \Phi(\frac{n}{k})$$

From the bijection established,

$$\sum_{d} |\{x \in \{1, 2, ..n\} | gcd(x, n) = d\}| = \sum_{k} \Phi(\frac{n}{k})$$

Notice that the summation on L.H.S will be equal to n that's because every number $l \in [1, n]$ will be counted exactly once in the summation when the variable of summation $d = gcd(x, n)$.
So,

$$n = \sum_{k} \Phi(\frac{n}{k})$$
$$\sum_{k} \Phi(\frac{n}{k}) = n$$

Hence, the proof. □

14.3 Möbius Function

For any positive integer n, Möbius Function $\mu(n)$ is defined as, 53

$$\mu(n) = \begin{cases} +1, & if\ n\ is\ a\ square-free\ positive\ integer\ with\ an\ even\ number\ of\ prime\ factors \\ -1, & if\ n\ is\ a\ square-free\ positive\ integer\ with\ an\ odd\ number\ of\ prime\ factors \\ 0, & otherwise \end{cases}$$

For example,$15 = 3 * 5$ has even number of prime factors which are square-free, hence $\mu(15) = 1$.
Similarly, $30 = 2 * 3 * 5$ and $20 = 2^2 * 5$ has μ values equal to -1 and 0.
Now, consider the factors of 30 and their μ values

Factors	30	15	10	6	5	3	2	1
μ	-1	1	1	1	-1	-1	-1	1

We Observe the sum of μ values of the factors of 30 are equal to 0. This isn't a coincidence and we will formally define this property and prove it.

Property 14.3.1. $\sum_{d|n} \mu(d) = \begin{cases} 1, & if\ n = 1 \\ 0, & otherwise \end{cases}$

Proof.

$$\mu(1) = 1 \ \ (\ by\ \ definition\ )$$

Take $n = \prod_{i=1}^{k} (p_i)^{a_i}$, we will consider only those factors of n whose prime factors have multiplicity 1 other factors of n which have prime factors multiplicity greater than 1 have μ value 0 and does not contribute to the sum.

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 p_2 \ldots p_k} \mu(d) \tag{14.41}$$

$$= \sum_{I \subseteq [k]} (-1)^I \tag{14.42}$$

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

$$= 0$$

Notice that in 14.47 the μ value depends only on whether we are picking odd number of primes or an even number and not on actual primes themselves so we could rewrite the summation to 14.48. □

Now, we will see a corollary of the above propery that connects the two functions μ and Φ.

Corollary 14.3.1. $\frac{\Phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}$

Proof. From 8.2.2

$$\Phi(n) = n\prod_{i=1}^{k}(1-\frac{1}{p_i}) \tag{14.43}$$

$$= n\sum_{I\subseteq[k]}(-1)^{|I|}\frac{1}{(\prod_{i\in I}p_i)} \tag{14.44}$$

$$= n\sum_{d|p_1..p_k}\frac{\mu(d)}{d} \tag{14.45}$$

$$= n\sum_{d|n}\frac{\mu(d)}{d} \tag{14.46}$$

In step 14.44, $I \subseteq [k]$ can be thought of as those prime indices that are picked which contribute to d so the $(\prod_{i\in I} p_i)$ becomes equal to d and the numerator $(-1)^{|I|}$ is exactly $\mu(d)$. The generalisation of step 14.45 to 14.46 is done following the observation that if $d|n$ but $d \nmid \prod p_1..p_k$ then d must have a prime factor whose multiplicity is greater than 1. Therefore, $\mu(d)$ becomes 0 for such d's. □

14.4 Möbius Inversion

$f, g : \mathbb{N} \to \mathbb{R}\ satisfying, \forall n\ g(n) = \sum_{d|n} f(d)\ \ then,$

$$\forall n\ f(n) = \sum_{d|n}\mu(d)d(\frac{n}{d})$$

Proof. Consider,

$$\sum_{d|n}\mu(d)g(\frac{n}{d}) = \sum_{k=\frac{n}{d}}\mu(\frac{n}{d})g(d) \tag{14.47}$$

$$= \sum_{d|n}\mu(\frac{n}{d})g(d) \tag{14.48}$$

$$= \sum_{d|n}\mu(\frac{n}{d})(\sum_{d'|d}f(d') \tag{14.49}$$

$$= \sum_{d'|n}C_{d'}f(d') \tag{14.50}$$

$$= f(n) \tag{14.51}$$

At 14.50 $C_{d'}$ represents the constant that tells us how many times $f(d')$ is going to appear in the summation. Note that, if $d|n$ then $(\frac{n}{d})|n$ so using a change of variable we were able to reach 14.48 from 14.48.

Now, we have two tasks, first calculate the value of $C_{d'}$ and next to show the summation value of 14.50 is $f(n)$.

Plan: Evaluate $(C_{d'})$ for differnet d'

Case1: If $d' = n$ then, $f(n)$ occurs only once in the summation 14.49. So, $C_n = 1$.

Case2: $d' < n \ \ and \ \ d'|n$.

$$C_{d'} = \sum_{d'|d|n} \mu(\frac{n}{d}) \tag{14.52}$$

$$= \sum_{d|n} \mu(\frac{n}{d}) \tag{14.53}$$

$$= \sum_{d|n} \mu(d) \tag{14.54}$$

$$= 0$$

In step $d \neq 1$ so by Property 14.3.1 (14.3.1) we get the value 0. Observe that in step 14.52 the summation value doesn't depend on d' so by change of variable we reach step 14.53.Similarly, we reached step 14.54 from 14.53 using change of variable that we have seen earlier.
Since we have calculated the value of $C_{d'}$ for different d's we will now show the value of summation in 14.50 is $f(n)$.

$$\sum_{d'|n} C_{d'} f(d') = C_n f(n) \ + \sum_{(d' < n)|n} C_{d'} f(d')$$

$$= 1 * f(n) + 0$$

$$= f(n)$$

Hence, proved. □

14.4.1 Application of Möbius Inversion

Problem Statement: Count the number of circular sequences/strings of 0's and 1's of length n.
Solution: We know that there are 2^n possible strings of 0's and 1's but some of them are clockwise rotations of each other and we consider them equal.So the circular sequences which are clockwise rotations of one another are equivalent.
Consider the following example of circular sequences of 0's and 1's of length 9. In order to represent a circular string in a normal form we fix a starting point and iterate it until it's length.
A = 001011010
B = 110100010
C = 100100100
By our definition of equivalence $A \equiv B \not\equiv C$.
Observe that sequence C is periodic, it has a repeating subsequence 100 whereas sequences A and

B do not contain any such repeating sub sequence.We call them aperiodic. In general a sequence is said to be aperiodic if it cannot be written as several times of a shorter sequence.
For every circular sequence there is a unique aperiodic circular sequence that we can associate with.
Instead of proving this claim we will write it as an example
For $n = 6$,
$000000 \Rightarrow 0$
$001001 \Rightarrow 001$
$111111 \Rightarrow 1$
$010010 \Rightarrow 010$
$001001 \Rightarrow 001$
Observe that the last two examples are equivalent and their circular subsequences are also equivalent. So their is an unique association (bijection) of circular sequences and their circular subsequences.
Another obvious observation is that the length of the circular subsequence must divide the original sequence.
Let,

$$M(d) = \ no.\ of\ periodic\ circular\ sequences\ of\ length\ d$$

Denote, N_n as the number of circular sequences of length n, then

$$N_n = \sum_{d|n} M(d) \tag{14.55}$$

Since we don't know the values of d we are summing up over all values of d that divides n.
Now we need to compute $M(d)$ as a function of d. **Aim:** Compute $M(d)$ as a function of d. **Solution:** Consider,the query how many aperiodic sequences of length d. Observe, that we have removed circular so equivalent ones are counted different. So, for every aperiodic circular sequence of length d, every shift of it is counted different hence, there are $dM(d)$ aperiodic sequences of length d.
We know that there are 2^n sequences(not circular) of length n each one uniquely corresponds to an aperiodic sequence.
Hence,

$$2^n = \sum_{d|n} dM(d) \tag{14.56}$$

Now, this is of the form $g(x) = \sum_{d|n} f(d)$ where, $g(x) = 2^n$ and $f(d) = d.M(d)$.
Using Möbius Inversion,

$$
\begin{aligned}
f(n) &= nM(n) \\
&= \sum_{d|n} \mu(d) g(\frac{n}{d}) \\
&= \sum_{d|n} \mu(d) 2^{\frac{n}{d}}
\end{aligned}
$$

From 14.55,

$$
\begin{aligned}
N_n &= \sum_{d|n} M(d) \\
&= \sum_{d|n} \frac{1}{d} (\sum_{l|d} \mu(l)\ 2^{\frac{d}{l}}) \\
&= \sum_{d|n} \frac{1}{d} \sum_{l|d} \mu(\frac{d}{l})\ 2^l \\
&= \sum_{l|n} (\sum_{l|d|n} \frac{1}{d} \mu(\frac{d}{l}) 2^l \\
&= \sum_{l|n} \sum_{1|\frac{d}{l}|\frac{n}{l}} \frac{1}{d}\ \mu(\frac{d}{l})\ 2^l
\end{aligned}
$$

Substituting $d = k\,l$,

$$
\begin{aligned}
&= \sum_{l|n} \sum_{k|\frac{n}{l}} \frac{2^l}{kl}\ \mu(k) \\
&= \sum_{l|n} \frac{2^l}{l} \sum_{k|\frac{n}{l}} \frac{\mu(k)}{k} \\
&= \sum_{l|n} \frac{2^l}{l}\ \frac{\Phi(\frac{n}{l})}{\frac{n}{l}} \\
&= \sum_{l|n} \frac{2^l\ \Phi(\frac{n}{l})}{n} \\
N_n &= \frac{1}{n} \sum_{l|n} 2^l\ \Phi(\frac{n}{l})
\end{aligned}
$$

Instructor : Jayalal Sarma
Scribe : Simran (*TA:* JS)
Date : Oct 5, 2020
Status : α

Lecture
15

Generating Functions

15.1 Introduction

In this lecture, we will see a new tool for solving counting problems, namely generating functions method. To get an intuition of this method, let's think about a counting problem with parameter n and say, we are interested in counting the number of objects of size n, denoted by a_n. We can view a_n as an infinite sequence of integers $(a_0, a_1, a_2, \dots)$, where we write down the first few terms of sequence explicitly . Next we try to match it up with some known integer sequence, say Maclaurin sequence or fabonacci sequence .
If we find some initial matching, say first 4 or 5 terms, then we try for a bijection between matching sequence and the corresponding problem to our setting.
The overall idea of this method is to view the counting problem as infinite sequences and then encode these sequences using the algebraic expression (namely power series) and then do some power series manipulation to recover some meaningful things corresponding to the counting problem we are interested in .

15.2 Generating Functions

Definition 15.2.1. ***Generating Functions*** *The generating function for a sequence of non-negative integers* $(a_n)_{n\in\mathrm{N}} = (a_0, a_1, a_2, \dots)$ *is given by*

$$F(x) = \sum_{n=0}^{\infty} a_n x^n$$

Remarks:

1 We are not going to evaluate the power series for any random value of x, say $F(100)$, as the series may not even be convergent .

2 We think of x in the expression $F(x)$ as a formal variable

We will indirectly use these expression in order to achieve our combinatorial goals without actually worrying about the convergence of the expression.
Let's look at an example to get more flavour of the idea introduced.

Consider a sequence with the first few terms as $a_0 = 1, a_1 = 42, a_2 = 23, \ldots$. The series corresponding to it is given by $A(x) = 1 + 42x + 23x^2 + \ldots$.
The advantage with this translation is that we can manipulate sequences in useful ways with simple algebra.
For the given $A(x)$, let's look at what happens when we multiply it by x.

We have $xA(x) = x+42x^2+23x^3+\ldots$. So we get, $a_0 = 0, a_2 = 42, a_3 = 23, \ldots$ as the coefficient of the series $xA(x)$. Hence we see that multiplying by x corresponds to shifting the sequence to the right by 1.

15.2.1 Operations on Generating Functions

Let us look at other algebraic operations that can be easily and more naturally performed on the given generating functions, $F(x) = \sum_{n=0}^{\infty} a_n x^n$ and $G(x) = \sum_{n=0}^{\infty} b_n x^n$

1 **Addition:**
$$F(x) + G(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

2 **Multiplication by a scalar** $\lambda \in \mathbb{R}$
$$\lambda F(x) = \sum_{n=0}^{\infty} \lambda a_n x^n$$

3 **Differentiation**
$$\frac{d}{d(x)}(F(x)) = F'(x) = \sum_{n=1}^{\infty} (n x^{n-1}) a_n$$

Substituting n with $n + 1$, we get
$$F'(x) = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n$$

Suppose the sequence corresponding to $F(x)$ is $(a_0, a_1, a_2, \ldots)$, then the sequence corresponding to $F'(x)$ is clearly $(a_1, 2a_2, 3a_3, \ldots)$

4 **Multiplication**
$$F(x)G(x) = \sum_{n=0}^{\infty} (\sum_{k=0}^{n} a_n b_{n-k}) x^n$$

Remark: Note that the coefficients resulting after applying differentiation or multiplication to the generating function may sometimes not always be meaningful, but as we proceed we will

look at few examples where the coefficients from multiplication will help us in countings.

15.2.2 A Quick Example: Maclaurin Series

The Maclaurin series is given by $1 + x + x^2 + \dots$ which corresponds to the sequence $(1, 1, 1, \dots)$. The shorthand algebraic expression corresponding to this series is given by

$$F(x) = \frac{1}{1-x}$$

To see this note that

$$(1-x)F(x) = F(x) - xF(x) = (1 + x + x^2 + \dots) - (x + x^2 + x^3 + \dots) = 1$$

Hence we have a neat shorthand algebraic expression for the Maclaurin Series . We will always think of this expression as a formal power series and never going to substitute the value for x. Now, let us demonstrate few of the discussed algebraic operations on the generating function of Maclaurin Series and use it or manipulate it to reach some new generating functions and the corresponding sequence

- Differentiating $F(x) = \frac{1}{1-x}$ with respect to x,

  $$F'(x) = \sum_{n=0}^{\infty}(n+1)a_{n+1}x^n = \frac{1}{(1-x)^2}$$

  So, we can say that $F'(x)$ is the generating function for the sequence $b_n = (n+1) = (1, 2, 3, \dots)$

- Substituting $x = -y$ in the generating function $F(x)$ gives us a new generating function $G(y)$ corresponding to the alternating sequence $(1, -1, 1, -1, \dots)$.
  Formally, we have $G(y) = F(-y) = \frac{1}{1+y}$.

15.3 Applying Generating Functions To Counting Problems

In this section we will look at the ways to use generating functions to solve the counting problems.

Example 1: Consider the situation where we need to distribute n votes to k candidates such that every candidate gets atleast one vote.
Note: In this example, we will see the correspondence of the multiplication of two generating functions to our counting problem.
Let $a_n^{(k)}$ denote the number of ways of distributing n votes to k candidates with each candidate getting atleast one vote and Let $B^{(k)} = \sum_{n=0}^{\infty} a_n^{(k)} x^n$, be the generating function corresponding to

$a_n^{(k)}$.
Let us look at the case where we have only candidate, i.e $k = 1$, we have:

$$a_n^{(1)} = \begin{cases} 0, & \text{for } n = 0 \\ 1, & \text{for } n \geq 1 \end{cases}$$

So, $a_n^{(1)} = (0, 1, 1, \dots)$, which is shifted version of Maclaurin Series. So the corresponding generating function is given by $B^{(1)}(x) = x\frac{1}{1-x}$
Observation: Let there be s male candidates and t female candidates. So $a_n^{(s+t)}$ can be thought as distributing n votes to $s+t$ candidates. Suppose male candidates got l votes and female candidates got $n - l$ votes. Also, each candidate gets 1 vote. So,

$$a_n^{(s+t)} = \sum_{l=0}^{n} a_l^{(s)} a_{n-l}^{(t)}$$

Using the observation, we get

$$B^{(s+t)}(x) = B^{(s)} B^{(t)}$$

Note that

$$a_n^{(s+t)} x^{s+t} = \left(\sum_{l=0}^{n} a_l^{(s)} a_{n-l}^{(t)} \right) x^{s+t}$$

So, the product of two generating function has a meaning in this context, hence we can use it. We are interested in $B^{(k)}(x)$ and we have $B^{(1)}(x)$. Hence,

$$B^{(k)}(x) = \left(B^{(1)}(x) \right)^k = \left(\frac{x}{1-x} \right)^k$$

Now, we have a generating function for the count we wanted. Our next step is to recover the count from this generating function.

Aim: To write down the Generating Function in the form of individual coefficient and then read off $a_n^{(k)}$
We have $B^{(k)}(x) = \frac{x^k}{(1-x)^k}$ Observe that,

$$\frac{d^{k-1}}{dx^{k-1}} \left(\frac{1}{1-x} \right) = (k-1)! \left(\frac{1}{(1-x)^k} \right)$$

Using the observation, we have

$$
\begin{aligned}
B^{(k)}(x) &= \frac{x^k}{(k-1)!}\left(\frac{d^{k-1}}{dx^{k-1}}\left(\frac{1}{1-x}\right)\right) \\
&= \frac{x^k}{(k-1)!}\left(\frac{d^{k-1}}{dx^{k-1}}(1+x+x^2+\dots)\right) \\
&= \frac{x^k}{(k-1)!}\left(\sum_{n=k-1}^{\infty} n(n-1)\dots(n=k+2)x^{n-k+1}\right) \\
&= \sum_{n=k-1}^{\infty} \frac{n(n-1)\dots(n=k+2)}{(k-1)!}x^{n+1}
\end{aligned}
$$

Using the expansion of $\binom{n}{k-1}$, we get

$$
\begin{aligned}
B^{(k)}(x) &= \sum_{n=k-1}^{\infty} \binom{n}{k-1}x^{n+1} \\
&= \sum_{n=k}^{\infty} \binom{n-1}{k-1}x^{n} \\
&= \sum_{n=0}^{\infty} \binom{n-1}{k-1}x^{n}
\end{aligned}
$$

Hence by reading off the coefficient of x^n, we have $a_n^{(k)} = \binom{n-1}{k-1}$.

To summarise the above example, we had a Counting problem, from the counting world we went to generating functions world and then manipulated it to get the power series of the required count and then we recovered $a_n^{(k)}$.

Example 2: Suppose Count the number of non negative solutions to $a+b+c=n$, such that,

- a is an even integer
- b is a non negative integer
- $c \in \{0,1,2\}$

Intuitively, we can think of this as having n votes and 3 candidates where the first candidate, a, should receive an even number of votes and b, c receives at most 2 votes.
The idea here is to use generating functions to split the problem nicely.
Let us consider three simpler settings ,

1 Suppose we have only one candidate a.
So, our equation reduces to $a = n$ and a should get even votes. So we have,

   – if n is odd, there is no solution

– if n is even, there is exactly one solution

Hence the corresponding sequence for this case looks like $(1, 0, 1, \dots)$ and the generating function is given by

$$A(x) = \sum_{n=0}^{\infty} x^{2n} = \sum_{n=0}^{\infty} (x^2)^n = \frac{1}{1-x^2}$$

2 Suppose we have b as the only candidate.
So, our equation reduces to $b = n$ and b should get non-negative number of votes. So, whatever the value of n is there exists a unique solution for the equation $b = n$.
Hence the corresponding sequence for this case looks like $(1, 1, 1, \dots)$ and the generating function is given by

$$B(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

3 Suppose we have c as the only candidate.
So, our equation reduces to $c = n$ and $c \in \{0, 1, 2\}$. Clearly,

– the number of solution is unique for $n \in \{0, 1, 2\}$
– the number of solutions is 0 for $n > 2$.

Hence, the generating function for this function is given by

$$C(x) = 1 + x + x^2$$

Observation : We are looking for non negative solutions of $a + b + c = n$, satisfying the three conditions discussed above.The coefficient of $x^n = x^{a+b+c}$ gives us the required number of solutions in the cases, where the coefficient of x^a, x^b and x^c will give us the number of solutions where a is even, b is non-negative integer and $c \in \{0, 1, 2\}$ respectively.
Using these the generating function of the count we are interested in is given by multiplying the generating functions of the cases discussed. Hence we have,

$$F(x) = A(x)B(x)C(x) = \frac{1 + x + x^2}{(1-x^2)(1-x)}$$

Now we want to write $F(x)$ as sum of terms where we will have the well known Maclaurin Series equation, to simplify our work
Using the method of partial fraction we have

$$\begin{aligned} F(x) &= \frac{R}{1+x} + \frac{S}{1-x} + \frac{T}{(1-x)^2} \\ &\Rightarrow \frac{1 + x + x^2}{(1-x^2)(1-x)} = \frac{R}{1+x} + \frac{S}{1-x} + \frac{T}{(1-x)^2} \end{aligned} \tag{15.57}$$

Multiplying both sides by $(1-x^2)(1-x)$, we get

$$\begin{aligned} 1+x+x^2 &= R(1-x)^2 + S(1-x)(1+x) + T(1+x) \\ &= (R+S+T) + (T-2R)x + (R-S)x^2 \end{aligned}$$

Equating the coefficients and solving we get,

$$R = 1/4, S = -3/4, T = 3/2$$

Finally substituting the values of R, S and T we have

$$F(x) = \frac{1}{4}\left(\sum_{n=0}^{\infty}(-1)^n x^n\right) - \frac{3}{4}\left(\sum_{n=0}^{\infty} x^n\right) + \frac{3}{2}\left(\sum_{n=0}^{\infty}(n+1)x^n\right)$$

Reading off the coefficients of x^n, the number of solutions of $a+b+c=n$ satisfying the properties specified is given by

$$a_n = \frac{(-1)^n}{4} - \frac{3}{4} + \frac{3(n+1)}{2}$$

15.4 Catalan numbers using generating functions

We already have come across Catalan numbers in Week3 lectures and seen that

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

In this section we will derive this count using generating functions. Here we interpret Catalan Numbers C_n as number of ways of forming well formed paranthesised expression with n pairs of brackets. In this example we will also see the notion of recurrence relation.

Recurrence Relation for Catalan numbers Basically, the recurrence relation for a sequence $(a_0, a_1, a_2, \ldots, a_n, \ldots)$, tries to figure out the relation between a_n and the previous a_i's.
Let $(a_0, a_1, a_2, \ldots)$ denote the sequence for the given counting problem, where we use a_n to denote the number of ways of forming well formed paranthesised expression with n pairs of brackets.
To count a_n, we approach in the following steps:

1 Place one pair of bracket (and)

2 Place k pairs of brackets inside the already placed pair of brackets

3 Place the remaining $n-k-1$ pairs of brackets adjacent to this placed bracketing

With this conditioning on k, we can write

$$a_n = \sum_{k=0}^{n-1} a_k a_{n-k-1}$$

So, generating function for a_n

$$F(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + \sum_{n=1}^{\infty} a_n x^n$$

Here a_0 is the number of ways of forming well formed paranthesised expression with 0 pairs of brackets, which is unique.
So,

$$F(x) = 1 + \sum_{n=1}^{\infty} a_n x^n$$

Substituting for a_n using the recurrence relation obtained, we get

$$\begin{aligned} F(x) &= 1 + \sum_{n=1}^{\infty} \left(\sum_{k=0}^{n-1} (a_k a_{n-k-1}) x^n \right) \\ &= 1 + x \left(\sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} (a_k a_{n-k-1}) x^n \right) \right) \\ &= 1 + x(F(x)F(x)) \end{aligned}$$

So, we get

$$\begin{aligned} F(x) &= 1 + x(F(x)^2) \\ &\Rightarrow x(F(x))^2 - F(x) + 1 = 0 \end{aligned} \tag{15.58}$$

Solving the quadratic equation, we get

$$F(x) = \frac{1 - \sqrt{1 - 4x}}{2x}$$

Now, to simplify $F(x)$ into some known power series form, we need to simply the $\sqrt{1-4x}$ term in the function. For this we need a separate tool, informally the generalisation of the binomial theorem.

Binomial Theorem : For every $n, k \in \mathbb{N}$, we have

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{k=0}^{\infty} \binom{n}{k} x^k$$

Now, we will see the extended version of the Binomial Theorem, known as Newton's Binomial Theorem, where we consider any $n \in \mathbb{R}$

Theorem 15.4.1. *Newton's Binomial Theorem*
For all non-zero $n \in \mathbb{R}$, we have

$$(1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k$$

Proof Omitted

So, for any $n \in \mathbb{R}, n \neq 0$, we can compute the value of $\binom{n}{k}$ by using the expression

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

.

Example: Take $n = -7/2$ and $k = 5$, so we have

$$\binom{-7/2}{5} = \frac{(-7/2)(-9/2)(-11/2)(-13/2)(-15/2)}{5!} = -\frac{9009}{256}$$

Now, getting back to the generating function for the catalan numbers

$$F(x) = \frac{1-\sqrt{1-4x}}{2x} = \frac{1-(1-4x)^{1/2}}{2x} \tag{15.59}$$

Let us look at a lemma which will help us simplify the square root term.

Lemma 15.4.2. *For $n \in \mathbb{N}$, we have*

$$\binom{1/2}{n} = (-1)^{n+1} \binom{2n-2}{n-1} \frac{1}{2^{2n-1}} \cdot \frac{1}{n}$$

Proof. Left as an exercise to the readers. *Hint*: Use induction on n

□

Applying 15.4.2 to $\sqrt{1+x} = (1+x)^{1/2}$, we have

$$\begin{aligned} \sqrt{1+x} &= \sum_{n=0}^{\infty} \binom{1/2}{k} x^n \\ &= 1 + \sum_{n=1}^{\infty} (-2) \binom{2n-2}{n-1} \frac{1}{2^{2n}} \cdot \frac{1}{n} (-1)^{n+1} \end{aligned} \tag{15.60}$$

Substituting 15.60 in 15.59 we get,

$$\begin{aligned} F(x) &= \frac{1}{2x}\sum_{n=1}^{\infty} 2\binom{2n-2}{n-1}\frac{(-1)^n(-4x)^n}{2^{2n}n} \\ &= \frac{1}{x}\sum_{n=1}^{\infty}\binom{2n-2}{n-1}\frac{1}{n}x^n \\ &= \sum_{n=0}^{\infty}\binom{2n}{n}\frac{1}{n+1}x^n \end{aligned}$$

Hence the generating function for the catalan numbers is,

$$F(x) = \sum_{n=0}^{\infty}\binom{2n}{n}\frac{1}{n+1}x^n$$

and the coefficient $a_n = \binom{2n}{n}\frac{1}{n+1}$ denotes the catalan numbers.

15.5 Live Discussion Session, Oct 8

Consider a standard dice with $(1, 2, 3, 4, 5, 6)$ as the number on it's faces. Let us look at the sum values that can be obtained when two standard dice are rolled together and number of different ways in which the pair of standard dice results to the sum value . Note that the minimum sum that can be obtained is 2 (when 1 appears on each dice) and the maximum sum that a pair of standard dice can yeild is 12 (when 6 appears on each dice).

Sum Value	2	3	4	...	12
# of pairs	1	2	3	...	1

Now, let's compute the value Pr[Sum value $= 8$]. We know that there are 36 different pairs as an outcome when we two standard dice are rolled together. The pairs that result in 8 are $(2, 6), (3, 5), (4, 4), (5, 3), (6, 2)$. So we get

$$\text{Pr[Sum value} = 8] = \frac{5}{36}$$

15.5.1 Crazy Dice Problem and Generating Functions

The question of interest here is can we find a pair of dice with $(a_1, a_2, a_3, a_4, a_5, a_6)$ and $(b_1, b_2, b_3, b_4, b_5, b_6)$ as their faces, such that throwing the two dice in sequence gives us the same sum distribution as a standard dice. Let's try to figure it out using the generating functions method. First, we try to relate a standard dice with $(1, 2, 3, 4, 5, 6)$ as the number on it's faces to a sequence and then using the sequence we can figure out it's generating function.

Generating Function for a Standard Dice Let a_n denote the number of ways in which a dice when rolled can produce the number n. So for the standard dice ($1 \leq n \leq 6$) we know there is a unique way to get each face $\{1, 2, \ldots, 6\}$. So, the infinite sequence representing it is $(1, 1, 1, 1, 1, 1, 0, 0, \ldots)$ and the corresponding generating function is

$$F(x) = x + x^2 + x^3 + x^4 + x^5 + x^6$$

The generating function for the sum value when two dice are thrown in a sequence can be given by multiplying the respective generating function of each die.

So, for two standard dice thrown in a sequence, the generating function for the sum of the values appeared on each die is given by

$$f(x) = (x + x^2 + x^3 + x^4 + x^5 + x^6)^2 \tag{15.61}$$

Observation: For two dice with $(a_1, a_2, a_3, a_4, a_5, a_6)$ and $(b_1, b_2, b_3, b_4, b_5, b_6)$ as their faces such that they fit in the requirement of our question, the product of their generating functions must be equal to 15.61

Let $p(x) = x^{a_1} + x^{a_2} + \cdots + x^{a_6}$ and $p(x) = x^{b_1} + x^{b_2} + \cdots + x^{b_6}$ denote the generating function of the two dice considered respectively.

So, from the observation we have that

$$p(x)q(x) = (x + x^2 + x^3 + x^4 + x^5 + x^6)^2 \tag{15.62}$$

Using few algebraic manipulation we get

$$x + x^2 + x^3 + x^4 + x^5 + x^6 = x(1 + x)(1 + x + x^2)(1 - x + x^2)$$

. Substituting this in 15.62, we have

$$\begin{aligned} p(x)q(x) &= (x(1 + x)(1 + x + x^2)(1 - x + x^2))^2 \\ &= x^2(1 + x)^2(1 + x + x^2)^2(1 - x + x^2)^2 \end{aligned} \tag{15.63}$$

An additional constraint on $p(x)$ and $q(x)$ is that $p(1) = q(1) = 6$, since the sequence corresponding to both these must have 6 terms.

Now our task is to distribute the factors of $x^2(1+x)^2(1+x+x^2)^2(1-x+x^2)^2$ to $p(x)$ and $q(x)$ such that the 15.63 and the constraint $p(1) = q(1) = 6$ is satisfied. One such valid distribution of the factors is $p(x) = x(1 + x)(1 + x + x^2)$ and $q(x) = x(1 + x)(1 + x + x^2)(1 - x + x^2)^2$. Simplifying these gives us

$$p(x) = x + 2x^2 + 2x^3 + x^4 \tag{15.64}$$

$$q(x) = x + x^3 + x^4 + x^5 + x^6 + x^8 \tag{15.65}$$

Using 15.64, we get $(a_1, a_2, a_3, a_4, a_5, a_6) = (1, 2, 2, 3, 3, 4)$ and from 15.65, we get $(b_1, b_2, b_3, b_4, b_5, b_6) = (1, 3, 4, 5, 6, 8)$.

So, we were able to get two dice with faces $(1, 2, 2, 3, 3, 4)$ and $(1, 3, 4, 5, 6, 8)$ such that throwing these two dice in sequence gives us the same sum distribution as throwing a pair of standard dice.

Instructor : Jayalal Sarma
Scribe : K Sampreeth Prem (*TA:* JS)
Date : Oct 5, 2020
Status : α

Lecture
16

Recurrence relation for Derangements

16.1 Introduction

We were looking at the tool named generating functions and towards the end of last lecture we have seen recurrence relation for catalan numbers.The idea was to express the n^th term of the sequence as a function of the previous terms and along with the generating functions obtain a closed form expression for the generating function, then use the series expansion to get the n^th term of the infinite sequence. In this lecture we will focus on getting a recurrence relation for Derangements.

16.2 Derangements

A Derangement is a permutation in which none of the objects appear in their "natural" (i.e., ordered) place.

$$D_n = |\{\sigma \in S_n | \forall i\, \sigma(i) \neq i\}|$$

We have already seen the expression for D_n using P.I.E in 8.2.1 which is,

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

Now we will try to obtain this expression using recurrence relations.

16.2.1 Recurrence relations for Derangements

Before we state the recurrence relations, let's fix the initial conditions.
$D_0 = 1$ because there are no elements out of their natural position so we take it as 1 and $D_1 = 0$ since, we cannot have a derangement on one element.

Recurrence Relation 16.2.1.

$$D_n \;=\; (n-1)\,(D_{n-1} \;+\; D_{n-2}) \tag{16.66}$$

Proof. We will use a double counting argument to prove this.
On **L.H.S** it's the number of derangements on n elements.
On **R.H.S**, let $\sigma \in S_n$ denote the derangement. So, $\sigma(n) \;\neq\; n$.
Let $\sigma(n) = k$, now there are two cases,
Case 1: $\sigma(k) = n$
So, we can remove n and k from the set $\{1, ..., n\}$ and by appropriate renaming the new $\sigma(say\ \sigma')$ corresponds to a derangement $S_n - 2$.Since there are $n-1$ ways of choosing k
Case 2: $\sigma(k) \neq n$
Consider the following bijection to a derangement in S_{n-1}.
Swap $\sigma(k)$ and $\sigma(n)$ in the permutation. In the resulting permutation($say\ \sigma'$) $\sigma'(n) = j(j \neq n)$ and $\sigma'(k) = k$. This isn't a derangement because $\sigma'(k) = k$. So remove k and by appropriate renaming σ' gives a derangement in S_{n-1}.
So from **Case 1** and **Case 2** we conclude by fixing k there are $(D_{n-1} \;+\; D_{n-2}\,)$ derangements possible. Since, k is arbitrary and there are $n-1$ ways of choosing k we get number of derangements possible as, $(n-1)\,(D_{n-1} \;+\; D_{n-2})$. □

Recurrence Relation 16.2.2.

$$D_n \;=\; nD_{n-1} \;+\; (-1)^n \tag{16.67}$$

Proof. From 16.2.1,

$$\begin{aligned} D_n \;&=\; (n-1)\,(D_{n-1} \;+\; D_{n-2}) \\ D_n \;-\; nD_{n-1} \;&=\; -\,(D_{n-1} \;-\; (n-1)D_{n-2}) \end{aligned}$$

Substitute $A_n = D_n - nD_{n-1}$,

$$\begin{aligned} A_n \;&=\; -\,A_{n-1} \\ A_n \;&=\; (-1)^n \\ D_n \;-\; nD_{n-1} \;&=\; (-1)^n \end{aligned}$$

□

Recurrence Relation 16.2.3.

$$D_n \;=\; n! - \sum_{k=0}^{n-1} \binom{n}{k} D_k \tag{16.68}$$

Proof.

$$\begin{aligned} D_n \;&=\; n! - \sum_{k=0}^{n-1} \binom{n}{k} D_k \\ n! \;&=\; D_n + \sum_{k=0}^{n-1} \binom{n}{k} D_k \\ n! \;&=\; \sum_{k=0}^{n} \binom{n}{k} D_k \end{aligned} \tag{16.69}$$

Now we will argue 16.69 using double counting argument.
On **L.H.S** it's the number of permutations on n numbers.
On **R.H.S**, observe that each permutation has some points which are in their natural position i.e., $\sigma(i) \;=\; i$ and others are derangements on the remaining elements.Now we condition on number of fixed points and there are $\binom{n}{k}$ ways of fixing k points and remaining form derangements.Notice that we are not over counting across sums because once we fix the number of fixed points one permutation cannot have two different number of fixed points. □

We have stated and proved the recurrence relations associated with derangements. Now, we will derive the formula for Derangements using the recurrence relations.
Consider 16.2.2,

$$\begin{aligned} D_n \;&=\; nD_{n-1} \;+\; (-1)^n \\ D_n \;-\; nD_{n-1} \;&=\; (-1)^n \end{aligned}$$

Divide throughout by $n!$

$$\begin{aligned} \frac{D_n}{n!} \;-\; \frac{D_{n-1}}{n-1!} \;&=\; \frac{(-1)^n}{n!} \\ Substitute\ B_n \;&=\; \frac{D_n}{n!} \\ B_n \;-\; B_{n-1} \;&=\; \frac{(-1)^n}{n!} \end{aligned}$$

$$
\begin{aligned}
B_n &= B_{n-1} + \frac{(-1)^n}{n!} \\
B_n &= B_{n-1} + \frac{(-1)^n}{n!} \\
B_n &= B_{n-2} + \frac{(-1)^{n-1}}{n-1!} + \frac{(-1)^n}{n!}
\end{aligned}
$$

By repeatedly expanding the terms on **R.H.S**,we get

$$
\begin{aligned}
B_n &= \sum_{k=0}^{n} \frac{(-1)^k}{k!} \\
D_n &= n!(\sum_{k=0}^{n} \frac{(-1)^k}{k!})
\end{aligned}
$$

Instructor : Jayalal Sarma
Scribe : Lalithaditya (*TA:* JS)
Date : Oct 19, 2020
Status : α

Lecture 17

Generating Functions(continued)

17.1 Quick Recap of Previous Two Lectures

- We represented the sequence of non-negative integers in the form of a formal power series.
- Operations on power series corresponding to combinatorial meanings.
- We used the concept of Generating Functions for the following examples:
  1. Distributing 'n' votes to 'k' candidates such that every candidate gets atleast one vote.
  2. Count the number of non-negative solutions for the equation $a + b + c = n$
  3. Derving the expression for Catalan numbers.

17.2 Recurrence Relations

There are three types of recurrence relations,that are being discussed in this lecture. There are Linear Recurrence Relations, Degree Recurrence Relations and Homogenous Recurrence Relations. Before getting into examples,lets discuss about these relations.

- **Linear Recurrence Relation:**

  A Linear Recurrence Relation is a equation that defines n^{th} in a sequence in terms of the k previous terms in the sequence. The recurrence relation is in the form:

$$a_n = c_1.a_{n-1} + c_2.a_{n-2} + c_3.a_{n-3} + \ldots + c_k.a_{n-k}$$
$$= \sum_{i=1}^{k} c_i * a_{n-i}$$

  where $c_i's$ *are constants independent of* n,
  $c_1, c_2, c_3, \ldots, c_k \in \mathbb{R}$ and $c_k \neq 0$.

- **Degree Recurrence Relation:**

  A recurrence relation of degree d is said to be Degree Recurrence Relation where a_n depends only on a_{n-d}.

- **Homogenous Recurrence Relation:**

  A recurrence relation where each term of the right hand side of the equation has the same degree.

- **Some examples on recurrence relations:**

  1. $a_n = 5.a_{n-1} + a_{n-2}.a_{n-3}$: This is neither linear nor homogenous.
  2. $a_n = a_{n-1}.a_{n-2} + a_{n-3}.a_{n-4}$: This is not linear but homogenous of degree 4.
  3. $a_n = 5.a_{n-2} + 10^n$: This is linear but not homogenous of degree 2.

17.3 Using Generating Functions to solve recurrence relations

In this section, we will look how to solve recurrence relations using generating functions.

Example 1:
In the previous lectures,we can calculated the number of binary strings of length n, which have even number of 0's. It turned out to be 2^{n-1}.
Similarly, calculate the number of decimal strings of length n, which contain even number of 0's.

Solution:
Let the a_n be the number of decimal strings,which satisfy the given condition.
By convention,lets take that when $n = 0$, the number of such strings is 1.
If $n = 1$,then the number of such strings will be 9.
$\Rightarrow a_0 = 1$ and $a_1 = 9$.

Forming the recurrence relation: Let's take a n-length decimal string, and let d_n be the last digit in the string. There are two cases for this type of situation i.e. if $d_n = 0$ and $d_n \neq 0$.
Case-I:
If the last digit is 0, then the remaining string must have odd number of zeroes.Then the number of such strings will be $(10^{n-1} - a_{n-1})$.

Case-II:
If the last digit is not zero, then the remaining string must have even number of zeroes,which is equal to number of such strings of length $n-1$ i.e. a_{n-1}. The last digit can vary from $1, 2, 3, \ldots, 9$.

Therefore, the number of such strings will be $(9a_{n-1})$.

The resultant recurrence relation for a_n is,

$$\Rightarrow a_n \ = \ (10^{n-1} - a_{n-1} + 9a_{n-1})$$

$$\Rightarrow a_n \ = \ (10^{n-1} + 8a_{n-1})$$

The generating function for this problem will be,

$$G(x) = \sum_{n\geq 0} a_n.x^n \tag{17.70}$$

$$G(x) \ = \ a_0 \ + \ \sum_{n\geq 1} a_n.x^n$$

$$G(x) \ = \ a_0 \ + \ \sum_{n\geq 1} .(10^{n-1} + 8a_{n-1})x^n$$

$$G(x) \ = \ 1 \ + \ \sum_{n\geq 1} 8.a_{n-1}.x^n \ + \ \sum_{n\geq 1} 10^{n-1}.x^n$$

$$G(x) \ = \ 1 \ + \ 8.x \ \sum_{n\geq 1} a_{n-1}.x^{n-1} \ + \ x \ \sum_{n\geq 1} 10^{n-1}.x^{n-1}$$

Let $n - 1 \ = \ h$.Then,

$$G(x) \ = \ 1 \ + \ 8.x \ \sum_{h\geq 0} a_h.x^h \ + \ x \ \sum_{h\geq 0} 10^h.x^h$$

After renaming the variable, we have

$$G(x) \ = \ 1 \ + \ 8.x \ \sum_{n\geq 0} a_n.x^n \ + \ x \ \sum_{n\geq 0} 10^n.x^n$$

From the equation (17.72), we can see that $G(x) = \sum_{n\geq 0} a_n.x^n$

$$G(x) \ = \ 1 \ + \ 8.x.G(x) \ + \ x \ \sum_{n\geq 0} 10^n.x^n$$

$$G(x) \ = \ 1 \ + \ 8.x.G(x) \ + \ x \ \sum_{n\geq 0} (10.x)^n$$

From the summation of infinte geometric progression, we have

$$\sum_{n\geq 0} (10.x)^n = \frac{1}{1 - 10.x}$$

$$G(x) \;=\; 1 \;+\; 8.x.G(x) \;+\; x.\left(\frac{1}{1-10.x}\right)$$

After rearranging the terms, we finally $G(x)$ as,

$$G(x) \;=\; \frac{(1-9.x)}{(1-8.x).(1-10.x)}$$

By using the concept of partial fractions, let's split the above into two fractions,

$$\frac{(1-9.x)}{(1-8.x).(1-10.x)} \;=\; \frac{A}{(1-8.x)} \;+\; \frac{B}{(1-10.x)}$$

$$=\; \frac{A+B-(10.A.x)-(8.B.x)}{(1-8.x).(1-10.x)}$$

$$\Rightarrow A+B=9 \; and \; 10.A+8.B=9$$

After solving for A and B, we get $A=\frac{1}{2}$ and $B=\frac{1}{2}$

$$G(x) \;=\; \frac{\frac{1}{2}}{(1-8.x)} \;+\; \frac{\frac{1}{2}}{(1-10.x)} \tag{17.71}$$

Our aim was to find the number a_n,which is nothing but the coefficient of x^n in $G(x)$.

$$\Rightarrow Coefficient\ of\ x^n\ in\ G(x) \;=\; \left(\frac{1}{2}.8^n\right)+\left(\frac{1}{2}.10^n\right)$$

$$=\; \frac{8^n+10^n}{2}$$

$\therefore$ Number of decimal strings with even number of zeroes is $\left(\frac{8^n+10^n}{2}\right)$.

Example 2:

In this example, we are not using any recurrence relations. We are proving combinatorial equations using generating functions.

For $n \geq k$, prove that

$$\sum_{m=k}^{k} \binom{m}{k} \;=\; \binom{n+1}{k+1} \tag{17.72}$$

Solution:

For a fixed k, lets assume that

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

The generating function for this problem will be,

$$S(x) \;=\; \sum_{n\geq k} a_n.x^n \tag{17.73}$$

We can observe that in the above summation, n starts from k. It can also start from n = 0, but it is the same, as $k \geq 0$.

Lets introduce a new function σ,

$$\sigma = \begin{cases} 1 & if\ k \leq m \leq n \\ 0 & otherwise \end{cases}$$

From equation (17.74),

$$S(x) \;=\; \sum_{n\geq k} a_n.x^n$$

$$S(x) \;=\; \sum_{n\geq k} \sum_{m=k}^{n} \binom{m}{k}.x^n$$

$$S(x) \;=\; \sum_{n\geq k} \left(\sum_{m\geq k} \binom{m}{k}.x^n\,(\sigma) \right)$$

After rearranging the summations,

$$S(x) \;=\; \left(\sum_{m\geq k} \sum_{n\geq k} \binom{m}{k}.x^n\,(\sigma) \right)$$

Since $k \leq m$ and $k \leq n$ the new function σ becomes 1.

Also $k \leq m$ and $k \leq n$, $\Rightarrow m \leq n$.

$$\Rightarrow\; S(x) \;=\; \left(\sum_{m\geq k} \sum_{n\geq m} \binom{m}{k}.x^n \right)$$

Since, $\binom{m}{k}$ is independent of n,

$$S(x) \;=\; \left(\sum_{m\geq k} \binom{m}{k}. \sum_{n\geq m} x^n \right)$$

$$S(x) \;=\; \sum_{m\geq k} \binom{m}{k}. \left(x^m \sum_{n\geq m} x^{n-m} \right)$$

We can observe that the second summation is the sum of an infinite geometric progression.

$$S(x) \;=\; \sum_{m\geq k} \binom{m}{k}.\left(\frac{x^m}{1-x}\right)$$

$$S(x) \;=\; \frac{x^k}{1-x}\left(\sum_{m\geq k} \binom{m}{k}.x^{m-k}\right) \tag{17.74}$$

We know that,

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots + \ldots$$

and also,

$$\left(\frac{1}{1-x}\right)^{k+1} = (1 + x + x^2 + \cdots + \ldots)^{k+1}$$

$$(1 + x + x^2 + \cdots + \ldots)^{k+1} = (1 + x + x^2 + \ldots).(1 + x + x^2 + \ldots).\ldots$$

Let $d_1, d_2, d_3, \ldots, d_{k+1}$ be the degree of each x terms in the product.
Our aim is to get the coefficient of x^{m-k} in the above product, this is equivalent to the question

In how many ways can we pick $d_1, d_2, \ldots, d_{k+1}$ such that

$$\sum_{i=1}^{k+1} d_i = (m-k)$$

This is an example of multichoosing. As discussed in the previous lectures, the number of solutions to this question is

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

and also,

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

From the equation (17.76), we can replace $\binom{m}{k}.x^{m-k}$ with $\left(\frac{1}{1-x}\right)^{k+1}$

$$S(x) \;=\; \frac{x^k}{1-x}\left(\frac{1}{1-X}\right)^{k+1}$$

$$S(x) \;=\; \frac{x^k}{(1-x)^{k+2}} \tag{17.75}$$

Our aim is to find the number a_n, which is nothing but the coefficient of x^n in the generating function $S(x)$.

We can observe that the,

$$Coefficient\ of\ x^n\ in \frac{x^k}{(1-x)^{k+2}} \quad = \quad Coefficient\ of\ x^{n-k}\ in\ \left(\frac{1}{1-x}\right)^{k+2}$$

As we proved earlier in this example, that the coefficient of x^{n-k} in the right hand side, is equivalent to the sum of degrees of x terms by expanding $\left(\frac{1}{1-x}\right)$ equal to $(k+2)$.
As proved in earlier lectures, this sum is equal to

$$a_n = \binom{k+2+n-k-1}{n-k}$$

$$\binom{k+2+n-k-1}{n-k} = \binom{n+1}{n-k}$$

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

$$\boxed{\therefore a_n = \binom{n+1}{k+1}}$$

Instructor : Jayalal Sarma
Scribe : Lalithaditya and Pragnya (*TA:* JS)
Date : Oct 20, 2020
Status : α

Lecture 18

Two Variable Generating Functions

Till now we had discussed Generating Functions with one variable. In this lecture, we are going to discuss Generating Functions with two variables. Such type of Generating functions are known as **Bivariate Generating Functions**.

The general form of the Bivariate Generating functions is,

$$G(x, y) = \sum_{n,k \geq 0} a_{n,k}.x^n.y^k$$

These type of generating functions are useful, when dealing combinatorial problems with two variables.
Lets try out some examples, to get an idea on how to use Generating Functions with two variables.

18.1 Examples based on Bivariate Generating Functions

Example 1:
Prove the binomial theorem in single variable using the two variable generating functions.
Binomial Theorem in single variable:

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k}.x^k$$

Solution:

We know that the number of ways of choosing a k-sized subset from n-sized set is equal to $\binom{n}{k}$.

Let the number be $b_{n,k}$.
When $n = 0$, $b_{0,k} = 0$ and when $k = 0$, $b_{n,0} = 1$.

As discussed in previous lectures, we can choose a k-sized subset from n-1 elements or from n elements.

Recurrence relation:

$$b_{n,k} = b_{n-1,k-1} + b_{n-1,k}$$

The generating function for this problem is,

$$B(x,y) = \sum_{n,k\geq 0} b_{n,k}.\left(x^n.y^k\right) \tag{18.76}$$

$$B(x,y) = \sum_{n\geq 0,k=0} b_{n,0}x^n + \sum_{n=0,k\geq 0} b_{0,k}.y^k + \sum_{n,k\geq 1} b_{n,k}.\left(x^n.y^k\right)$$

We know that $b_{0,k} = 0\ and\ b_{n,0} = 1$.

$$B(x,y) = \sum_{n\geq 0,k=0} 1.\left(x^n\right) + \sum_{n=0,k\geq 0} 0.\left(y^k\right) + \sum_{n,k\geq 1} b_{n,k}.\left(x^n.y^k\right)$$

$$B(x,y) = \sum_{n\geq 0,k=0} \left(x^n\right) + \sum_{n,k\geq 1} b_{n,k}.\left(x^n.y^k\right)$$

By using the recurrence relation,

$$B(x,y) = \sum_{n\geq 0,k=0} \left(x^n\right) + \sum_{n,k\geq 1} b_{n-1,k-1}.\left(x^n.y^k\right) + \sum_{n,k\geq 1} b_{n-1,k}.\left(x^n.y^k\right)$$

We know that,

$$\sum_{n\geq 0} x^n = \frac{1}{1-x}$$

$$B(x,y) = \frac{1}{1-x} + \sum_{n,k\geq 1} b_{n-1,k-1}.\left(x^n.y^k\right) + \sum_{n,k\geq 1} b_{n-1,k}.\left(x^n.y^k\right)$$

$$B(x,y) = \frac{1}{1-x} + (x.y)\sum_{n,k\geq 1} b_{n-1,k-1}.\left(x^{n-1}.y^{k-1}\right) + x.\sum_{n,k\geq 1} b_{n-1,k}.\left(x^{n-1}.y^k\right)$$

$$B(x,y) = \frac{1}{1-x} + (x.y)\sum_{n,k\geq 1} b_{n-1,k-1}.\left(x^{n-1}.y^{k-1}\right) + x.\sum_{n,k\geq 1} b_{n-1,k}.\left(x^{n-1}.y^k\right)$$

Let $(n-1) = h\ and\ (k-1) = p$

$$B(x,y) = \frac{1}{1-x} + (x.y)\sum_{h,p\geq 1} b_{h,p}.\left(x^h.y^p\right) + x.\sum_{n,k\geq 1} b_{n-1,k}.\left(x^{n-1}.y^k\right)$$

After renaming of variables,

$$B(x,y) = \frac{1}{1-x} + (x.y) \sum_{n,k\geq 1} b_{n,k}.\left(x^n.y^k\right) + x.\sum_{n,k\geq 1} b_{n-1,k}.\left(x^{n-1}.y^k\right)$$

$$B(x,y) = \frac{1}{1-x} + (x.y) \sum_{n,k\geq 1} b_{n,k}.\left(x^n.y^k\right) + x.\left(\sum_{n,k\geq 0} b_{n,k}.\left(x^n.y^k\right) - \sum_{n\geq 0,k=0} x^n\right)$$

$$B(x,y) = \frac{1}{1-x} + (x.y) \sum_{n,k\geq 0} b_{n,k}.\left(x^n.y^k\right) + x.\left(\sum_{n,k\geq 0} b_{n,k}.\left(x^n.y^k\right) - \sum_{n\geq 0,k=0} x^n\right)$$

From the equation (18.78),

$$B(x,y) = \frac{1}{1-x} + (x.y)\,.B(x,y) + x.\left(B(x,y) - \frac{1}{1-x}\right)$$

After rearranging the terms,

$$B(x,y) = 1 + x.\,(y+1)\,.B(x,y)$$

$$B(x,y) = \frac{1}{1-x.\,(y+1)}$$

$\therefore$ The generating function $B(x,y)$ is,

$$\boxed{B(x,y) = \frac{1}{1-x.\,(y+1)}} \tag{18.77}$$

Coefficient of x^n in the Left hand side of the above equation is equal to the coefficient of x^n in the right hand side of the above equation.

Coefficient of x^n in the left hand side $= \sum_{k\geq 0} b_{n,k}.y^k$ ($\because$ *From equation* (18.78))

Note: Coefficient of x^n in $\left(\frac{1}{1-ax}\right)$ is a^n.

$\Rightarrow$ Coefficient of x^n in the right hand side $= (1+y)^n$

Hence,

$$\sum_{k\geq 0} b_{n,k}.y^k = (1+y)^n$$

After renaming of variables,

$$(1+x)^n = \sum_{k\geq 0} b_{n,k}.x^k$$

At the beginning of the proof, we assumed that $b_{n,k} = \binom{n}{k}$

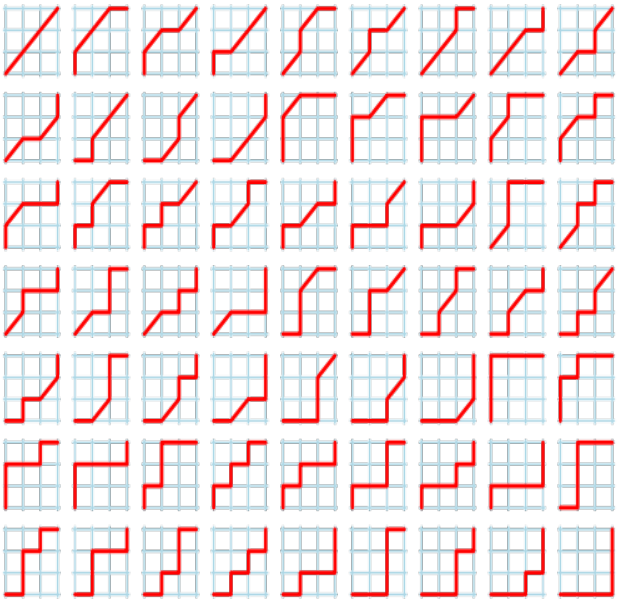
$$\boxed{\therefore (1+x)^n = \sum_{k\geq 0} \binom{n}{k} .x^k} \tag{18.78}$$

which completes our proof.

Example 2 (Delannoy Numbers):
Consider a nxn grid. Delannoy number D counts the number of paths from the left-bottom corner (0,0) to any other point on the grid (n,m).
The path can be reached by only three paths i.e Upward edges(U), Rightward edges(R) and upward forward diagonals(F). Find the Delannoy Number.

Solution:
Let $d_{n,m}$ be the number of Delannoy paths from (0,0) to (n,m), by using the above edges only.

For example,When n=3 and m=3, then the number of Delannoy paths is 63.



Aim: To find $d_{n,m}$

Recurrence Relation:

Lets find a recurrence relation for $d_{n,m}$.
A point (n,m) can be reached from three ways i.e. from (n-1,m), from (n-1,m-1) and from (n,m-1).

Hence, the recurrence relation for $d_{n,m}$ will be,

$$\boxed{d_{n,m} = d_{n,m-1} + d_{n-1,m} + d_{n-1,m-1}} \tag{18.79}$$

Generating Function:

The generating function for this problem is,

$$\boxed{D(x,y) = \sum_{n,m\geq 0} d_{n,m}.x^n.y^m} \tag{18.80}$$

We can observe that $d_{n,0} = d_{0,m} = 1$.

$$D(x,y) = \sum_{n\geq 0,m=0} d_{n,0}.x^n + \sum_{n=0,m\geq 1} d_{0,m}.y^m + \sum_{n\geq 1,m\geq 1} d_{n,m}.x^n.y^m$$

$$D(x,y) = \sum_{n\geq 0,m=0} 1.x^n + \sum_{n=0,m\geq 1} 1.y^m + \sum_{n\geq 1,m\geq 1} d_{n,m}.x^n.y^m$$

We know that,

$$\sum_{n\geq 0} x^n = \frac{1}{1-x}$$

$$D(x,y) = \frac{1}{1-x} + \sum_{n=0,m\geq 1} y^m + \sum_{n\geq 1,m\geq 1} d_{n,m}.x^n.y^m$$

$$D(x,y) = \frac{1}{1-x} + y.\sum_{n=0,m\geq 1} y^{m-1} + \sum_{n\geq 1,m\geq 1} d_{n,m}.x^n.y^m$$

Let $(m-1) = h$,

$$D(x,y) = \frac{1}{1-x} + y.\sum_{n=0,h=0} y^h + \sum_{n\geq 1,m\geq 1} d_{n,m}.x^n.y^m$$

After renaming the variables,

$$D(x,y) = \frac{1}{1-x} + y.\sum_{n=0,m=0} y^m + \sum_{n\geq 1,m\geq 1} d_{n,m}.x^n.y^m$$

$$D(x,y) = \frac{1}{1-x} + y.\left(\frac{1}{1-y}\right) + \sum_{n\geq 1,m\geq 1} d_{n,m}.x^n.y^m$$

Using the recurrence relation from equation (18.81),

$$D(x,y) = \frac{1}{1-x} + \frac{y}{1-y} + \sum_{n\geq 1,m\geq 1} (d_{n,m-1} + d_{n-1,m} + d_{n-1,m-1}).x^n.y^m$$

$$D(x,y) = \frac{1}{1-x} + \frac{y}{1-y} + \sum_{n\geq 1,m\geq 1} d_{n,m-1} + \sum_{n\geq 1,m\geq 1} d_{n-1,m} + \sum_{n\geq 1,m\geq 1} d_{n-1,m-1}.x^n.y^m$$

$$D(x,y) = \frac{1}{1-x} + \frac{y}{1-y} + x.y.\sum_{n\geq 1,m\geq 1} d_{n-1,m-1}.x^{n-1}.y^{m-1} + \sum_{n\geq 1,m\geq 1} d_{n,m-1} + \sum_{n\geq 1,m\geq 1} d_{n-1,m}$$

Let $(n-1) = h \; and \; (m-1) = p$,

$$D(x,y) = \frac{1}{1-x} + \frac{y}{1-y} + x.y.\sum_{h\geq 0,p\geq 0} d_{h,p}.x^h.y^p + \sum_{n\geq 1,m\geq 1} d_{n,m-1} + \sum_{n\geq 1,m\geq 1} d_{n-1,m}$$

After renaming the variables,

$$D(x,y) = \frac{1}{1-x} + \frac{y}{1-y} + x.y.\sum_{n\geq 0,m\geq 0} d_{n,m}.x^n.y^m + \sum_{n\geq 1,m\geq 1} d_{n,m-1}.x^n.y^m + \sum_{n\geq 1,m\geq 1} d_{n-1,m}.x^n.y^m$$

From the equation (18.82),

$$D(x,y) = \frac{1}{1-x} + \frac{y}{1-y} + x.y.D(x,y) + \sum_{n\geq 1,m\geq 1} d_{n-1,m}.x^n.y^m + \sum_{n\geq 1,m\geq 1} d_{n,m-1}.x^n.y^m \quad (18.81)$$

Consider the fourth term in the above equation,

$$\sum_{n\geq 1,m\geq 1} d_{n-1,m}.x^n.y^m = x.\sum_{n\geq 1,m\geq 1} d_{n-1,m}.x^{n-1}.y^m$$

Let $(n-1) = h$

$$x.\sum_{n\geq 1,m\geq 1} d_{n-1,m}.x^{n-1}.y^m = x.\sum_{h\geq 0,m\geq 1} d_{h,m}.x^h.y^m$$

After renaming the variables,

$$x.\sum_{h\geq 0,m\geq 1} d_{h,m}.x^h.y^m = x.\sum_{n\geq 0,m\geq 1} d_{n,m}.x^n.y^m$$

$$x.\sum_{n\geq 0,m\geq 1} d_{n,m}.x^n.y^m = x.\left(\sum_{n\geq 0,m\geq 0} d_{n,m}.x^n.y^m - \sum_{n\geq 0,m=0} d_{n,0}.x^n\right)$$

$$x.\left(\sum_{n\geq 0,m\geq 0} d_{n,m}.x^n.y^m - \sum_{n\geq 0,m=0} d_{n,0}.x^n\right) = x.\left(D(x,y) - \frac{1}{1-x}\right)$$

Substituting the above value in the equation (18.83),then

$$D(x,y) = \frac{1}{1-x} + \frac{y}{1-y} + x.y.D(x,y) + x.\left(D(x,y) - \frac{1}{1-x}\right) + \sum_{n\geq 1, m\geq 1} d_{n,m-1}.x^n.y^m$$

After rearranging the terms,

$$D(x,y) = 1 + \frac{y}{1-y} + x.y.D(x,y) + x.D(x,y) + \sum_{n\geq 1, m\geq 1} d_{n,m-1}.x^n.y^m \tag{18.82}$$

Consider the last term of the above equation,

$$\sum_{n\geq 1, m\geq 1} d_{n,m-1}.x^n.y^m = y.\sum_{n\geq 1, m\geq 1} d_{n,m-1}.x^n.y^{m-1}$$

Let $p = (m-1)$,then

$$y.\sum_{n\geq 1, m\geq 1} d_{n,m-1}.x^n.y^{m-1} = y.\sum_{n\geq 1, p\geq 0} d_{n,p}.x^n.y^p$$

After renaming the variables,

$$y.\sum_{n\geq 1, m\geq 0} d_{n,m}.x^n.y^m = y.\left(\sum_{n\geq 0, m\geq 0} d_{n,m}.x^n.y^m - \sum_{n=0, m\geq 0} d_{0,m}.y^m\right)$$

$$y.\left(\sum_{n\geq 0, m\geq 0} d_{n,m}.x^n.y^m - \sum_{n=0, m\geq 0} d_{0,m}.y^m\right) = y.\left(D(x,y) - \frac{1}{1-y}\right)$$

Substitute the above value in the equation (18.84),

$$D(x,y) = 1 + \frac{y}{1-y} + x.y.D(x,y) + x.D(x,y) + y.\left(D(x,y) - \frac{1}{1-y}\right)$$

$$D(x,y) = 1 + x.y.D(x,y) + x.D(x,y) + y.D(x,y)$$

After rearranging the terms,

$$D(x,y) = \frac{1}{1-x-y-xy}$$

$$D(x,y) = \left(\frac{1}{1-y}\right).\left(\frac{1}{1-\left(\frac{1+y}{1-y}\right).x}\right)$$

We know that,

$$\frac{1}{1-a.x} = \sum_{n\geq 0} a^n.x^n$$

$$D(x,y) = \left(\frac{1}{1-y}\right).\left(\sum_{n\geq 0}\left(\frac{1+y}{1-y}\right)^n.x^n\right)$$

The generating function is,

$$\boxed{D(x,y) = \left(\sum_{n\geq 0}\frac{(1+y)^n}{(1-y)^{n+1}}.x^n\right)} \tag{18.83}$$

The required number $d_{n,m}$ is,

$$d_{n,m} \;=\; Coefficient\ of\ x^n.y^m\ in\ D(x,y)$$

$$d_{n,m} \;=\; Coefficient\ of\ y^m\ in\ \frac{(1+y)^n}{(1-y)^{n+1}}$$

$$d_{n,m} \;=\; Coefficient\ of\ y^m\ in\ (1+y)^n.\left(\frac{1}{1-y}.\frac{1}{1-y}.\ldots.(n+1)times\right)$$

We know that,

$$\frac{1}{1-y} = 1+y+y^2+\ldots$$

$$d_{n,m} \;=\; Coefficient\ of\ y^m\ in\ (1+y)^n.\left((1+y+y^2+\ldots).(1+y+y^2+\ldots).\ldots.(n+1)times\right)$$

Let's say that a number $k \geq 0$ is taken, such that the term along with its coefficient y^k comes from $(1+y)^n$ and the remaining term along with its coefficient y^{m-k} comes from the (n+1) term product.

The coefficient of y^k in $(1+y)^n$ is $\binom{n}{k}$.

Let $c_1, c_2, \ldots, c_{n+1}$ be the degrees of x from the (n+1)-term product.

Finding out the coefficient of y^{m-k} from the (n+1) term product is equivalent to count the number of ways of picking c_i's such that $c_1 + c_2 + \cdots + c_{n+1} = m-k$

The number of such pickings = $\binom{n+1+m-k-1}{m-k} = \binom{n+m-k}{m-k} = \binom{n+m-k}{n}$.

Therefore, the required number $d_{n,m}$ is,

$$d_{n,m} = \sum_{k \geq 0} \binom{n}{k} . \binom{n+m-k}{n}$$

Hence,

$$\boxed{Delannoy\ Number\ (D) = \sum_{k \geq 0} \binom{n}{k} . \binom{n+m-k}{n}} \tag{18.84}$$

Instructor : Jayalal Sarma
Scribe : Pragnya (*TA:* JS)
Date : Oct 21, 2020
Status : α

Lecture
17

Generating Functions(continued)

17.1 Introduction

In this section we'll see some examples of ordinary generating functions and get introduced to exponential generating functions.

17.1.1 Example 3 :

To show two combinatorial qualities are equal it sufficies to show that they have same generating functions. Consider the following,

$$B_n(m) = \{(x_1, x_2, \ldots x_n) \mid \forall i \; x_i \in \mathbb{Z}, \sum |x_i| \leq m\}$$

let $b_{n,m} = |B_n(m)|$. Let's see properties of $b_{n,m}$:

1. $b_{n,m} = \sum_{k=0}^{n} \binom{n}{k}\binom{m}{k}2^k$.
2. $b_{n,m} = b_{m,n}$. This can also be proved using bijection.
3. $b_{n,m} = d_{m,n}$.

We'll prove property 3 by showing they have same generating functions.

$$\begin{aligned}
B_{x,y} &= \sum_{n,m\geq 0} b_{n,m}x^n y^m \\
&= \sum_{n,m\geq 0} (\sum_{k=0}^{n} \binom{n}{k}\binom{m}{k}2^k)x^n y^m \\
&= \sum_{n,m,k\geq 0} \binom{n}{k}\binom{m}{k}2^k x^n y^m \\
&= \sum_{k\geq 0} 2^k \sum_{n,m\geq 0} \binom{n}{k}\binom{m}{k}x^n y^m \\
&= \sum_{k\geq 0} 2^k (\sum_{n\geq 0} \binom{n}{k}x^n)(\sum_{m\geq 0} \binom{m}{k}y^m) \\
B_{x,y} &= \sum_{k\geq 0} 2^k (x^k \sum_{n\geq 0} \binom{n}{k}x^{n-k})(y^k \sum_{m\geq 0} \binom{m}{k}y^{m-k})
\end{aligned}$$

Consider $\frac{1}{(1-x)^{k+1}}$:

$$\frac{1}{(1-x)^{k+1}} = \frac{1}{(1-x)}.\frac{1}{(1-x)}\cdots\frac{1}{(1-x)}\ (k+1\ times)$$

Coefficient of x^{n-k} in $\frac{1}{(1-x)^{k+1}}$ is equivalent to no.of solutions of $a_1+a_2+\cdots+a_{k+1}=n-k$ which is $=\binom{(n-k)+(k+1)-1}{n-k}=\binom{n}{k}$. Hence

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

Similarly

$$\sum_{m\geq 0}\binom{m}{k}y^{m-k} = \frac{1}{(1-y)^{k+1}}$$

Substituting them in the above derived $B_{x,y}$ -

$$\begin{aligned}
B_{x,y} &= \sum_{k\geq 0} 2^k x^k y^k \frac{1}{(1-x)^{k+1}} \frac{1}{(1-y)^{k+1}} \\
&= \sum_{k\geq 0} (2xy)^k \frac{1}{(1-x)^{k+1}} \frac{1}{(1-y)^{k+1}} \\
&= \frac{1}{(1-x)(1-y)} \sum_{k\geq 0} \frac{(2xy)^k}{(1-x)^k (1-y)^k} \\
&= \frac{1}{(1-x)(1-y)} \sum_{k\geq 0} (\frac{(2xy)}{(1-x)(1-y)})^k \\
&= \frac{1}{(1-x)(1-y)} \frac{1}{1-\frac{2xy}{(1-x)(1-y)}} \\
&= \frac{1}{(1-x)(1-y)-2xy} \\
B(x,y) &= \frac{1}{1-x-y-xy} = D(x,y)
\end{aligned}$$

Since $b_{n,m}$ and $d_{n,m}$ have same generating functions, $b_{n,m} = d_{n,m}$. Hence $b_{n,m}$ also satisfies recurrence relation of $d_{n,m}$ -

$$b_{n,m} = b_{n-1,m} + b_{n,m-1} + b_{n-1,m-1}$$

17.1.2 Example 4 : Stirling number of second kind

As discussed in previous lectures, number of ways to partition set $\{1, 2, 3 \dots n\}$ into k non-empty parts is called stirling number of second kind. Let's represent by $S_{n,k}$. It's recurrence relation is given by -

$$S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$$

LHS : number of ways to partition set $\{1, 2, 3 \dots n\}$ into k non-empty parts $= S_{n,k}$
RHS :

1. If element 1 occurs in a singleton set. No.of ways to partition remaining $n-1$ elements to $k-1$ sets $= S_{n-1,k-1}$.

2. If element 1 doesn't occur in a singleton set. Then we can partition remaining $n-1$ elements to k sets and add element 1 to one of these k sets $= kS_{n-1,k}$

We can also see that $S_{0,0} = 1,\ S_{n,0} = 0,\ S_{0,k} = 0.$

$$\begin{aligned}
S(x,y) &= \sum_{n,k\geq 0}^{\infty} S_{n,k} x^n y^k \\
&= S_{0,0}\, x^0 y^0 + \sum_{n=0,k\geq 1}^{\infty} S_{0,k}\, x^0 y^k + \sum_{n\geq 1,k=0}^{\infty} S_{n,0}\, x^n y^0 + \sum_{n\geq 1,k\geq 1}^{\infty} S_{n,k}\, x^n y^k \\
&= 1 + \sum_{n\geq 1,k\geq 1}^{\infty} S_{n,k}\, x^n y^k \\
&= 1 + \sum_{n\geq 1,k\geq 1} S_{n-1,k-1}\, x^n y^k + \sum_{n\geq 1,k\geq 1} k S_{n-1,k}\, x^n y^k \\
&= 1 + xy \sum_{n\geq 1,k\geq 1} S_{n-1,k-1} x^{n-1} y^{k-1} + x \sum_{n\geq 1,k\geq 1} k S_{n-1,k}\, x^{n-1} y^k \\
&= 1 + xy\, S(x,y) + x \sum_{n\geq 0,k\geq 1} k S_{n,k}\, x^n y^k \\
&= 1 + xy\, S(x,y) + \frac{\partial}{\partial y} S(x,y)
\end{aligned}$$

Note : $\frac{\partial}{\partial y} S(x,y) = \sum_{n\geq 0,k\geq 1} k S_{n,k}\, x^n y^{k-1}$

Consider y^k coefficients on both sides :

$$\begin{aligned}
LHS &= \sum_{n\geq 0} S_{n,k} x^n \\
RHS &= x \sum_{n\geq 0} S_{n,k-1} x^n + xk \sum_{n\geq 0} S_{n,k} x^n
\end{aligned} \tag{17.85}$$

Equating LHS and RHS :

$$\begin{aligned}
\sum_{n\geq 0} S_{n,k}\, x^n &= x \sum_{n\geq 0} S_{n,k-1}\, x^n + xk \sum_{n\geq 0} S_{n,k}\, x^n \\
\sum_{n\geq 0} S_{n,k}\, x^n &= \frac{x}{1-xk} \sum_{n\geq 0} S_{n,k-1}\, x^n \\
&= \frac{x}{1-xk} \frac{x}{1-x(k-1)} \sum_{n\geq 0} S_{n,k-2}\, x^n \\
&= \frac{x}{1-xk} \frac{x}{1-x(k-1)} \cdots \frac{x}{1-x(k-(k-1))} \sum_{n\geq 0} S_{n,0}\, x^n \\
&= \frac{x^k}{(1-x)(1-2x)\ldots(1-kx)} \times 1\ (Note : S_{0,0} = 1, S_{n,0} = 0) \\
\sum_{n\geq 0} S_{n,k}\, x^n &= x^k \times \left(\frac{A_1}{1-x} + \frac{A_2}{1-2x} + \cdots + \frac{A_k}{1-kx}\right)
\end{aligned}$$

Solving for $A_1, A_2, \ldots A_k$ we'll get $A_r = (-1)^{k-r} \frac{r^{k-1}}{(r-1)!(k-r)!}$.

$S_{n,k}$ is the coefficient of x^n in RHS. i.e.,

$$\begin{aligned} S_{n,k} &= coeff\ of\ x^n\ in\ x^k \times (\frac{A_1}{1-x} + \frac{A_2}{1-2x} + \cdots + \frac{A_k}{1-kx}) \\ &= coeff\ of\ x^{n-k}\ in\ \sum_{r=1}^{k} \frac{A_r}{1-rx} \end{aligned}$$

Coefficient of x^p in $\frac{1}{1-rx} = r^p$. hence,

$$\begin{aligned} S_{n,k} &= \sum_{r=1}^{k} A_r r^{n-k} \\ &= \sum_{r=1}^{k} (-1)^{k-r} \frac{r^{k-1}}{(r-1)!(k-r)!}\ r^{n-k} \\ S_{n,k} &= \sum_{r=1}^{k} (-1)^{k-r} \frac{r^n}{(r-1)!(k-r)!} \end{aligned}$$

The above expression is Stirling number of second kind

17.2 Exponential generating functions

In ordinary generating functions we associate sequence, $(a_n)_{n\geq 0}$ with $G(x) = \sum_{n\geq 0} a_n x^n$. In $G(x)$ we chose basis $\{1, x, x^2, x^3 \dots\}$ for set of all polynomials in one variable. But there are many other basis for set of polynomials, like $\{1, x, x(x-1), x(x-1)(x-2), \dots\}$. We chose basis $\{1, x, x^2, x^3 \dots\}$ because it has combinatorial meaning. Other such meaning full basis are $\{\frac{x^n}{n!}\}_{n\in\mathbb{N}}$, $\{e^{-x}\frac{x^n}{n!}\}_{n\in\mathbb{N}}$ and $\{\frac{1}{n^x}\}_{n\in\mathbb{N}}$. In this lecture we'll explore exponential generating functions which use basis $\{\frac{x^n}{n!}\}_{n\in\mathbb{N}}$. So $(a_n)_{n\geq 0}$ is associated with $E(x) = \sum_{n\geq 0} a_n \frac{x^n}{n!}$. Let's see a few examples -

$$\begin{aligned} (1,1,1,\dots) &\xrightarrow[generating function]{exponential} \sum_{n\geq 0} \frac{x^n}{n!} = e^x \\ &\xrightarrow[generating function]{ordinary} \sum_{n\geq 0} x^n = \frac{1}{1-x} \\ (1!,2!,3!,\dots) &\xrightarrow[generating function]{exponential} \sum_{n\geq 0} n!\frac{x^n}{n!} = \sum_{n\geq 0} x^n = \frac{1}{1-x} \end{aligned}$$

$\frac{1}{1-x}$ is ordinary generating function(ogf) of $(1,1,1,\dots)$ and exponential generating function(egf) of $(1!,2!,3!,\dots)$.

Operations of EGF

1. **Addition :** It's similar to ogf.

$$\{a_n\}_{n\geq 0} \xrightarrow{egf} E(x)$$
$$\{b_n\}_{n\geq 0} \xrightarrow{egf} F(x)$$
$$\{a_n + b_n\}_{n\geq 0} \xrightarrow{egf} E(x) + F(x)$$

2. **Shifting :** Multiplying ogf by x shifts the sequence to left as seen in earlier lectures.

$$\{a_0, a_1, a_2 \dots\} \xrightarrow{egf} E(x)$$
$$\{0, a_0, a_1, a_2 \dots\} \xrightarrow{egf} xE(x)$$

   Differentiating egf function will shift the sequence to right.

$$\{a_0, a_1, a_2 \dots\} \xrightarrow{egf} E(x)$$
$$\{a_1, a_2, a_3 \dots\} \xrightarrow{egf} \frac{d}{dx}E(x)$$
$$\frac{d}{dx}E(x) = \sum_{n\geq 1} a_n \frac{n.x^{n-1}}{n!} = \sum_{n\geq 1} a_n \frac{x^{n-1}}{(n-1)!} = \sum_{n\geq 0} a_{n+1} \frac{x^n}{n!}$$

3. **Multiplication :** EGFs are used if the sequence counts labelled structures like permutations, derangements and partitions. Let $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0}$ count arrangements of type A and type B respectively using n labelled objects. If we want to count type C arrangements, that can be obtained by a unique split of n objects into two sets and then arranging first set according to type A and second set according to type B -
   No.of arrangements of type C of size $n, c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$.

Now Let's see how multiplication of $A(x)$(egf of A) and $B(x)$(egf of B) is useful

$$\begin{aligned}
A(x).B(x) &= (\sum_{n=0}^{\infty} a_n \frac{x^n}{n!})(\sum_{n=0}^{\infty} b_n \frac{x^n}{n!}) \\
&= \sum_{n=0}^{\infty}(\sum_{k=0}^{n} \frac{a_k}{k!}.\frac{b_{n-k}}{(n-k)!})x^n \\
&= \sum_{n=0}^{\infty}(\sum_{k=0}^{n} \frac{n!}{k!(n-k)!}a_k b_{n-k})\frac{x^n}{n!} \\
&= \sum_{n=0}^{\infty}(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k})\frac{x^n}{n!} \\
&= \sum_{n=0}^{\infty} c_n \frac{x^n}{n!} \\
A(x).B(x) &= C(x)
\end{aligned}$$

Now Let's see few examples of egf

17.2.1 Derangements

Recall that we've discussed derangements in PIE and recurrence relations. Now let's derive it using egf. Let D_n represent set of derangements of n objects and let $d_n = |D_n|$. we can see that $d_0 = 1,\ d_1 = 0,\ d_2 = 1$. Recall the recurrence relation :

$$d_{n+2} = (n+1)(d_{n+1} + d_n)$$

$$
\begin{aligned}
D(x) &= \sum_{n=0}^{\infty} d_n \frac{x^n}{n!} \\
D'(x) &= \sum_{n=0}^{\infty} d_{n+1} \frac{x^n}{n!} \ (by\ shifting\ operation) \\
&= \sum_{n=1}^{\infty} n(d_n + d_{n-1}) \frac{x^n}{n!} \\
&= \sum_{n=1}^{\infty} n d_n \frac{x^n}{n!} + \sum_{n=1}^{\infty} n d_{n-1} \frac{x^n}{n!} \\
&= x \sum_{n=1}^{\infty} d_n \frac{x^{n-1}}{(n-1)!} + x \sum_{n=1}^{\infty} d_{n-1} \frac{x^{n-1}}{(n-1)!} \\
&= x \sum_{n=0}^{\infty} d_{n+1} \frac{x^n}{n!} + x \sum_{n=0}^{\infty} d_n \frac{x^n}{n!} \\
D'(x) &= xD'(x) + xD(x) \\
(1-x)D'(x) &= xD(x) \\
\frac{D'(x)}{D(x)} &= \frac{x}{1-x} = \frac{1}{1-x} - 1
\end{aligned}
$$

Integrating on both sides

$$\ln D(x) = \ln(1-x) - x + c$$

Since $D(0) = d_0 = 1 \Rightarrow c = 0$.

$$\ln D(x) = \ln(1-x) - x$$

$$D(x) = \frac{e^{-x}}{1-x} = \sum_{n=0}^{\infty} d_n \frac{x^n}{n!}$$

To get d_n we need coefficient of $\frac{x^n}{n!}$ in LHS.

$$e^{-x} \frac{1}{1-x} = (\sum_{n=0}^{\infty} (-1)^n \frac{x^n}{n!})(\sum_{n=0}^{\infty} n! \frac{x^n}{n!})$$

Coefficient of $\frac{x^n}{n!}$ by multiplication property = $\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$

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

d_n is count of derangements of n objects.

17.2.2 Bell Numbers

Let $S_{n,k}$ represent number of ways of partitioning $\{1, 2, 3 \dots n\}$ into k non empty blocks and B_n represent number of ways of partitioning $\{1, 2, 3 \dots n\}$ ($B_0 = 1$). By definitions,

$$B_n = \sum_{k=0}^{n} S_{n,k}$$

Equivalent intrepretation : Consider a number whose prime factorization is square free i.e., $k \in \mathbb{N}$ such that $k = p_1 p_2 \dots p_n$ where $\{p_1, p_2, \dots p_n\}$ are distinct primes. Number of ways of writing k as product of natural numbers ≥ 2 = number of ways of partitioning $\{p_1, p_2, \dots p_n\}$ $= B_n$.
Recurrence Relation :

$$B_n = \sum_{k=0}^{n-1} \binom{n-1}{k} B_k$$

Let's derive closed form expression for B_n :

$$\begin{aligned}
B(x) &= \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} \\
B'(x) &= \sum_{n=0}^{\infty} B_{n+1} \frac{x^n}{n!} \ (by\ shifting\ rule) \\
&= \sum_{n=0}^{\infty} (\sum_{k=0}^{n} \binom{n}{k} B_k) \frac{x^n}{n!} \\
&= \sum_{n=0}^{\infty} (\sum_{k=0}^{n} \binom{n}{k} . 1 B_k) \frac{x^n}{n!} \\
&= (\sum_{n=0}^{\infty} B_n \frac{x^n}{n!}) (\sum_{n=0}^{\infty} 1 \frac{x^n}{n!}) \ (by\ multiplication\ rule) \\
B'(x) &= B(x).e^x \\
\frac{B'(x)}{B(x)} &= e^x
\end{aligned}$$

Integrating on both sides

$$\ln B(x) = e^x + c$$

Since $B(0) = B_0 = 1 \Rightarrow c = -1$. Hence,

$$
\begin{aligned}
B(x) &= e^{e^x - 1} \\
&= \frac{e^{e^x}}{e} \\
&= \frac{1}{e}(\sum_{k=0}^{\infty} \frac{(e^x)^k}{k!}) \\
&= \frac{1}{e}(\sum_{k=0}^{\infty} \frac{e^{kx}}{k!}) \\
&= \frac{1}{e}(\sum_{k=0}^{\infty} \frac{1}{k!} (\sum_{n=0}^{\infty} \frac{(kx)^n}{n!})) \\
&= \frac{1}{e}(\sum_{n=0}^{\infty} \frac{x^n}{n!} (\sum_{k=0}^{\infty} \frac{k^n}{k!})) \\
B(x) &= \sum_{n=0}^{\infty} \frac{1}{e}(\sum_{k=0}^{\infty} \frac{k^n}{k!}) \frac{x^n}{n!} \\
B_n &= \frac{1}{e}(\sum_{k=0}^{\infty} \frac{k^n}{k!})
\end{aligned}
$$

We've derived closed form expression for bell number. Above expression for B_n is also called as Dobinski's formula.

Instructor : Jayalal Sarma
Scribe : Shivlal Gangesh (*TA:* JS)
Date : Oct 19, 2020
Status : α

Lecture
18

Introduction to Ramsey Numbers

18.1 Introduction

Till now we have seen advanced versions of the discrete mathematics topics we already know. Now we are going to get into Extremal combinatorics. Here we are interested in questions of the form

- *If this structure appears, then what is the minimum/maximum size of the object?*
- *If the size is at least this much , then what kind of structures appear in the object?*
- *What is the minimum size of the collection such that it is guaranteed to have certain property?*

In general we are interested in the extreme behaviors in combinatorics. The classic example we start with is an extension to an example that we have done in the beginning of the course as an Application of Pigeon Hole Principle.

18.2 Starting Point

Theorem 18.2.1. *Six people meet in a party. Then either there exist three people who are friends with each other or there exist three people who are strangers with each other.(Note : Any two people can either be friends or strangers)*

We are interested in proving the above statement. Lets look into two different approaches

18.2.1 Model 1 (Using Cliques and Independent Sets)

Model Let us represent the problem as a 6 vertex graph $G(V, E)$with each person corresponding to a vertex. $(u, v) \in E$ if and only if person u is a friend of person v. In this Model the original statement can be reformulated as

Statement *Any graph on* 6 *vertices must either have a clique on* 3 *vertices or an independent set on* 3 *vertices.*

Proof. Consider any vertex v in the graph G, without loss of generality we can assume that the degree of v is greater than or equal to 3 because suppose it is not the case then consider $\overline{G}$; as Cliques in $G \leftrightarrow$ Independent Sets in $\overline{G}$.
Let the 3 neighbours of v be a, b and c. Consider the two exhaustive cases :

Case 1 : There are no edges among a**,** b **and** c
Here we have $\{a, b, c\}$ as the 3-Independent Set

Case 2 : There is at least one edge among a**,** b **and** c
Let $(a, b) \in E$ be that edge, then we have $\{v, a, b\}$ as the 3-clique

Therefore the given statement holds true. □

Proof for tightness To prove that this is tight we need to show there is a graph with 5 vertices such that it does not have 3-clique and 3-Independent Set. Given below is one such example

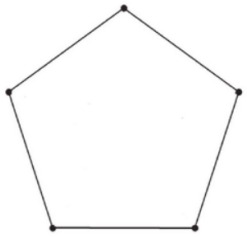


Figure 18.15: 5-vertex graph with no 3-clique and no 3-Independent Set

18.2.2 Model 2 (Using Graph Edge colouring)

Model Let us represent the problem as 2-edge coloring of a K_6 graph with each vertex corresponding to a person. Color the edge (u, v) with *red* if u and v are friends, color it with *blue* if u and v are strangers. In this Model the original statement can be reformulated as

Statement *For any 2-edge colouring of* K_6*, there must exist either a red* K_3 *or a blue* K_3

Proof. Consider any Red,Blue-edge coloring of K_6. Consider any vertex v, the degree of v is 5 as the graph is a complete graph. By Pigeon Hole Principle , v must have either 3 red edges incident on it or 3 blue edges incident on it. Consider the case when v is incident on with 3 red edges. Let the 3 neighbours of v be a, b and c. Now there are 2 cases :

Case 1 : There is no red colored edge among (a, b)**,** (b, c) **and** (c, a)
Then all the three edges (a, b), (b, c) and (c, a) are colored blue. Therefore $\{a, b, c\}$ forms a blue K_3

Case 2 : There is at least one red colored edge among (a, b), (b, c) and (c, a)
Let (a, b) be the red colored edge, then $\{v, a, b\}$ forms a red K_3

Therefore the given statement holds true. □

Proof for tightness To prove that this is tight we need to show there is a 2-edge coloring of K_5 Such that it does not have red K_3 and blue K_3. Given below is one such example

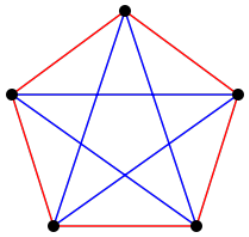


Figure 18.16: 2-edge coloring of K_5 with no red K_3 and no blue K_3

Generalizing the above problem with arbitrary red k_p and blue k_q has been extensively studied by Ramsey and has led to the definition of Ramsey numbers.

18.3 Ramsey numbers

Definition 18.3.1 (Ramsey number)**.** *The Ramsey number denoted by $R(p, q)$ is the minimum number of vertices say n such that any 2-edge coloring of K_n must have either a red K_p or a blue K_q.*
*(**Or equivalently as**)*
The minimum number of vertices (n) such that any graph on n vertices must either have a clique on p vertices or an independent set on q vertices.

18.3.1 Some Observations

Property 18.3.1. $R(3, 3) = 6$

This is the direct formulation of the example we have done previously in 18.2

Property 18.3.2. $R(p, q) = R(q, p)$

The colors *red* and *blue* are just placeholders for two colors, thus swapping the colors will still preserve the Ramsey number property. Therefore $R(p, q) = R(q, p)$.

Property 18.3.3. $\forall l \geq 1 \quad R(l, 1) = 1$

The existence of a blue K_1 is nothing but the presence of single vertex and any graph with a single vertex satisfies this property. Therefore $R(l, 1) = 1$

18.4 Existence of R(p,q)

The Proof for the existence of $R(p, q)$ is due to Erdős–Szekeres. The existence was proved by providing an upper bound as a recurrence relation as follows :

Theorem 18.4.1.

$$\forall p, q \geq 2 \quad R(p, q) \ \leq \ R(p, q-1) + R(p-1, q)$$

Proof. Let us prove this by mathematical induction on n where $n = p + q$.

Idea To show the upper bound for $R(p, q) \leq n$, we must argue that for any 2-edge coloring of K_n there exist a red K_p or blue K_q

Base case $p = q = 2$

$$R(2, 2) \leq R(2, 1) + R(1, 2)$$

$$2 \leq 1 + 1$$

Hence it holds true for the base case.

Induction Hypothesis Assume the recurrence relation is true for $n < l$. Then we need to prove it for $n = l$. Let $n = R(p-1, q) + R(p, q-1)$. Let w be any vertex in G (K_n) and consider any 2 -edge coloring of G. Let H_1 be the subgraph of G formed from the vertices sharing a red-edge with v and H_2 be the the subgraph of G formed from the vertices sharing a blue-edge with v.

Case 1 : There are at least $R(p-1, q)$ many red edges incident on vertex w

H_1 is a complete graph on $R(p-1, q)$ vertices with 2-edge coloring. By definition and Induction Hypothesis we have that there exist a red K_{p-1} or blue K_q in H_1. So in graph G (along with vertex w) there exist a red K_p or blue K_q

Case 2 : There are at least $R(p, q-1)$ blue edges incident on vertex w

H_2 is a complete graph on $R(p, q-1)$ vertices with 2-edge coloring. By definition and Induction Hypothesis we have that there exist a red K_p or blue K_{q-1} in H_2. So in graph G (along with vertex w) there exist a red K_p or blue K_q.

□

Instructor : Jayalal Sarma
Scribe : Shivlal Gangesh & Reetwik Das (*TA:* JS)
Date : Oct 21, 2020
Status : α

Lecture
19

Computing Ramsey Numbers and Multidimensional Ramsey numbers

19.1 Generalizing Ramsey numbers

Definition 19.1.1 (3-dimensional Ramsey numbers)**.** *$R_3(p, q, r)$ is the minimum number n, such that any 3-edge coloring K_n must have either a red K_p or a blue K_q or a green K_r*

Definition 19.1.2 (k-dimensional Ramsey numbers)**.** *$R_k(s_1, s_2, \cdots, s_k)$ is the minimum number of vertices n such that for any k-edge coloring of K_n there must exist an i such that there is a K_{s_i} of colour i*

19.2 Some Observations

Property 19.2.1. $R(2, p) = p$

Proof.

Case1 : $R(2, p) \leq p$

Any 2-coloring of K_p must have either a red K_2 or blue K_p. This is true because either there can exist a red edge (red K_2) or no red edge (blue K_p) in K_p

Case 2 : $R(2, p) \geq p$

There exist a 2-coloring of edges of K_{p-1} such that no red K_2 exists and no blue K_p exists. Coloring all the edges of K_{p-1} with blue will result in no red K_2 and no blue K_p in K_{p-1}

□

Claim 19.2.1.

$$R(p, q) \leq \binom{p+q-2}{p-1}$$

Proof.

$$
\begin{aligned}
R(p,q) &\leq R(p,q-1) + R(p-1,q) && \text{(Erdos-Szekeres recurrence relation)} \\
&\leq \binom{p+(q-1)-2}{p-1} + \binom{p-1+q-2}{p-2} \\
&\leq \binom{p+q-3}{p-1} + \binom{p+q-3}{p-2} \\
&\leq \binom{p+q-2}{p-1} && \left(\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}\right)
\end{aligned}
$$

□

19.3 Explicit Computation of R(3,4)

We don't know the exact values of Ramsey numbers for higher values as their computation becomes very hard. There is this famous saying by Paul Erdos on the difficulty of computing Ramsey numbers that

Paul Erdos on Ramsey numbers

> *"Suppose aliens invade the earth and threaten to obliterate it in a year's time unless human beings can find the Ramsey number for red five and blue five. We could marshal the world's best minds and fastest computers, and within a year we could probably calculate the value. If the aliens demanded the Ramsey number for red six and blue six, however, we would have no choice but to launch a preemptive attack."*

So let us now try to calculate the value of $R(3,4)$.

Claim 19.3.1.

$$R(3,4) = 9$$

Proof. Consider any 2-coloring of K_9 and call it as G. We need to prove that G has either a red K_3 or a blue K_4. Any vertex in G can have it's incident edges as one of the three cases below

- **Case 1 :** There are at least 4 red edges going out of the vertex
- **Case 2 :** There are at least 6 blue edges going out of the vertex
- **Case 3 :** There are exactly 3 red edges and 5 blue edges going out of the vertex

However note that not all vertices in G come under **Case 3** because, if so then the total sum of degrees of all vertices becomes odd which is not possible. So let v be a vertex in G which does not fall under **Case 3**. Then

Case 1 : There are at least 4 red edges going out of v

Let H_1 be the subgraph of G formed from the four vertices which are sharing the red edge

with v. Since we know that $R(2,4) = 4$, H_1 with 4 vertices must have a red K_2 or a blue $K4$, So along with vertex v, G must have a red K_3 or a blue K_4.

Case 2 :There are at least 6 blue edges going out of v

Let H_2 be the subgraph of G formed from the six vertices which are sharing the blue edge with v. Since we know that $R(3,3) = 6$, H_2 with 6 vertices must have a red K_3 or a blue $K3$, So along with vertex v, G must have a red K_3 or a blue K_4.

Proof for tightness

To prove that 9 is tight, we need to show that there is a 2-coloring of K_8 such that it does not have red K_3 or blue K_4. Given below is one such example

Figure 19.17: 2-coloring of K_8 with no red K_3 and no blue K_4

□

As the values p, q increases we can only calculate the range of the Ramsey number. The following is a table with value or range of Ramsey numbers for the first few natural numbers.

p, q	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10
3	1	3	6	9	14	18	23	28	36	40-43
4	1	4	9	18	25	35-41	49-61	56-84	73-115	92-149
5	1	5	14	25	43-49	58-87	80-143	101-216	125-316	143-442
6	1	6	18	35-41	58-87	102-165	113-298	127-495	169-780	179-1171
7	1	7	23	49-61	80-143	113-298	205-540	216-1031	233-1713	298-2826
8	1	8	28	56-84	101-216	127-495	216-1031	282-1870	317-3583	317-6090
9	1	9	36	73-115	125-316	169-780	233-1713	317-3583	565-6588	580-12677
10	1	10	40-43	92-149	143-442	179-1171	289-2826	317-6090	580-12677	798-23556

Figure 19.18: Table for $R(p,q)$

19.4 Multidimentional Ramsey numbers

Definition 19.4.1. *$R_k(S_1, S_2, ..S_k)$ is mininum number n such that any k-edge coloring of K_n must have K_{S_i} of color i for some $i \in \{1, 2..k\}$*

We need to show that why should exist $R_k(S_1, S_2, ..S_k)$.

Claim 19.4.2.

$$R_k(S_1, S_2, ..S_k) \leq R_{k/2}(R(S_1, S_2), R(S_3, S_4)....R(S_{k-1}, S_k))$$

Proof. Let $n = R_{k/2}(R(S_1, S_2), R(S_3, S_4)....R(S_{k-1}, S_k))$
Consider K_n and any K-edge coloring of the edges of K_n

We need to show that $\exists S_1$ clique of color 1 or S_2 clique of color 2.
Consider colors paired up and rename them $\{1, 2\} = 1, \{3, 4\} = 2, ...\{k-1, k\} = k/2$
By the definition of $R_{k/2}$ we are guaranteed $\exists i$ such that $\exists$ a clique of size $R(S_{2i-1}, S_{2i})$ of color i.

After we uninterpret the color i as the original pair of colors we get a 2-coloring of the clique that we have $R(S_{2i-1}, S_{2i})$
By the definition of R_2 we know that $\exists$ a S_{2i-1} clique of color $2i-1$ or S_{2i} clique of color $2i$. □

19.5 Fermat's last theorem

We know from Pythagoras theorem that $x^2 + y^2 = z^2$ has integral solutions. But we want to know if this equation has any integral solutions for any power greater than 2.

Theorem 19.5.1. *$x^n + y^n = z^n$ doesn't have any integral solutions $\forall n > 2$.*

Instructor : Jayalal Sarma
Scribe : Reetwik Das (*TA:* JS)
Date : Oct 22, 2020
Status : α

Lecture
20

Finite fields

20.0.1 Finite fields

$x^n + y^n = z^n$ does have integeral solutions for finite fields such as for Z_p.
$Z_p = \{0, 1, ...p-1\}$ and addition and multiplication are $modulo\ p$ within this field.

Definition 20.0.1. *Z_p^* is a cyclic group $\{1, 2, 3....p-1\}$*

Claim 20.0.2. *If p is a prime then Z_p^* is generated by a single element, and the element is known as the generator.*

Fermat's last theorem is completely algebraic to connect it to coloring we need a tool.

Theorem 20.0.3. ***Schur's theorem :*** *If $r \geq 0$ positive integer then. $\exists$ integer $S(r)$ such that if we color $\{1, 2, ...S(r)\}$ vertices with r colors then $\exists x, y, z$ in the set and $x + y = z$*

Proof. Given an r, Let $S(r) = R_r(3, 3, 3, ...3)$
Consider K_n, $n = S(r)$ by the definition if we color the edges of K_n using r colors then we are guaranteed a monochromatic K_3.
We are given a coloring $\{1, 2, ...S(r)\}$
Define a coloring for edges in K_n.
Associate vertices of K_n with elements in $\{1, 2, ...S(r)\}$
$\forall a, b \in V$ the color of edge (a, b) = color of $|a - b|$

Let $\{\alpha, \beta, \gamma\}$ be the vertices of the monochromatic triangle. Let $x = \alpha - \beta$, $y = \beta - \gamma$ and $z = \alpha - \gamma$ then x, y, z have the same color. It also satifies the equation $x + y = z$.

□

Theorem 20.0.4. *$\forall m \exists q$ such that $\forall p \geq q$ in Z_p (p is a prime)*
$x^m + y^m = z^m$ has a solution.

Proof. Given m from $x^m + y^m = z^m$
$p = q = S(m) + 1$ by Schur's theorem any coloring of $\{1, 2...q\}$ must have a triplet $a + b = c$.
$Z_p = 0, 1, 2...q - 1$
Let g be the generator of Z_p then every non-zero element in $Z_p = g^k$ for some k.

Assign the coloring $\{1, 2...q\}$ as follows :
$\forall x \in Z_p^*, x = g^{mi+j}$ and $color(x) = j = k(mod m)$

By Schur's theorem, $\exists a, b, c$ such that $a + b = c$ and all have the same color.

$$g^{mi_a+j} + g^{mi_b+j} = g^{mi_c+j}$$

$$(g^{i_a})^m + (g^{i_b})^m = (g^{i_c})^m$$

and we have the solution for $x^m + y^m = z^m$. □

20.0.2 Lower bounds for Ramsey numbers

Claim 20.0.5.

$$\forall k, R(k, k) > 2^{k/2}$$

Proof. Suffices to show that $n = 2^{k/2}$, $\exists$ a 2-coloring of the edges of K_n such that there is no monochromatic K_k in it.

Fix $m = 2^{k/2}$ there are $\binom{n}{2}$ many edges.
A coloring is said to be bad if $\exists$ no monochromatic K_k in it.

Probabilistic method :
For every edge, assign red/blue color with probability $1/2$ each.
if we show that the probability[coloring is bad]> 0 then this means $\exists$ a bad coloring.

Suffices to show that the Pr[coloring is good] < 1
Pr[$\exists K_k$ which is monochromatic] $\leq \Sigma_{S \subseteq K_k, |S|=k}$ Pr[S is monochromatic]
$= \binom{n}{k}$ Pr[S is monochromatic]

$$= \binom{n}{k} \frac{2}{2^{\binom{k}{2}}}$$

$$= \binom{n}{k} 2^{1-\binom{k}{2}}$$

$$= \frac{n(n-1)...(n-k+1)}{k!} \frac{2^{1+k/2}}{2^{k^2/2}}$$

$$\leq \frac{n^k}{k!} \frac{2^{1+k/2}}{2^{k^2/2}}$$

$$= \frac{2^{1+k/2}}{k!} < 1$$

□

Instructor : Jayalal Sarma
Scribe : Praharsh Allada (*TA:* JS)
Date : Oct 26, 2020
Status : α

Lecture
23

Extremal Problems In Graphs-Three Proofs,Mantels Theorem

23.1 Introduction

This week we are going to look at some extremal problems in graphs.The techniques we use to Solve the problems are more important than the problems themselves.In fact we will look at multiple ways of proving the same statement using different techniques to prove.

23.2 Some Examples

Example 1:-
Suppose an Undirected Graph G ,does not have triangle(no k_3), what is the maximum number of edges the graph G can have?
(OR)
What is the minimum number of edges that a graph G with n vertices should have so that it always contains at least 1 triangle?
Solution:-
The graph can be divided Into 2 sets of vertices of size $\frac{n}{2}$ and from all the possible edges from one set to another.In this case we put in $\frac{n^2}{4}$ edges.(From a little thought and AM$\geq$GM we can see that the highest number of edges are produced when each set contains $\frac{n}{2}$ vertices).The answer to the question is this the best we can do is yes,this is the best that we can do, we can not have more than $\frac{n^2}{4}$ edges with no triangle in the graph.

23.3 Mantel's theorem

Theorem 23.3.1. *Any graph G on n vertices having more than $\frac{n^2}{4}$ edges must contain a triangle*

Proof. Let us prove Mantel's theorem using three simple techniques and shifting argument.Let us look at the three different techniques in this lecture and then look at shifting argument in the

next.Later let us also look at generalisation of Mantel's theorem.The three techniques we will be using are double counting argument(we will be using cauchy schwarz inequality),Arithmetic Mean-Geometric Mean Inequality,An application of P.H.P.

Proof1:-Double Counting argument

We define a mathematical quantity and find its upper and lower bound using two different methods thus calculating an inequality for the parameters involved.

Let m be the number of edges in a graph G that does not have any triangles we have to show that $m \leq \frac{n^2}{4}$

Let, x,y $\in$ V and G contains the edge between x and y the x and y cannot have an edge with a common vertex.(i.e, adjacent vertices can not have common neighbours). In other words d(x)+d(y)$\leq$ n (Since,they cannot have any other common neighbours d(x)+d(y) $\leq$ n-2 without counting edge (x,y) and then we add 2 for the edge (x,y))

Now the quantity we are going to double count is $\sum_{x \in V} d(x)^2$ First let us find the Upper bound for this.Now the above quantity can be thought as d(x) being summed d(X) times

$$\Rightarrow \sum_{x \in V} d(x)^2 = \sum_{(x,y) \in E} (d(x) + d(y)) \leq m * n(Since, \sum_{(x,y) \in E} \leq n)$$

Now we will calculate the lower bound on the above quantity in terms of m so that the upper and lower bounds to gather w=might give us a bound on m Now for this let us first take a look at cauchy schwarz inequality.

Theorem 23.3.2. ***cauchy schwarz inequality:-***

let u,v $\in R^n$,$< u, v >= \sum_{i=1}^{n} u_i * v_i$, $||u|| = < u, u >= \sum_{i=1}^{n} u_i^2$

$$| < u, v > |^2 \leq ||u|| * ||v||$$

$$i.e, (\sum_{i=1}^{n} u_i * v_i)^2 \leq (\sum_{i=1}^{n} u_i^2)(\sum_{i=1}^{n} v_i^2)$$

Proof. let us assume $u \neq 0$ and $\lambda \in \mathbb{R}$

$0 \leq < \lambda u - v, \lambda u - v >= \lambda^2 < u, u > -\lambda < u, v > -\lambda < v, u > + < v, v >$

$= \lambda^2 < u, u > -2\lambda < u, v > + < v, v >$

Choose $\lambda = \frac{<u,v>}{<u,u>}$ substituting in the equation yields

$$\frac{< u, v >^2}{< u, u >} - 2\frac{< u, v >^2}{< u, u >} + < v, v > \geq 0$$

$$\Rightarrow < u, v >^2 \leq < u, u >< v, v >$$

□

Now let us use the cauchy schwarz inequality to obtain the lower bound. Let $V = x_1, x_2, ...x_n$ *now let us define* $u = (d(x_1), d(x_2), ...d(x_n), v = (1, 1, 1, ..., 1)$

$u_i v_i = d(x_i)$

$\Rightarrow \sum(u_i * v_i)^2 = (\sum d(x))^2 \Rightarrow \sum(d(x)^2) \geq \frac{(\sum d(x)^2)}{n} = \frac{(2m)^2}{n} = \frac{4m^2}{n} \Rightarrow \frac{4m^2}{n} \leq mn \Rightarrow m \leq \frac{n^2}{4}$

Proof 2:- AM-GM Inequality

Neighbours of any vertex x ∈ V can not have any edges among themselves.(i.e, they must form an independent set). Let A be the largest independent set in the graph, then we have $\forall x$ d(x) $\leq |A|$ .If we consider B=V-A then every edge has at least one end point in B(since we can not have edges between the vertices of A from definition).Sets such as B are vertex covers.If A is the largest Independent Set then B is the smallest vertex cover.Anyway, $|E| \leq \sum_{x \in B} d(x) \leq |B| * |A| \leq (\frac{|A|+|B|}{2})^2 = \frac{n^2}{4}$

Proof 3:- Using P.H.P

Let us consider a graph with 2*n vertices and every such graph with more than $n^2 + 1$ edges must have a triangle.

Let us prove by Induction on n,

Base case (n=1)

If 2 vertex graph has $1^2 + 1 = 2$ vertices has edges from A to B and B to A making it a triangle with a 0 edge as the 3rd side

Induction step

Assume it is true for n=k and try to prove for n=k+1, number of vertices =2*(k+1)=2k+2 and the number of edges =$(k + 1)^2 + 1 = k^2 + 2k + 2$ Now let us consider an edge (x,y) ∈ E and call the remaining graph and the edges among themselves as H.

Case1:-

If H has more than $k^2 + 1$ edges then since we know that the statement is true for k by induction and now since H has a triangle G also has a triangle and hence the statement is true for n=k+1

Case2:-

If H has less than $k^2 + 1$ edges therefore number of edges between the vertices x,y to H are total edges-(edges in H)-edge (x,y)$\geq (k + 1)^2 + 1 - k^2 - 1 = 2k + 1$.Now if we consider each of the vertex in H as a Hole and the number of pigeons in a given hole as number of edges it has with vertices x,y now since there are 2n holes (2k vertices in H) and at least 2k+1 pigeons (each pigeon represents a distinct edge) there exists a hole with more than 1 pigeon which means there exists a vertex with more than one edge to x,y which makes it a common neighbour to both x and y (making (x,z) ∈ E and (y,z) ∈ E)thus forming a triangle and hence the statement is true for k+1

conclusion any graph with 2*n vertices and more than $n^2 + 1$ edges must have a triangle for all values of n. □

Instructor : Jayalal Sarma
Scribe : Praharsh Allada (*TA:* JS)
Date : Oct 28, 2020
Status : α

Lecture
24

The Shifting technique

24.1 Introduction

In the last lecture we have seen 3 different techniques for mantel's theorem based on Double counting,AM-GM Inequality and Pigeon Hole principle.In this lecture we are going to look at a new technique to prove the existence of things in general.This technique is based on a principle called averaging principle which is like a cousin to pigeon hole principle.

24.2 proving existence using shifting technique

Averaging Principle The averaging principle states that every set of numbers contain at least one number which is as large as the average and one number which is as small as the average .
To Prove some Good object exist
* Assign weights to objects such that Objects with large weights are good
* Show that the average weight is large enough for it to be a good object and hence there exists at least one object with as much weight as average and hence proved that at least one good object exists
Shifting would be used in computing the sum and finding the average.

24.3 Some examples using Shifting technique

Example 1:-
Let $n \leq m \leq 2n$ where m is the number of pigeons and n is number of hole.For any distribution where no hole is left empty there can be at most 2*(m-n) pigeons which are happy (Happy pigeons are not alone)
Proof
let us try to maximise the number of happy pigeon,consider any distribution of pigeons such that

no hole is empty.if some hole contains grater than 2 pigeons then shift one of the pigeons from that hole to another hole with an unhappy pigeon.(thus increasing the number of happy pigeons by 1).Therefore the distribution which maximises the number of happy pigeons must necessarily have less than or equal to 2 pigeons in each hole.which naturally gives the configuration which can be obtained bu putting one pigeon in each hole and then putting the remaining (m-n) pigeons in different holes thus making the total number of happy pigeons per filled hole as 2 and thus making the maximum number of happy pigeons as 2*(m-n)

Example2:-

Graham and kleitman Trail of a graph is a walk in a graph without repeating edges.If the edges of a complete graph k_n is labelled with distinct numbers $1, 2, 3, ..., \binom{n}{2}$,with no repetition then there is a trail of length n-1 with an increasing sequence of edge labels.

For n=3, take a triangle ABC let us try to label the edges to avoid a trail of length 2 (n-1=2). If AB=1, in both the cases of BC=2 and CA=2 we will clearly have a trail of increasing edge labels.

For n=4, take a square ABCD with diagonals AC and BD and label the edges from 1 to 6 by trying to avoid 3 length trails of increasing length let us start with BD=1 and AC=2 to keep it disconnected then AD=3 because where ever we put 3 tail length will increase by 1 DC cant be 4 because ADCA will form a trail of length 3 and also AB cant be 4 because in that case BCAB will from a trail of length 3 hence let us put BD=4.But now we cant get put CD=5 since CBDC will form a trail of length 3 with increasing labels and also we cant put AB=5 since ACBA will form a trail of length 3 with increasing labels hence a trail of length 3 with increasing labels is unavoidable.

Proof

We assign a weight to each vertex,x $\in$ v $- >$ W_x is it's weight.Where W_x is the length of the longest increasing trail ending at x.Now, it suffices to argue $\exists x \in V$,such that $W_x \geq n-1$. Now we have to find argue the average weight,if we prove $\frac{1}{n}\sum_{x\in V} W_x \geq n-1$ the by averaging principle we have show the existence.This is equivalent to proving $\sum_{x\in V} W_x \geq n*(n-1)$.Shifting algorithm is problem dependent so in this case let us consider building the graph by adding edges one after the other.Let us add the edges in the order of increasing labels which keeps modifying the weights of vertices. Initially $W_x = 0 \forall x$ we add edges in the increasing label order.

At some later instant let us say (x,y) is the edge being added now.So already some edges have been added so let us say there is a path ending at x and y the length of which is the weight of x and y respectively. SO now we update $W_x and W_y$.

Case1:- if $W_x = W_y$ and all the already existing edges have smaller labels since edges are added in that order. Increase both $W_x and W_y by 1.W'_x = W_x + 1 and W'_y = W_y + 1$

Case2:- if $W_x < W_y$ since now edge (x,y) is present the trail previously ending at y plus the edge (x,y) forms a new trail of length $W_y + 1 > W_x$ ending at x and hence $W'_x = W_y + 1 and W'_y = W_y$

Case3:- if $W_x > W_y$ since now edge (x,y) is present the trail previously ending at x plus the edge (x,y) forms a new trail of length $W_x + 1 > W_y$ ending at y and hence $W'_y = W_x + 1$ and $W'_x = W_x$

Observation

The value of $W_x + W_y$ increase by 2 in case one and in case 2 it increased by $W_y - W_x + 1$ and in case 3 it increased by $W_x - W_y + 1$ which are grater than or equal to 2 therefore for each edge added the value of $\sum_{x \in V} W_x$ increased by at least 2. Therefore by the time we add $\binom{n}{2}$ edges the value of $\sum_{x \in V} W_x \geq 2 * \binom{n}{2} \geq n * (n-1)$.Hence,Graham and kleitman has been proved

Instructor : Jayalal Sarma
Scribe : Venkat Nikhil Kotagiri (*TA:* JS)
Date : Oct 29, 2020
Status : α

Lecture
25

Fourth Proof of Mantels Theorem, Turans Theorem

25.1 Introduction

In previous lectures, we have seen three different proofs of Mantel's theorem. In this lecture we will see a fourth proof using *shifting method*.

25.2 Proof of Mantel's theorem using shifting method

Theorem 25.2.1. *Any simple graph with $2n$ vertices and $\geq n^2 + 1$ edges must have a triangle.*

Proof. Let G be a simple graph on $2n$ vertices with no triangles.Let m be number of edges in G. It suffices to prove that $m \leq n^2$.

Shifting argument includes assignment of weights to objects, and shifting those weight to maximize/minimize an objective function. The weights assignment, constraints we chose are problem dependent.

In this proof, for each vertex $x \in V$, we'll assign a weight $w_x \in [0, 1]$, such that $\sum_{x \in V} w_x = 1$.
Let $S = \sum_{(x,y) \in E} w_x w_y$ and S_{max} be the max value of S.
Consider the weight assignment in which every vertex is assigned equal weight, i.e.,
$w_x = \frac{1}{2n}, \forall x \in V$
Value of S in this case is

$$S = \sum_{(x,y) \in E} w_x w_y$$
$$S = \sum_{(x,y) \in E} \frac{1}{4n^2}$$
$$S = \frac{m}{2n^2} \qquad (\textit{each edge is counted twice})$$

Therefore, lower bound for S_{max} is $\frac{m}{2n^2}$,i.e.,

$$S_{max} \geq \frac{m}{2n^2} \tag{25.86}$$

We'll now use shifting argument to prove that $S_{max} \leq \frac{1}{2}$. Consider two vertices $x, y \in V$ such that $(x, y) \notin E$. Let Γ_x denote the sum of weights of neighbours of x, and Γ_y denote the sum of weights of neighbours of y. $\Gamma_x = \sum_{(x,z)\in E} w_z, \Gamma_y = \sum_{(y,z)\in E} w_z$. The contribution of w_x towards S is $w_x \sum_{(x,z)\in E} w_z = w_x\Gamma_x$. Similarly the contribution of w_y towards S is $w_y\Gamma_y$.

Without loss of generality assume that $\Gamma_x \geq \Gamma_y$, then by shifting a small weight ϵ from y to x, the change in S is equal to

$$= ((w_x + \epsilon)\Gamma_x + (w_y - \epsilon)\Gamma_y) - (w_x\Gamma_x + w_y\Gamma_y) \quad = \epsilon(\Gamma_x - \Gamma_y) \geq 0 \qquad (\textit{since } \epsilon \geq 0 \textit{ and } \Gamma_x \geq \Gamma_y)$$

Therefore, by shifting ϵ weight from w_y to w_x, we have not decreased the value of S.

Claim 25.2.2. *Max S is achieved when the weight is concentrated on a edge.*

Proof. Using the above argument,we can keep shifting the weight from vertex y to vertex x until w_y becomes zero,without decreasing S. Repeat this $\forall u, v \in V$ satisfying $(u, v) \notin E, w_u > 0, w_v > 0$. Now, for two vertices u, v, if $w_u > 0$ and $w_y > 0$ then the edge (u, v) must be present in E. Therefore the weight is concentrated on a clique. □

Using the above claim, and using the fact that G is triangle free, we can conclude that the total weight is concentrated over a single edge (say (x,y)).

$$\begin{aligned} S_{max} &\leq max\{w_x w_y + w_y w_x | (x, y) \in E, w_x + w_y = 1\} \\ S_{max} &\leq \frac{1}{4} + \frac{1}{4} \\ S_{max} &\leq \frac{1}{2} \ ^{4} \end{aligned}$$

Therefore using equation (25.88),

$$\begin{aligned} \frac{m}{2n^2} \leq S_{max} &\leq \frac{1}{2} \\ \frac{m}{2n^2} &\leq \frac{1}{2} \\ m &\leq n^2 \end{aligned}$$

□

[4] $S_{max} = \frac{1}{2}$ if the graph contains at least one edge, otherwise $S_{max} = 0$.

25.3 Generalization of Mantel's Theorem: Turán's theorem

In this section we will see a generalization of Mantel's theorem, called Turán's theorem.

Theorem 25.3.1. *If a simple graph $G = (V, E)$ with n vertices has no k-cliques, the $|E| \leq (1 - \frac{1}{k-1})\frac{n^2}{2}$*

Proof. We will restate the theorem as follows: If G has no (k+1)-clique then $|E| \leq (1 - \frac{1}{k})\frac{n^2}{2}$.
We will use induction on number of vertices n.
Induction hypothesis: Assume that the threorem is true $\forall n^{'} < n$.

Consider G that has max number of edges but still does not have a (k+1)-clique. Then G must have a k-clique.Let $A \subseteq V, |A| = k$, be a k-clique in G. Let $B = V \setminus A$. Let E_A, E_B, E_{AB} denote the edges in A, edges in B, edges across AB respectively. Clearly E_A, E_B, E_{AB} is a partition of E. Therefore, we can write,

$$|E| = |E_A| + |E_B| + |E_{AB}|$$

Since A is a k-clique, $E_A = \binom{k}{2}$
Estimating $|E_{AB}|$:

If a vertex u in B is connected to all the vertices in A, then $A \cup u$ is (k+1)-clique, which is a contradiction. Therefore every vertex in B is connected to at-most $k-1$ vertices in A. Therefore, $|E_{AB}| \leq |B|(k-1) = (n-k)(k-1)$.
Estimating $|E_B|$:

Since B is simple graph which does not have (k+1)-cliques, we can use the induction hypothesis to estimate E_B. $E_B \leq (1 - \frac{1}{k})\frac{(n-k)^2}{2}$
Therefore,

$$|E| \leq \binom{k}{2} + (n-k)(k-1) + (1 - \frac{1}{k})\frac{(n-k)^2}{2}$$
$$|E| \leq (1 - \frac{1}{k})\frac{n^2}{2}$$

□

25.4 Complementary of Turán's theorem

For a simple graph G, let $\alpha(G)$ be the maximum number of pairwise non-adjacent vertices of G. If G has n vertices and $\frac{nk}{2}$ edges then, $\alpha(G) \leq \frac{n}{k+1}$.

We will prove this by using *probabilistic method*.
Before that, we will do a quick recap of probability.

25.5 Recap of probability

The set of all possible outcomes is called sample space(Ω). Events are subsets of sample space. The probability distribution assigns values in Ω to $[0, 1]$, such that $\sum_{x \in \Omega} p(x) = 1$.

Random variable: Random variable(X) is function that assigns real values to elements in the sample space.

$$X : \Omega \to \mathsf{R}$$

Expected value of a Random variable: The expected value of X, where X is a random variable, is the weighted average of the possible values that X can take, each value being weighted according to the probability of that event occurring.

$$E[X] = \sum_{w \in \Omega} p(w)X(w)$$

Linearity of Expectation:
If X_1, X_2 are random variables such that $X_1, X_2 : \Omega \to \mathsf{R}$, then

$$E[c_1X_1 + c_2X_2] = c_1E[X_1] + c_2E[X_2]$$

One way to interpret averaging argument is that,

$$\exists w \in \Omega \ \textit{ such that } \ X(w) \geq E[X]$$

25.6 Expection Method, Independence Number

In this lecture, we will use expectation method to prove the complementary of Turán's theorem discussed in the previous lecture. Before that, let's see an example on how to use expectation method.

Statement: $\exists$ graph G that has n vertices and at least 3 connected components.

Let each edge (x, y) be present with probability p and be absent with probability $1 - p$. This is called random graph model.

The sample space $\Omega =$ set of all graphs with n vertices. Consider a random variable X, which maps an element G in Ω to number of components in G,i.e, $X(G) =$ number of components in G.

To prove that there exists a graph with at least 3 connected components, we need to prove that $E(X) \geq 3$.

25.7 Complementary of Turán's theorem

Theorem 25.7.1. *Let G be a graph on n vertices and let d_i denote the degree of the i^{th} vertex. Let $\alpha(G)$ be the Independence number (cardinality of the largest independent set) of G. Then $\alpha(G) \geq \sum_{i=1}^{n} \frac{1}{d_i+1}$*

Our earlier statement is slightly different from the above theorem.
Statement: If G has n vertices and $\frac{nk}{2}$ edges then $\alpha(G) \geq \frac{n}{k+1}$

Claim 25.7.2. *This statement can be derived from the above theorem.*

Proof. The theorem states that

$$\alpha(G) \geq \sum_{i=1}^{n} \frac{1}{d_i + 1} \tag{25.87}$$

Let $d_i = k \; \forall 1 \leq i \leq n$, Then number of edges= $\frac{1}{2} \sum_{i=1}^{n} d_i = \frac{nk}{2}$.
Using equation (26.89),

$$\alpha(G) \geq \sum_{i=1}^{n} \frac{1}{d_i + 1}$$
$$\alpha(G) \geq \sum_{i=1}^{n} \frac{1}{k + 1}$$
$$\alpha(G) \geq \frac{n}{k+1}$$

□

We will now prove the above theorem.

Proof. Before moving forward with the proof, let's recall the recipe of a proof using expectation method

- Set up an experiment
- Relate the quantity that we want to expectation
- Bound expectation

Setting up the experiment:
Let $V = \{1, 2, \ldots, n\}$, let $\pi : V \to V$ be a permutation of V.
Experiment: Chose a permutation uniformly at random.

Relating the required quantity to expectation:
Let A_i be the event that all neighbours j of vertex i are greater than i in the ordering,i.e., $\forall j : (i, j) \in E, \pi(j) > \pi(i)$
Probability of event A_i happening is $Pr(A_i) = \binom{n}{d_i+1} \frac{d_i!(n-d_i-1)!}{n!}$.

Idea: If for x,y, A_x and A_y holds then $(x, y) \notin E$.

Aim: To show that $\exists u \subseteq V$ such that $|u| \geq \sum_{i=1}^{n} \frac{1}{d_i+1}$, and for no vertex inside u, the event holds.

Using the expectation method, let U be the set of vertices i such that A_i holds.

Define random variable, $X_i = \begin{cases} 1 & \text{if } A_i \text{ holds} \\ 0 & \text{otherwise} \end{cases}$

$$\begin{aligned}
E[|U|] &= E[X_1 + X_2 + \ldots, X_n] \\
&= \sum_{i=1}^{n} E[X_i] \\
&= \sum_{i=1}^{n} \sum_{w \in \Omega} X_i(w) Pr(w) \\
&= \sum_{i=1}^{n} 0.pr[X_i == 0] + 1.pr[X_i == 1] \\
&= \sum_{i=1}^{n} Pr[A_i] \\
&= \sum_{i=1}^{n} \binom{n}{d_i + 1} \frac{d_i!(n - d_i - 1)}{n!} \\
&= \sum_{i=1}^{n} \frac{n!}{(d_i + 1)!(n - d_i - 1)!} \frac{d_i!(n - d_i - 1)!}{n!} \\
&= \sum_{i=1}^{n} \frac{1}{d_i + 1}
\end{aligned}$$

So, there must exist $u \subseteq V$ such that, $|u| \geq \sum_{i=1}^{n} \frac{1}{d_i+1}$ and $\forall x \in u$, the event A_x happens for a permutation. That implies $\exists$ an independent set $|u| \geq \sum_{i=1}^{n} \frac{1}{d_i+1}$. Therefore

$$\alpha(G) \geq \sum_{i=1}^{n} \frac{1}{d_i + 1}$$

□

Instructor : Jayalal Sarma
Scribe : Sampriti Roy (*TA:* JS)
Date : Nov 2, 2020
Status : α

Lecture
24

Algebraic Methods in Combinatorics

24.1 Introduction

In this chapter the plan is to switch to algebraic methods in combinatorics and the first structure we are going to explore is the concepts related to group theory. It's essentially going to be presented from the combinatorial side. As, a motivation we can think of the following problems:

- *How many distinct squares can be there with yellow and blue coloured corners?*

Our task is to develop a method to count distinct colourings of such squares out of total $2^4 = 16$ possible colourings. If we consider the set of all coloured squares to be Ω, there will be some squares that are equivalent to each other under some rotation. As, we are interested in counting distinct colouring, the equivalent squares should not be counted twice.

One more question, we can think about is :

- *How many necklaces can be formed with solid beads and transparent beads?*

Based on the colouring of square, we can say that there are total $2^4 = 16$ possible colourings but there are few operations under which two colourings can be viewed as same. Let's get familiar with such operations:

- R_0 : Rotation by 0°
- R_{90} : Rotation by 90°
- R_{180} : Rotation by 180°
- R_{270} : Rotation by 270°
- H : Horizontal flip
- V : Vertical flip

- D : Diagonal flip (bottom left top right)
- D' : Diagonal flip (bottom right top left)

Now, let's consider all the above set of operations together to be :

$$G = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

We will see that the elements of set G are inter related with each other. If we apply two operations from G, one after another, we will get the result of applying an operation from G itself. Let's verify it:

- Rotate the square two times horizontally, it will result rotating it by $0°$. That is $H.H = R_0$
- Rotate the square two times diagonally, it will result rotating it by $0°$. That is $D.D = R_0$
- Rotate the square two times vertically, it will result rotating it by $0°$. That is $V.V = R_0$
- Rotate the square two times by $180°$, it will result rotating it by $0°$. That is $R_{180}.R_{180} = R_0$
- Rotate the square by $90°$ first then rotate it by $180°$, it will result rotating by $270°$. That is $R_{90}R_{180} = R_{270}$
- Rotate the square by $90°$ first then rotate it by $270°$, it will result rotating by $0°$. That is $R_{90}R_{270} = R_0$
- Rotate the square by $90°$ first then rotate it vertically, it will result rotating diagonally. That is $R_{90}.V = D$

24.2 Incremental definition of Group

Consider a set G with binary operation $\circ$. Now, take any two elements of G and apply the operation, a natural question to ask is whether we will get any element from the set G or not. We will answer this question along with other related questions and finally move on to the definition of Group incrementally.

- *Groupoid* : Let $a, b \in G$. If $a \circ b \in G$, then G is *Closed* under the operation $\circ$. And G is called *Groupoid*. We can easily verify that our example set G is a *Groupiod*.
- *Semigroup* : $a, b, c \in G$; if $a \circ (b \circ c) = (a \circ b) \circ c$, then G is *associative* under $\circ$ or, the order of $\circ$ does not matter. If a groupoid is associative, it is called *Semigroup*. We can try out and check that our example set G is associative and so it is a *Semigroup*.
- *Monoid* : $\forall a \in G$, if there is an $e \in G$ such that $a \circ e = e \circ a \forall$, e is called identity element. A Semigoup with identity is called *Monoid*. In our example set G, R_0 is the identity element, so it is a *Monoid*.

- *Group* : $\forall a \in G$ if $\exists b \in G$ such that $a \circ b = b \circ a = e$; where e is identity element, b is called the *inverse* of a. A Monoid with inverse element is called a *Group*. In our example set G, R_{180} is it's own inverse, H is it's own inverse and we can try out that every element has it's inverse and so it is a *Group*.

Hence, we can conclude that $G = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ is not just a set, rather it has more structural properties. $(G, \circ)$ is a *Group*. Now, we are ready to define *Group* formally.

Definition 24.2.1. *$(G, \circ)$ is a group if it satisfies closure, associativity and it has identity and inverse element.*

Example1 : Let's consider $\mathbb{Z}_p = \{0, 1, ..., p-1\}$ where p is a prime number. Define the operation to be $+ \ mod \ p$. Let's verify whether $(\mathbb{Z}_p, + \ mod \ p)$ is a group or not:

- *Closure* : $\forall a, b \in \mathbb{Z}_p; a + \ mod \ p \in \mathbb{Z}_p$. So, $\mathbb{Z}_p$ is closed under the operation $+ \ mod \ p$
- *Associativity* : As modulo arithmetic is associative, $\mathbb{Z}_p$ is associative under $+ \ mod \ p$
- *Identity* : 0 is the identity element for all elements in $\mathbb{Z}_p$.
- *Inverse* : For any element $a \in \mathbb{Z}_p$, $(p - a)$ will be the inverse of a.

Hence, $(\mathbb{Z}_p, + \ mod \ p)$ is a group.

Let's check whether $(\mathbb{Z}_p, \times \ mod \ p)$ is group or not:

- *Closure* : $\forall a, b \in \mathbb{Z}_p; a \times \ mod \ p \in \mathbb{Z}_p$. So, $\mathbb{Z}_p$ is closed under the operation $\times \ mod \ p$
- *Associativity* : As modulo arithmetic is associative, $\mathbb{Z}_p$ is associative under $\times \ mod \ p$
- *Identity* : 1 is the identity element for all elements in $\mathbb{Z}_p$
- *Inverse* : The element 0 does not have any inverse.

Hence, $(\mathbb{Z}_p, \times \ mod \ p)$ is not a group but it is a *Monoid*.

Consider the group $\mathbb{Z}_p^*$ under the operation $\times \ mod \ p$; for example we can verify that $(\mathbb{Z}_p^*, \times \ mod \ p)$ satisfies closure, associativity, identity and inverse properties. Hence, $(\mathbb{Z}_p^*, \times \ mod \ p)$ is a group.
Exercise : Use *pigeon hole principle* to prove that every element has it's inverse in $(\mathbb{Z}_p^*, \times \ mod \ p)$.

Example2 : Set of bijection from $\{1, 2, ..., n\}$ to $\{1, 2, ..., n\}$ forms a group under composition $(\circ)$.

- *Closure* : Composition of two bijections is bijection
- *Associative* : Using function composition property, if f, g, h are functions, $f \circ (g \circ h) = (f \circ g) \circ h$

- *Identity* : Identity function will be there
- *Inverse* : Every element will have inverse

Hence, set of bijections $(S_n, \circ)$ forms a group.

24.3 Group (abstractly)

So far, we have seen the definition of a group G, under some operation $\circ$. Now, we will move on the definition of *Subgroup*.

Definition 24.3.1. *Let $(G, \circ)$ be a group. $H \subseteq G$ is said to be a subgroup if H forms a group by itself with respect to the same operation $\circ$. A subgroup of G is denoted by $H \leq G$.*

Example : $(\mathbb{Z}_{15}, + \ mod\ 15)$ is a group. Consider $H = \{0, 3, 6, 9, 12\}$. $H \subseteq G$ and H satisfies closure, associativity, identity, inverse and so it forms a group under $+ \ mod\ 15$, so $H \leq G$.

24.3.1 Subgroup

Consider a group G and $H \leq G$. Let's take an element g from $G \setminus H$ and multiply it with H, define:

$$Hg = \{hg | h \in H\} \tag{24.88}$$

Observation 24.3.2. *If $g \in H$; then $Hg \subseteq H$ as H is closed by itself.*

It's not just $Hg \subseteq H$; something more is true. For that, we will have the following claim

Claim 24.3.3. *$|Hg| = |H|$ when $g \in H$*

Proof. $\forall h_1 \neq h_2 \in H$, we need to argue that $h_1 g \neq h_2 g$. Or multiplication by g is actually a bijection.
Let's prove it by contradiction and let $\forall h_1 \neq h_2 \in H$

$$\begin{aligned} h_1 g &= h_2 g \\ h_1 &= h_2 g g^{-1} \\ h_1 &= h_2 \end{aligned}$$

Hence, we get a contradiction. So, $h_1 g \neq h_2 g$ □

Now, let's move on to the following claim

Claim 24.3.4. *$\forall g_1, g_2$; if $Hg_1 \cap Hg_2 \neq \emptyset$; then $Hg_1 = Hg_2$. In other words, if Hg_1 and Hg_2 are overlapping, then they are same.*

Proof. Let $g_1, g_2 \in G$. Suppose $g \in Hg_1 \cap Hg_2$

$$\exists h \in H; g = hg_1$$
$$\exists h' \in H; g = h'g_2$$

Now, combining the above two,

$$hg_1 = h'g_2$$
$$g_1 = h^{-1}h'g_2$$

Now, we are ready to prove $Hg_1 \subseteq Hg_2$
Consider, any element in LHS $h'' \in H$, substituting g_1, we get:

$$h''g_1 = h''h^{-1}h'g_2$$
$$= h'''g_2$$

Hence, any element in LHS is in RHS. Similarly, we can prove $Hg_2 \subseteq Hg_1$. So, $Hg_1 = Hg_2$. □

So, we can argue that the multiplication of H by other elements will result in translation of H which are kind of tiling of group G. It does not mean that every g_i will give different tiles, but if they have common element, they are same. One interesting feature is that all such tiles will have equal size. One natural question is can there be any element that is not in any tiling? Yes, there can be. For example, $\forall g \in G, g \in Hg$ because H contains identity as it is subgroup. So,g is an element of Hg always. So, every element g will be there in some tile for sure. If there are total k tiles, we argue that:

$$|G| = k.|H|$$

Theorem 24.3.5. *Lagrange's Theorem : The size of a subgroup $|H$ must divide the size of a group $|G|$.*

For example, A group of size 100 can not have a subgroup of size 99. In fact it can only have subgroup of size at most 50. Any group with prime number of elements, can not have any non-trivial subgroup. So, *Lagrange's Theorem* is the example of algebraic structure implying combinatorial bounds.

Instructor : Jayalal Sarma
Scribe : Sampriti Roy (*TA:* JS)
Date : Nov 4, 2020
Status : α

Lecture
25

A step towards Polya's Theory

25.1 A quick recap

In last lecture, we started with a problem of counting number of distinct colourings when the corner of a square are coloured with 2 colours. We defined a set $G = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ that acts on set of all possible 2-coloured squares and some of them are equivalent under these operations. We have also talked about the definition of subgroup (H) of a group (G) and defined that for $g \in G \setminus H$, $Hg = \{hg : h \in H\}$. This Hg is called *coset* of H in G. We have also seen that if any two cosets overlap, they have to be same. We have also talked about *Lagrange's Theorem*. In this chapter the plan is to understand *Polya's Theory*. We will complete it only in next lecture but we will do a step towards it. The step is known to be *Burnside's Lemma*.

25.2 The abstract problem of counting distinct 2-coloured squares

Ω be the set of all 2-coloured squares. There $|\Omega| = 2^4 = 16$ possibilities. Our task is to count to number of distinct colourings among Ω. Let's define the equivalence between two coloured squares formally:

Definition 25.2.1. *Let $\alpha, \beta \in \Omega$, if $\exists g \in G$ such that the action on g on α returns β, or $\alpha^g = \beta$; then we say α and β are equivalent, $\alpha \sim \beta$.*

The relation $\sim$ between α and β satisfies the following properties:

- *Reflexive* : $\alpha \sim \alpha$
- *Symmetric* : $\alpha \sim \beta \rightarrow \beta \sim \alpha$; if the action of g makes the transformation from α to β, then g^{-1} will make the transformation from β to α. For example, R_{90} transform α to β, R_{270} will transform β to α.
- *Transitive* : If $\alpha \sim \beta$ by the action g_1, $\beta \sim \gamma$ by the action g_2; then the action of $g_1 g_2$ (composition of g_1, g_2) will transform $\alpha \sim \gamma$.

Hence, $\sim$ is an equivalence relation and it splits the set Ω into set of equivalence classes.

25.2.1 Orbit and Stabilizer

The action of g on Ω, partitions Ω into different equivalence classes but their sizes need not be equal. This equivalence classes are called *Orbit*. In our context, among set of all possible 2-colourings of a square, we don't want to count equivalent squares twice. In other words, the abstract problem that we are interested to study is to count the number of orbits of Ω. First, we are going to study the sizes of the orbits and using them we will have a mechanism to count them. Let's define the following

Definition 25.2.2. *$Orbit_G(\alpha)$ = orbit of α under the action of G on Ω*

$$Orbit_G(\alpha) = \{\beta : \exists g \in G \; s.t \; \alpha^g = \beta\}$$

Now, we are ready to define *Stabilizer* of α on an action of G. Let, $g \in G$ is acting on Ω. Let $\alpha \in G$, which are the elements in G that fixes α? i.e, the elements in G that takes α to itself.

Definition 25.2.3. *Stabilizer of an element α is a subset of G, which acts on α and takes it back to itself.*

$$Stab_G(\alpha) = \{g \in G : \alpha^g = \alpha\}$$

We will see few examples of stabilizer to make it more clear.

- *Example 1* : A simple example we can think of in our square setting is that, let α be the square where all the corners are coloured yellow. Now, we can easily conclude that any operation from the group G can fix α, i.e, no matter which action we are performing, α will be α itself. So, the stabilizer of α is the entire group G.
- *Example 2* : Let's think of another α where bottom left and top right corners are coloured blue and the other two are coloured yellow. Now, we can verify that the operations that fixes α are : $\{R_0, R_{180}, D, D'\}$.

An interesting observation is that stabilizers inside G are not only subset of G, they are actually subgroup of G. Let's prove the argument formally,

Claim 25.2.4.

$$Stab_G(\alpha) \leq G$$

Proof. Fix an α and verify the following :

- *Closure* : If $g_1, g_2 \in Stab_G(\alpha)$, then $g_1 g_2 \in Stab_G(\alpha)$. As, g_1, g_2 are fixing α, then their composition will also fix α.
- *Associativity* : As the operations performed are subset of G, associativity is inherited in $Stab_G(\alpha)$.

- *Identity* : Identity fixes every element, in particular it fixes α. So, identity element is present in $Stab_G(\alpha)$.
- *Inverse* : If an element g fixes α, then g^{-1} will also fix α. So, inverse element is always present in $Stab_G(\alpha)$. For example, if R_{90} fixes a coloured square, then R_{270} will also fix the same square.

Hence, $Stab_G(\alpha) \leq G$ □

There is a combinatorially useful relation between size of the stabilizer and the size of the of α. Let's define the following lemma;

Lemma 25.2.5. ***Orbit-Stabilizer Lemma*** *:*

$$\forall \in \Omega; |Orbit_G(\alpha)|.|Stab_G(\alpha)| = |G|$$

We will prove this lemma formally in next lecture, but here we are going to draw a outline of the thought process to prove this lemma.

Proof Idea : Let $Stab_G(\alpha)$ be denoted by H. We have already proved that $Stab_G(\alpha)$ is a subgroup of G. Using *Lagrange's theorem* we can say that

$$|G| = k.|Stab_G(\alpha)|$$

Where k is the number of cosets H in G. So, it is sufficient to prove that number of cosets H in G is exactly $|Orbit_G(\alpha)|$. We will show a bijection that for every element in the orbit of α, there is a way to associate a corresponding coset with it. Hence, the number of coset in $Stab_G(\alpha) = |Orbit_G(\alpha)|$. Now, we will quickly define the bijection:

Consider any $\beta \in Orbit(\alpha)$; it means $\exists g \in G$ s.t. $\alpha^g = \beta$. Now, coset corresponding to g is Hg. We required to show the following:

- *Well definedness* : There could be many $g \in G$ which makes α to β. We need to argue that no matter which $g \in G$ we choose, we will end up by getting the coset Hg.
- *Injection* : For $\beta \neq \beta' \in Orbit(\alpha)$; there is $g, g' \in G$ where $\alpha^g = \beta, \alpha^{g'} = \beta'$; we will end up by getting two different cosets, i.e., $Hg \neq Hg'$.
- *Surjection* : To show that for any coset we have corresponding element in the orbit of α.

An interesting observation we can make from the above lemma is that if the size of a group is any prime number then either $|Stab_G(\alpha)|$ is same as $|G|$ and $|Orbit_G(\alpha)| = 1$ or $|Stab_G(\alpha)| = 1$ and $|Orbit_G(\alpha)|$ is same as $|G|$. But, we are not interested in individual sizes of orbits but we want to count the number of orbits. We will use the *Orbit-Stabilizer lemma* to define the following lemma

to show that if we have a handle on the size of orbits then we can have a handle on the number on number of orbits as well. First, we will define the following:

Definition 25.2.6. ***Fix Points*** *: If G is acting on Ω, fix points of a group element are those elements on Ω that are fixed by g.*

$$fix(g) = \{\alpha \in \Omega : \alpha^g = \alpha\}$$

Now, we are ready to state the following lemma:

Lemma 25.2.7. ***Burnsides Lemma*** *:*

$$\#of\ orbits\ = \frac{1}{|G|}\sum_{g\in G}|fix(g)|$$

Proof. The proof is a classic proof by double counting method. Let's define the set

$$S = \{(g, \alpha) : g \in G, \alpha \in \Omega; \alpha^g = \alpha\}$$

We will estimate $|S|$ in two different ways:

- Answer 1 : For each g count number of different α that are fixed by g.

$$\begin{aligned}&\sum_{g\in G}(\#of\ \alpha\ s.t\ \alpha^g = \alpha)\\ &= \sum_{g\in G}|fix(g)|\end{aligned}$$

- Answer 2 : For each $\alpha \in \Omega$, count number of different g that fixes α.

$$\begin{aligned}&\sum_{\alpha\in\Omega}(\#of\ g\ s.t\ \alpha^g = \alpha)\\ &= \sum_{\alpha\in\Omega}|Stab_G(\alpha)|\\ &= \sum_{\alpha\in\Omega}\frac{|G|}{|Orbit_G(\alpha)|}\\ &= |G|.\sum_{\alpha\in\Omega}\frac{1}{|Orbit_G(\alpha)|}\end{aligned}$$

Let us consider the orbits of Ω are denoted by $\{\Omega_1, \Omega_2, ...\}$. Then the above expression be-

comes,

$$= |G|.(\sum_{\alpha \in \Omega_1} \frac{1}{|\Omega_1|} + \sum_{\alpha \in \Omega_2} \frac{1}{|\Omega_2|})$$
$$= |G|.(\#of\ orbits)$$

Equating Answer 1 and 2, we get:

$$|G|.(\#of\ orbits) = \sum_{g \in G} |fix(g)|$$
$$\#of\ orbits = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$$

□

25.3 Counting number of distinct coloured square using Bernsides Lemma

We we apply Bernsides lemma to our example problem to count number of distinct coloured squares in Ω. For that, first we have to compute $|fix(g)|$ for each $g \in G$. Where $G = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$.

- $g = R_0$; all the coloured squares in Ω are fixed by g. So, $|fix(R_0)| = |\Omega| = 16$
- $g = R_{90}$; the squares whose all corners are either blue or yellow will be fixed by g. So, $|fix(R_{90})| = 2$
- $g = R_{180}$; total 4 squares will be fixed by g. So, $|fix(R_{180})| = 4$
- $g = R_{270}$; the number of squares that will be fixed are same as R_{90}. Because, if a square is fixed by R_{90}, it will be fixed by it's inverse as well. So, $|fix(R_{270})| = 2$
- $g = H$; it will fix the squares where the upper half and lower half corresponding to the horizontal plane (line towards the middle of the square) will be coloured with same colour. so, $|fix(H)| = 4$
- $g = V$; the number of squares will be same as that are fixed by H. so, $|fix(V)| = 4$
- $g = D$; consider one diagonal and corresponding to it the upper half and lower half will be coloured with same colour, there are 2 ways to do it and for each such colour the diagonal can be coloured in 4 ways. So, $|fix(D)| = 8$
- $g = D'$; the number of squares will be same as that are fixed by D. So, $|fix(D')| = 8$

Using Bernsides lemma,

$$\begin{aligned} \#of\ orbits\ in\ \Omega &= \frac{1}{8}(16+2+4+2+4+4+8+8) \\ &= 6 \end{aligned}$$

So, out of the 16 total colourings 6 of them are in-equivalent to each other. To simulate the thought process, here is an exercise: *Exercise* : Consider all 2-coloured squares and the set of operations that are acting on it are defined by $G' = \{R_0, R_{90}, R_{180}, R_{270}\}$, i.e. we are not worried about the H, V, D, D' rotations. Under this operations count the number of distinct 2-coloured squares.

Instructor : Jayalal Sarma
Scribe : Achyuth Prakash (*TA:* JS)
Date : Nov 11, 2020
Status : α

Lecture
26

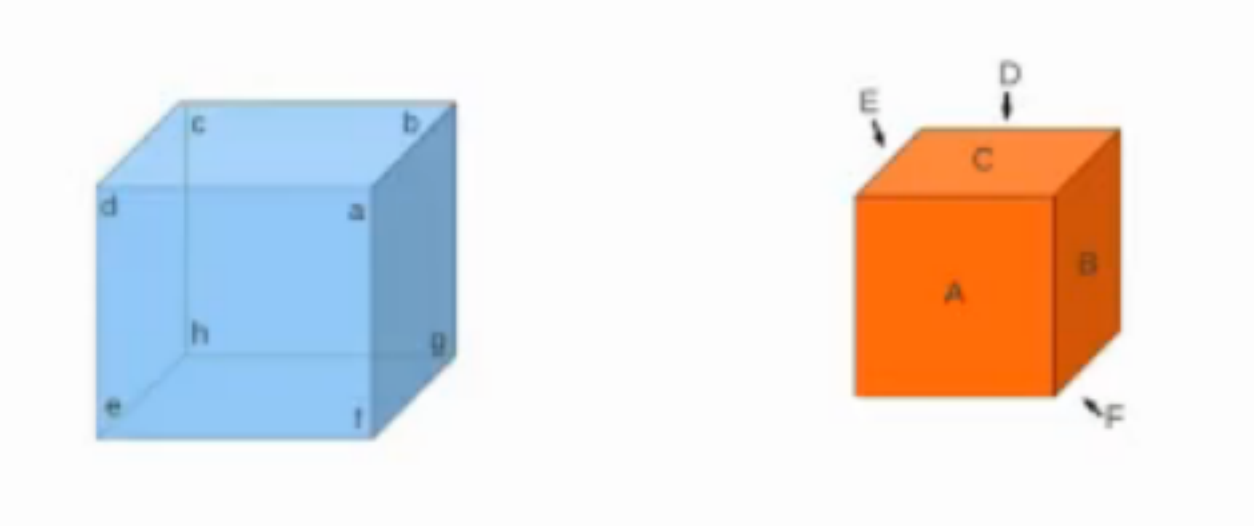
Another step towards Polya's Theory

26.1 A quick recap

In last lecture, we defined and proved the orbit-stabilizer lemma and Lagrange's theorem. In this chapter the plan is to better understand *Polya's Theory* by going through a further example.

26.2 Example 2: Coloring faces of a cube

Let us consider coloring the faces of a cube with 2 colors. As before we define, Ω as the set of all possible colorings. There are 6 faces, and each can can be colored with 2 colors, thus we have $|\Omega| = 2^6 = 64$.
Next we define the set of 'operations', G which can act on elements on Ω. What are the different possible operations? We list them and simultaneously compute $|fix(g)|$:
Here is the labelled cube for reference:



The different operations are:

- R_0 : Rotation by $0°$, i.e. identity. Since all elements of Ω when acted upon by R_0 give back the same element, we get $|fix(g)| = 64$.

- R_1 : Rotation by $180°$ w.r.t axis through the center of the opposite faces. (Observe that there are 3 pairs of such faces). Now consider 2 such faces, A, D. If we rotate the cube as per R_1, how many elements of Ω remain unchanged?
  Consider the faces A, D. They can be colored with any color each. Thus, there are $2 * 2 = 4$ choices. Now, for the other faces, consider C, F. These 2 must be colored with the the same color(because they exchange places) Thus there are 2 choices for C, F together. Similarly for B, E. Thus in total, there are $2^4 = 16$ elements which belong to $fix(g)$.

- R_2 : Rotation by $90°$ w.r.t axis through the center of the opposite faces. Observe that there are 3 pairs of such faces. Again let us compute $|fix(g)|$.
  Consider the faces A, D. They can be colored with any color each. Thus, there are $2 * 2 = 4$ choices. Now, for the other faces, they all must be colored with the same color, because, $C \to B$, $B \to F$, $F \to E$, and $E \to C$. Thus, there are 2 choices for B, C, E, F together. Hence, $|fix(g)| = 2^3 = 8$.

- R_3 : Rotation by $270°$ w.r.t axis through the center of the opposite faces. Observe that there are 3 pairs of such faces. Let us compute $|fix(g)|$.
  Since this is the exact opposite of the previous case, by symmetry, $|fix(g)| = 8$.

- R_4 : Rotation by $180°$ w.r.t axis through the midpoints of opposite edges. Observe that there are 6 pairs of such edges, i.e. (de, bg), (af, ch), (ad, hg), (cb, ef), (ab, eh), (cd, fg). To compute $|fix(g)|$,
  Suppose we do the rotation w.r.t the edges (de, bg). then observe that, now F is now the top face, and A occupies the place where E was initially, similarly, B and D swap places. Thus there are 2 choices together for C, F, 2 choices for A, E and 2 for B, D, giving 8 choices overall. Thus, $|fix(g)| = 8$.

- D : Diagonal flip by $120°$ w.r.t axis through the centers of opposite corners. First, note that there are 4 pairs of opposite corners. To compute $|fix(g)|$,
  Consider the vertex b. If we flip the cube along b by $120°$, then the face $B \to C$, i.e. B now occupies the initial position of C, $C \to D$ and $D \to B$. Thus together, for B, C, D there are 2 choices. Similarly for A, E, F. Thus totally we get $2 * 2 = 4$ possibilities, and $|fix(g)| = 4$.

- D' : Diagonal flip by $240°$ w.r.t axis through the centers of opposite corners. First, note that there are 4 pairs of opposite corners. To compute $|fix(g)|$,
  By symmetry, this is the opposite/complementary operation of the previous one, i.e. flip by $240°$ = flip by $120°$ in the other direction. Thus, $|fix(g)| = 4$.

Thus totally there are $1 + 3 * 3 + 6 + 4 * 2 = 24$ operations in G.

Now, if we apply the formula to calculate the number of orbits, we get:

$$\#of\ orbits\ in\ \Omega = \frac{1}{24}(64 + 3 * 16 + 3 * 8 + 3 * 8 + 6 * 8 + 4 * 4 + 4 * 4) = 10$$

Therefore, we observe that out of the 64 colorings, 10 of them are in-equivalent.

26.3 Cycle Index

We now introduce and define the notion of cycle indices. Let G be the set of some permutations on Ω. Let us decompose $g \in G$ into a collection of disjoint cycles.
For example, let $n = 5$. Consider the permutation $3, 1, 2, 5, 4$ we write this as $(1, 2, 3)\ (4, 5)$, i.e. this denotes $1 \to 2$, (i.e. 1 goes to position 2), $2 \to 3, 3 \to 1$ and so on.
Similarly, the identity permutation, $1, 2, 3, 4, 5$ would be written as $(1)(2)(3)(4)(5)$.

Definition 26.3.1. ***Type of permutation*** *π : A permuatation π is said to be of type $(b_1, b_2, \ldots b_m)$ if b_i represents the number of i length cycles in the cycle representation of π.*

For example if $\pi = (1, 2, 3)\ (4, 5)$ then it is of type $(0, 1, 1, 0, 0)$, because there are no 1 length cycles, $\Rightarrow b_1 = 0$, one 2 length cycle, i.e. $4 \to 5 \to 4 \Rightarrow b_2 = 1$, and one 3 length cycle.

Now, corresponding to type $(b_1, b_2, \ldots b_m)$ consider the monomial $x_1^{b_1}\ x_2^{b_2} \ldots x_m^{b_m}$. Using these terms we define a polynomial as follows:

Definition 26.3.2. *Cycle index polynomial of G:*

$$P(x_1, x_2, \ldots x_m) = \frac{1}{|G|} \sum_{g \in G} x_1^{b_1}\ x_2^{b_2} \ldots x_m^{b_m}$$

where $(b_1, b_2, \ldots b_m)$ is the cycle type of g.
We observe that the above polynomial generalises the Burnside's lemma because we can now substitute the number of possible colors say 2 in place of $x_1, x_2, \ldots x_m$. Thus, this theorem is much more versatile.

Instructor : Jayalal Sarma
Scribe : Achyuth Prakash (*TA:* JS)
Date : Nov 12, 2020
Status : α

Lecture
27

Polya's Theory - Part 1

27.1 Quick Recap

In the last lecture, we went through another example(of coloring the faces of a cube) and defined the cycle index polynomial of G.
Consider an example: Let G be a group such that $G = \{e, (1,2),\ (3,4),\ (1,2)(3,4)\} \leq S_4$ i.e., G is a subgroup of S_4.
Thus, let us write down the cycle index polynomial of G:

$$P(x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + x_1^2x_2 + x_1^2x_2 + x_2^2)$$

We get the RHS because e has 4 length 1 cycles, thus we get the x_1^4 term, $(1,2)$ has 2 length 1 cycles and 1 length 2 cycle, thus the term $x_1^2x_2$ and so on.

27.2 Polya's Theorem - version 1

Theorem 27.2.1. *Polya's theorem: Let G be the group of symmetry acting on Ω, then, if the number of distinct colored patterns with k colors = N, we have*

$$N = P_G(k, k, k, \ldots k)$$

, or $N = P(x_1, x_2, \ldots x_m)$ with $x_1 = x_2 = \ldots x_m = k$.

Proof. Let the domain size be $= m$. (Here by domain we mean the number of different objects we need to color. For example in the squares example, we had 4 corners and thus $m = 4$, similarly in the cube example, we had six faces to color, hence $m = 6$.) Then, the value of $|\Omega|$ will be k^m.
By Burnside's lemma, WKT,

$$Number\ of\ distinct\ colorings\ = Number\ of\ different\ orbits\ of\ G = \frac{1}{|G|}\sum_{g \in G} |fix(g)|$$

Let us thus compute $|fix(g)|$ for $g \in G$.
An example will make this more clear, before we generalize. Consider the previously discussed example of coloring the vertices of a square with 2 colors. Then, we can think of each operation $g \in G$ as a permutation. Consider the operation of rotating a square by $90°$, we can represent this by the cycle index $(1, 2, 3, 4)$, because $1 \to 2,\ 2 \to 3, \ldots$. Similarly, the operation of vertical flip corresponds to $(1, 2)\ (3, 4)$. Consider this operation. Since $1 \to 2$ and $2 \to 1$, we observe that for g to fix some element of Ω, the corners $1, 2$ must get the same color and corners $3, 4$ must get the same color. Thus there are k choices for $1, 2$ together and k choices for $3, 4$ and thus, totally k^2 colorings which are fixed by g.
In general, let the cycle structure of $g = (b_1, b_2, \ldots b_m)$. This means, g has b_1 cycles of length 1, b_2 cycles of length 2, and so on. Now, observe that all the elements that are part of a cycle must receive the same color, if g were to fix the particular coloring. Thus for each cycle of length i, there are k choices and as there are b_i cycles of length i, there are k^{b_i} choices for all of them. Thus,

$$the\ number\ of\ colorings\ fixed\ by\ g\ = k^{b_1} * k^{b_2} \ldots k^{b_m}$$

i.e. $|fix(g)| = x_1^{b_1} * x_2^{b_2} \ldots x_m^{b_m}$ with $x_1 = x_2 = \ldots x_m = k$. Thus,

$$P_G(k, k, k, \ldots k) = \frac{1}{|G|} \sum_{g \in G} (k^{b_1} * k^{b_2} \ldots k^{b_m}) = \frac{1}{|G|} \sum_{g \in G} |fix(g)|$$

Hence proved. □

27.3 Applying Polya's Theorem

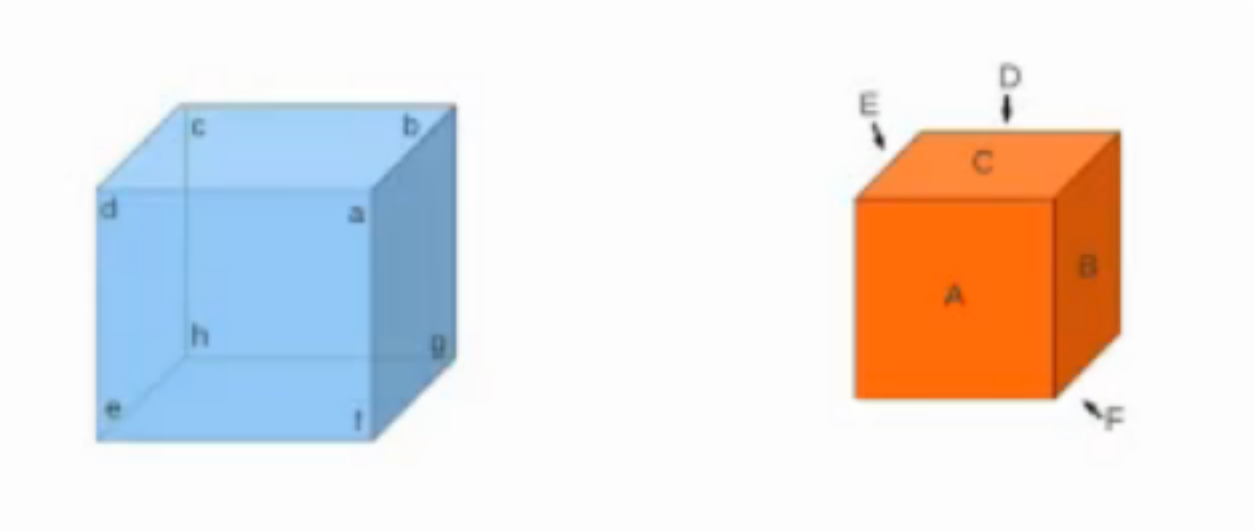
We now consider some examples and apply Polya's theorem for a more concrete understanding.

27.3.1 Example 1 - Coloring Necklaces with circular beads

Consider a necklace with 3 circular beads. We label the beads as $1, 2, 3$. First we ask: what are the possible symmetries? We get $G = \{e, R_{120}, R_{240}, F_{12}, F_{23}, F_{31}\}$, i.e. e is the identity, R_{120} represents a $120°$ clockwise rotation through the center, F_{12} represents flipping w.r.t the edge $1 - 2$, etc. Now let us represent each $g \in G$ as a cycle index permutation. Then we get that $G = \{(1)(2)(3), (1, 2, 3), (1, 3, 2), (1, 2)(3), (1)(2, 3), (2)(1, 3)\}$ respectively. Hence if we apply Polya's theorem, the number of distinct colorings = $\frac{1}{6}(x_1^3 + 3x_1x_2 + 2x_3)$, if we consider coloring with 2 distinct colors, then $k = 2 = x_1 = x_2 = x_3$, thus the number of distinct colorings with 2 colors = $\frac{1}{6}(2^3 + 3 * 2^2 + 2 * 2) = 4$.

27.3.2 Example 2 - Coloring faces of a cube

Let us revisit the cube example. We list the different elements of G as before, and simultaneously calculate the term they contribute to in Polya's formula.
Here is the labelled cube for reference:



- R_0 : Rotation by $0°$, i.e. identity. The cycle index of this permutation has 6 cycles of length 1, thus the number of colorings contributed will be $\boxed{x_1^6}$.
- R_1 : Rotation by $180°$ w.r.t axis through the center of the opposite faces. (Observe that there are 3 pairs of such faces). Consider the faces A, D. We have observed before that A, D remain in place, and B, E and C, F exchange their places, thus there are 2 length 1 cycles and 2 length 2 cycles, hence the contributing term will be $x_1^2x_2^2$. As there are 3 such pairs of faces, the total number of fixed colorings will be $\boxed{3x_1^2x_2^2}$.
- R_2 : Rotation by $90°$ w.r.t axis through the center of the opposite faces. Observe that there are 3 pairs of such faces. Consider the faces A, D. They retain their positions, i.e $A \to A$, $D \to D$. Now, for the other faces, we have, $C \to B$, $B \to F$, $F \to E$, and $E \to C$. Thus, there are 2 length 1 cycles and 1 length 4 cycle, hence the contributing term will be $x_1^2x_4$.As there are 3 such pairs of faces, the total number of fixed colorings will be $\boxed{3x_1^2x_4}$.
- R_3 : Rotation by $270°$ w.r.t axis through the center of the opposite faces. Observe that there are 3 pairs of such faces. Since this is the exact opposite of the previous case, by symmetry, the total number of fixed colorings will be $\boxed{3x_1^2x_4}$.
- R_4 : Rotation by $180°$ w.r.t axis through the midpoints of opposite edges. Observe that there are 6 pairs of such edges, i.e. $(de, bg),\ (af, ch),\ (ad, hg),\ (cb, ef),\ (ab, eh),\ (cd, fg)$. Suppose we do the rotation w.r.t the edges (de, bg). Then observe that, now F is now the top face, and A occupies the place where E was initially, similarly, B and D swap places. In other words,

$C \iff F$, $A \iff E$ and $B \iff D$, i.e. there are 3 length 2 cycles. Thus, the contributing term is x_2^3. As there are 6 pairs of edges, the total contributing term will be $\boxed{6x_2^3}$.

- D : Diagonal flip by $120°$ w.r.t axis through the centers of opposite corners. First, note that there are 4 pairs of opposite corners. Consider the vertex b. If we flip the cube along b by $120°$, then the face $B \to C$, i.e. B now occupies the initial position of C, $C \to D$ and $D \to B$. Thus there is the cycle $B \to C \to D \to B$. Similarly for the other three faces. Thus there are 2 cycles of length 3 and hence the contributing term will be x_3^2. As there 4 such pairs of corners, the total term contributed will be $\boxed{4x_3^2}$.
- D' : Diagonal flip by $240°$ w.r.t axis through the centers of opposite corners. First, note that there are 4 pairs of opposite corners. By symmetry, this is the opposite/complementary operation of the previous one, i.e. flip by $240°$ = flip by $120°$ in the other direction. Thus, the total term contributed will be $\boxed{4x_3^2}$.

Putting all the above together, we get

$$P_G(x_1, x_2, \dots x_4) = \frac{1}{24}(x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2)$$

if we substitute $x_i = 2$ for all i, we get

$$P_G(x_1, x_2, \dots x_4) = \frac{1}{24}(2^6 + 3 * 2^4 + 6 * 2^3 + 6 * 2^3 + 8 * 2^2) = 10$$

27.4 Towards a general formula

Let us go back to the the example of the square coloring, where $G = \{e, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$, and G as a cycle index permutation is $G = \{(1)(2)(3)(4), (1,2,3,4), (1,3)(2,4), (1,4,3,2), (1,4)(2,3), (1,2)(3,4), (2,4)(1,3), (1)(3)(2,4), (2)(4)(1,3)\}$ respectively.
Observe the 2nd, 3rd, and 4th elements of G. We know that $R_{90} \circ R_{90} = R_{180}$ i.e. $(1,2,3,4) \circ (1,2,3,4) = (1,3)(2,4)$. Therefore these elements are of the form g, g^2, g^3.
Thus, if we have a group whose elements are of the form $G = \{e, g, g^2, \dots g^k\}$ (called cyclic groups). Then the contribution of each term of $g \in G$ will be:

- $e - x_1^n$
- $g - x_n$
- $g^2 - x_{n/2}^2$ and so on

Thus, in general,

$$P_G(x_1, x_2, \ldots x_m) = \frac{1}{n} \sum_{d|n} \phi(d) x_d^{n/d}$$

where $\phi(m)$ is euler's totient function.

Proof. Consider the element g^i. Suppose it has a cycle of length d. Observe that under this operation, $1 \to 1 + i$, $1 + i \to 1 + 2i$, $\ldots$, $1 + d * i \to 1$. This must mean $d * i$ is a multiple of n. Specifically, we must have $d * i = lcm(n, i)$. Using $lcm(n, i) = \frac{n*i}{gcd(n,i)}$, we get $d * i = \frac{n*i}{gcd(n,i)} \Rightarrow gcd(n, i) = \frac{n}{d} \Rightarrow \boxed{gcd(d, \frac{i * d}{n}) = 1}$.
However there is a bijection between elements of $\phi(d)$ and i, because $i = x\frac{n}{d}$ for $x \in \phi(d)$. This implies the number of such $i = \phi(d)$. Thus, the above result shows that all i such that $gcd(d, i) = 1$ contribute n/d cycles of length d. Therefore the contribution to the term is $\phi(d) x_d^{\frac{n}{d}}$. Hence the proof. □

Thus, if we have the above formula, the group for the square coloring problem can be represented as $\{e, \sigma, \sigma^2, \ldots, \sigma^k, \pi * \sigma, \pi * \sigma^2, \ldots \pi * \sigma^{k-1}\}$. These are called dihedral groups. We discuss more about this in the next lecture.

Instructor : Jayalal Sarma
Scribe : Bhupathi Narasimha Rao (*TA:* JS)
Date : Nov 11, 2020
Status : α

Lecture
29

Applying Cycle Index in Polya's Theorem

29.1 Recall the definitions of Type and Cycle Index Polynomial

Let G be the set of some permutations of Ω , every $g \in G$ can be decomposed into a collection of disjoint cycles .
Example 1:- Consider $g = \{2, 3, 1, 5, 4\}$ which is a permutation on set $\{1, 2, 3, 4, 5\}$. So , the permutation g can be written as $(1\ 2\ 3)(4\ 5)$.
Example 2:- Identity on set $[n]$ can be written as $g = (1)(2)(3)\ldots(n)$ which is n-cycles of length 1.

Type of a permutation :- A permutation π is said to be of type $(b_1, b_2, \ldots, b_m)$ if

$$b_i = \text{\# of } i\text{-length cycles in the cyclic representation of } \pi$$

Example 1:- Type of an identity permutation is $(n, 0, \ldots, 0)$.
Example 2:- Type of the permutation $g = (1\ 2\ 3)(4\ 5)$ is $(0, 1, 1, 0, 0)$.

Cycle index Polynomial :-As discussed in previous lectures , a monomial is associated corresponding to every type as follows :

$$(b_1, b_2, \ldots, b_m) \longleftrightarrow x_1^{b_1} x_2^{b_2} \ldots x_m^{b_m}$$

And the cycle index polynomial of G is defined as:

$$P_G(x_1, x_2, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} (x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}) \quad \text{where } (b_1, b_1, \ldots, b_n) \text{ is the type of } g$$

Example 1:- Let $G = \{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \leq S_4$, then

$$P_G(x_1, x_2, x_3, x_4) = \frac{1}{4}\left(x_1^4 + x_1^2 x_2 + x_1^2 x_2 + x_2^2\right)$$

Example 2:- Let $G = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} = S_3$, then

$$P_G(x_1, x_2, x_3) = \frac{1}{6}\left(x_1^3 + x_1x_2 + x_1x_2 + x_1x_2 + x_3 + x_3\right) = \frac{1}{6}\left(x_1^3 + 3x_1x_2 + 2x_3\right)$$

Why are we doing this : The connection to Polya's Theorem will be found by the end of this lecture .

29.2 Polya's Theorem (Simpler version)

Theorem 29.2.1. *Let G be the group of symmetry acting on Ω (set of different coloring of the underlying object) , then*

$$\#\textit{ of distinct color patterns with } k\textit{-colrs } = P_G(k, k, \ldots, k)$$

Proof. Let the Domain be of size m and we have k colors , then $|\Omega| = k^m$. Using Burnsides's Lemma ,

$$\begin{aligned}\#\text{ of distinct colorings} &= \#\text{ of different orbits of G acting on}\Omega \\ &= \frac{1}{|G|}\sum_{g\in G}|fix(G)|\end{aligned}$$

We have to compute $|fix(g)|$ for $g \in G$. For example , the cyclic structure of g be $(1\ 2)(3\ 4)$, the coloring should be such that the domain under the permutation looks the same . So , the corners $1, 2$ should have same color and $3, 4$ should have same color . So , total number of colorings such that the domain looks the same under the permutation $g = k^2$. Hence all the corners in one cycle should get the same color . So , consider the type of some permutation $g = (b_1, b_2, \ldots, b_m)$, then

b_1 cycle of length 1 can have k^{b_1} possible coloring
b_2 cycle of length 2 can have k^{b_2} possible coloring
$\ldots$
$\ldots$
b_m cycle of length m can have k^{b_m} possible coloring

Therefore , # of colors fixed by $g = |fix(g)| = k_{b_1} * k^{b_2} * \cdots * k^{b_m} = x_1^{b_1} * x_2^{b_2} * \cdots * x_m^{b_m}$
where $x_i = k\ \forall i \in [k]$

Hence , # of distinct color patterns with k-colors is

$$\frac{1}{|G|}\sum_{g\in G}\left(k^{b_1} * k^{b_2} * \cdots * k^{b_m}\right) = P_G(k, k, \ldots, k)$$

□

29.3 Examples

Example 1:- Coloring necklace with 3 regular beads with black and white colors . Symmetries are rotation with respect to the axis passing through the center and rotation with respect to the axis passing through one vertex and center of the opposite edge . Hence ,

$$G = \{e, R_{120}, R_{240}, F_{12}, F_{23}, F_{31}\}$$

and cyclic representations are $\{(1)(2)(3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (2\ 3), (3\ 1)\} = S_3$. Cyclic index polynomial corresponding to G is:

$$P_G(x_1, x_2, x_3) = \frac{1}{6}\left(x_1^3 + 3x_1x_2 + 2x_3\right)$$

Hence # of different colorings with 2 colors $= \frac{1}{6}\left(2^3 + 3 * 2^2 + 2 * 2\right) = 4$

Example 2:- Consider cube coloring on faces and the symmetries group G defined previously as :

Permutation	**Corresponding Monomial**
Identity (e)	x_1^6
180^0 rotation wrt axis through centers of opposite faces (3 of them)	$3x_1^2x_2^2$
180^0 rotation wrt axis through centers of opposite edges (6 of them)	$6x_2^3$
90^0 rotation wrt axis through centers of opposite faces (3 of them)	$3x_1^2x_4$
270^0 rotation wrt axis through centers of opposite faces (3 of them)	$3x_1^2x_4$
120^0 rotation wrt axis thorough center and opposite corners (4 of them)	$4x_3^2$
240^0 rotation wrt axis through center and opposite corners (4 of them)	$4x_3^2$

Hence cyclic index polynomial corresponding to above symmetries is:

$$P_G(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24}\left(x_1^6 + 3x_1^2x_2^2 + 6x_2^3 + 3x_1^2x_4 + 3x_1^2x_4 + 4x_3^2 + 4x_3^2\right)$$

$$\Rightarrow P_G(x_1, x_2, x_3, x_4, x_5, x_6) = \frac{1}{24}\left(x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 8x_3^2 + 6x_2^3\right)$$

Question:- If the coloring is done on the corners rather than faces with same G, does the polynomial change ?

Example 3:- Square Problem discussed in previous lectures ,

$$G = \{e, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

and corresponding cyclic representations are

$$\{(1)(2)(3)(4), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 4)(2\ 3), (1\ 2)(3\ 4), (1\ 3), (2\ 4)\}<S_4$$

There is some connection between $(1\ 2\ 3\ 4)$ and $(1\ 3)(2\ 4)$. If the permutation $(1\ 2\ 3\ 4)$ is applied twice to the domain (square) , we get the permutation $(1\ 3)(2\ 4)$. That is $(1\ 2\ 3\ 4)$ composed with

itself gives $(1\ 3)(2\ 4)$. $(1\ 3)(2\ 4)$ composed with $(1\ 2\ 3\ 4)$ gives $(1\ 4\ 3\ 2)$.

Hence the set $\{e, R_{90}, R_{180}, R_{270}\}$ forms a subgroup . Suppose the permutation $(1\ 2\ 3\ 4)$ be g , then corresponding permutations are $\{e, g, g^2, g^3\}$ (g^4 is an identity)

Suppose we have a group of symmetry as (considering n to be even):

$G = \{e, g, g^2, g^3, \ldots, g^k\} = \{e, (1\,2\,3 \ldots\ n), (1\,3\,5\ \ldots\ n{-}1)(2\,4\,4\ \ldots\ n), \ldots\ldots\}$ with g^{k+1} as identity

Groups of type G are called as cyclic groups . The monomials corresponding to each permutations are as follows:

Permutation	**Corresponding Monomial**
e	x_1^n
g	x_n
g^2	$x_{\frac{n}{2}}^2$
g^3	$x_{\frac{n}{4}}^4$
$\ldots$	$\ldots$

So , the cyclic index polynomial corresponding to G can be written as:

$$P_G(x_1, x_2, \ldots, x_n) = \frac{1}{n} \sum_{d|n} \phi(\frac{n}{d}) x_{\frac{n}{d}}^d$$

where $\phi(.)$ is the Euler's function . $\phi(n)$ = # of positive integers up to n that are relatively prime to n . If n is odd ,

$$P_G(x_1, x_2, \ldots, x_n) = \frac{1}{2n} \sum_{d|n} x_{\frac{n}{d}}^d + \frac{1}{2} x_1 x_2^{\frac{n-1}{2}}$$

29.4 Dihedral Group

For the permutations $\sigma = (1\ 2\ \ldots\ n)$ and $\pi = (2\ n)(3\ n-1)$, the group defined as:

$$D_n = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \pi\sigma, \pi\sigma^2, \ldots, \pi\sigma^{n-1}\}$$

are called Dihedral groups . Here D_n is a Dihedral group .

Example 1:- Consider permutation on a square $\sigma = (1\ 2\ 3\ 4)$ and $\pi = (2\ 4)(3\ 3) = (2\ 4)(3)(1)$, then

$$\begin{aligned} \pi\sigma &= (2\ 4)(3)(1)(1\ 2\ 3\ 4) \\ &= (2\ 1)(3\ 4) \\ &= V \end{aligned}$$

Observation:-$|D_3| = 6 = |S_3|$ and $|D_4| = 8 \leq |S_4|$

29.5 Polya's Theorem (General Version)

Motivating Question:- How many in-equivalent colorings are there using 3 black and 1 white ?

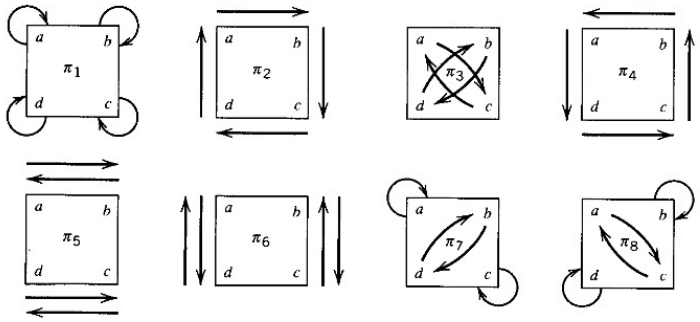


Figure 29.19: Symmetries on square

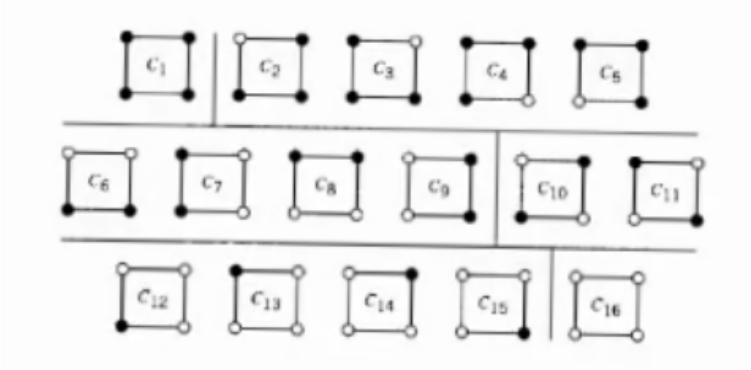


Figure 29.20: All possible coloring on square with black and white

AIM :- To write a polynomial $Q(b, w)$ such that coefficient of $b^2w^2 =$ # of inequivalent colorings with 2 Black and 2 White colors . Similarly , coefficient fo $b^3w =$# of inequivalent colorings with 3 Black and 1 White colors .

Consider the identity permutation e , no.of colorings fixed by e considering 2 colors = 16 . And no.of colorings fixed by e considering 3 Black and 1 White = 4 (from the above fig.) If we write this down for the permutations fixed by e , the expression will be as :

$$b^4 + 4b^3w + 4bw^3 + 6b^2w^2 + w^4 = (b + w)^4$$

Let us classify elements of $\Omega = \{C_1, C_2, \ldots, C_{16}\}$ into their corresponding coloring structures . The

classification will be as follows :

$$\begin{aligned} b^4 &\longleftrightarrow T_1 = \{C_1\} \\ b^3w &\longleftrightarrow T_2 = \{C_2, C_3, C_4, C_5\} \\ b^2w^2 &\longleftrightarrow T_3 = \{C_6, C_7, C_8, C_9, C_{10}, C_{11}\} \\ bw^3 &\longleftrightarrow T_4 = \{C_{12}, C_{13}, C_{14}, C_{15}\} \\ w^4 &\longleftrightarrow T_5 = \{C_{16}\} \end{aligned}$$

Suppose we want to know how many inequivalent colorings are possible with 3 Black and 1 White on a square when group G is applied , then it is enough to apply the group G on T_2 and count the inequivalent colorings . So , now we need to understand how many inequivalent colorings are there in each T_i .

G acting on T_i is well-defined . It is because when a rotation/flip is applied on a square , the number of colors or number of vertices is not changed . The image will be one of the elements of T_i itself . Hence , it is well-defined . So , for finding number of inequivalent colorings of a specific structure (like 3 Black and 1 White) , it is enough to apply G on corresponding T_i (T_2 if 3 Black and 1 White) and apply Burnside's lemma (*i.e.,* compute $|fix(g)|\forall g \in G$) .

Example 1:- Find the number of inequivalent colorings using 3 Black and 1 White when $G = \{e, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ applied on Ω .
Solution :- Consider action of G on $T_2 = \{C_2, C_3, C_4, C_5\}$,

$$\begin{aligned} \text{\# of inequivalent colorings } &= \frac{1}{|G|}\sum_{g\in G}|fix(g)| \\ &= \frac{1}{8}\left(|fix(e)| + |fix(D)| + |fix(D')|\right) \quad \text{Action of other } g\text{'s gives } |fix(g)| = 0 \\ &= \frac{1}{8}(4+2+2) \\ &= 1 \end{aligned}$$

Example 2:- Find the number of inequivalent colorings using 2 Black and 2 White when $G = \{e, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ applied on Ω .

Solution :- Consider action of G on $T_3 = \{C_6, C_7, C_8, C_9, C_{10}, C_{11}\}$,

$$\begin{aligned}\text{\# of inequivalent colorings } &= \frac{1}{|G|}\sum_{g\in G}|fix(g)| \\ &= \frac{1}{8}\left(|fix(e)| + |fix(R_{180})| + |fix(H)| + |fix(V)| + |fix(D)| + |fix(D')|\right) \\ &= \frac{1}{8}\left(6+2+2+2+2+2\right) \\ &= 2\end{aligned}$$

Example 3:- Given a permutation g with cycle structure $(1\ 2)(3)(4)$. How many inequivalent colorings are possible with different combinations of Black and White colors ?
Solution :- We have to count number of colorings that are fixed by g . So , $1, 2$ should have same color , $3, 4$ can have any color . Hence , the expression $(b^2 + w^2)(b + w)(b + w)$ represents the possible colorings where coefficient of each term correspond to the number of colorings which are inequivalent with that color structure .

$$(b^2 + w^2)(b + w)(b + w) = b^4 + 2b^3w + 2b^2w^2 + 2bw^3 + w^4$$

Hence , g fixes square with 4 corners coloured Black , 4 corners colored White , 2 squares colored with 3 Black and 1 White , 2 squares colored with 2 Black and 2 White , 2 squares colored with 1 Black and 3 White .
Example 4:- Given permutation g with cycle structure $(1\ 2)(3)(4)(5\ 6\ 7)$, the colorings which are fixed by g is given by $(b^2 + w^2)(b + w)(b + w)(b^3 + w^3)$.

29.6 Polya's Theorem

Theorem 29.6.1. *If the colors $\alpha_1, \alpha_2, \ldots, \alpha_k$ are used , then*

$$\textit{\# of inequivalent colorings expressed as generating function } = P_G(\sum_{i=1}^{k}\alpha_i, \sum_{i=1}^{k}\alpha_i^2, \ldots)$$

Example 1:- Consider the necklace with 3-half beads colored with Black and White . The group of symmetry is $G = \{e, R_{120}, R_{240}\}$. Then generating function is :

$$P_G(x_1, x_2, x_3) = \frac{1}{3}\left(x_1^3 + 2x_3\right)$$

Substitute x_1 with $(b + w)$, x_2 with $(b^2 + w^2)$ and x_3 with $(b^3 + w^3)$. Then the generating function

using Polya's theorem is:

$$\begin{aligned} P_G(b+w, B62+w^2, b^3+w^3) &= \frac{1}{3}\left((b+w)^3 + 2(b^3+w^3)\right) \\ &= b^3 + w^3 + b^2w + bw^2 \end{aligned}$$

Instructor : Jayalal Sarma
Scribe : Prasannasai Babu (*TA:* JS)
Date : Nov 12, 2020
Status : α

Lecture
30

Partial Order

30.1 Formal Definition and Examples

A partial order is a homogeneous binary relation $\leq$ over a set X satisfying particular axioms which are discussed below. When $x \leq y$, we say that x is related to y. (This does not imply that y is also related to x, because the relation need not be symmetric.)

The axioms for a partial order state that the relation $\leq$ is reflexive, antisymmetric, and transitive. That is, $\forall a, b, c \in X$, it must satisfy:

Reflexivity: $a \leq a$
Transitivity: if $a \leq b \ \ \& \ \ b \leq c$ then $a \leq c$
Antisymmetry: if $a \leq b \ \ \& \ \ b \leq c$ then $a = b$

Partial Ordered set is also called as **"Poset"**

Example 1: Natural numbers $\mathbb{N}$ with $\leq$ order
Example 2: Natural numbers $\mathbb{N}$ with $|$ (division) relation, That is $a \leq b$ if $a|b$
Example 3: Set $X = \{1, 2, 4, 3, 7, 6, 9, 10\}$ with $|$ relation. In this example 1 is less than or equal to every other element in the set as 1 divides every other element in the set. Now take two elements 3 and 7, now we can't say $3 \leq 7 \ \ \& \ \ 7 \leq 3$ as 3 doesn't divide 7 and 7 doesn't divide 3. So elements 3 and 7 are incomparable.
This leads to the notion of comparable and incomparable elements.
Example 4: Polynomials over $|$ (division) relation.
Example 5: Words(over English alphabets) over lexicographic order or dictionary order or graded lexicographic order.

A partial order is said to be total order of there are no incomparable elements.

Example 6: Set of subsets of $[n]$ and the ordering is by inclusion. This is not a total order.
Example 7: Set of the strings over the alphabet $\{0, 1\}$ of length n over the ordering for two strings x, y we say $x \leq y$ if $\forall i \in [n],\ x_i \leq y_i$

We know that there is a bijection between the sets in Example 6 and Example 7, and it turns out that the bijection is not only a bijection and it also preserves the ordering. Our claim here is for $A, B \subseteq [N]$, $A \subseteq B \iff \phi(A) \leq \phi(B)$, where ϕ is the bijective function.

30.2 Representation of Posets

A poset $p = (X, \leq)$ can naturally representes as a directed graph with X as the vertex set and the directed edges xy if x and y have a relation $x \leq y$. For example take three elements a, b, c from X, now we will draw edge from a to b if $a \leq b$ and edge from b to c if $b \leq c$, Now we don't need to draw edge from a to c, although we know $a \leq c$ through transitivity, because it unnecessarily increases the size of the graph.
Graph G has vertices V as $V = X$ and edges E as $E = \{(x, y) | x, y \in X, x \leq y\}$
The graphs that represents these posets are called as **Hasse diagram**. So transitive closure of the graph G is the graph of the relation.

30.3 New terms and Notations

Chain: $C \subseteq X$ is said to be a chain if every pair of elements in C is comparable. The chain C is a total order.

Height of Poset: Length of the longest chain.

Anti-Chain: $A \subseteq X$ is said to be anti-chain if every pair of elements in A is incomparable.

Width of Poset: Size of largest Anti-Chain.

Maximal Elements: $\{x \in X | \forall y \in X, y \leq x \ or \ x || y\}$. Here the symbol || represents incomparability.

Minimal Elements: $\{x \in X | \forall y \in X, x \leq y \ or \ x || y\}$. Here the symbol || represents incomparability.

Note: Maximal elements set and Minimal elements set, both are anti-chains.

30.4 Theorems on partitioning poset into chains and anti-chains

Theorem 30.4.1. *Every poset $P(X, \leq)$ can be partitioned into height(P) many antichains(and not less).*

Proof. We know that every element in anti-chain are incomparable. Now take the set of the elements in the longest chain. The length of the chain is height(P). We know every element in the chain are comparable. So every element in the longest chain must belong to different anti-chain. So there must be atleast height(P) many anti-chains.

Now, let's look at alternate proof using induction.

Claim: For any max chain C of poset P, min(P) $\cap\, C \neq \phi$

We will do induction on height(P). Now consider the longest chain C and remove min(P) from P to get P', so height of P' is height(P) -1. We assume that the theorem is true for P'.

Applying induction hypothesis, now add min(P) to P', the height will be increased by 1 that is height(P) = height(P') $+1$ and adding min(P) will result in increasing number of anti-chains by 1 to get full partition of P. □

Theorem 30.4.2. ***Dilworth's Theorem:*** *Every poset $P(X, \leq)$ can be partitioned into width(P) many chains(and no less).*

Proof. We will prove this by applying induction on the size of set X i.e., $|X|$ Let's take the width of the poset as w. Let $A \subseteq X$ be the anti-chain with size w. Now we will decompose P into $P_1 = (X_1, \leq)$ and $P_2 = (X_2, \leq)$.

$$X_1 = \{y \in X | \exists\, x \in A, x \leq y\}$$

$$X_2 = \{y \in X | \exists\, x \in A, y \leq x\}$$

Claim: $X_1 \cap X_2 = A$. So $A \subseteq X_1 \cap X_2$.
Suppose $y \in X_1 \cap X_2$, then $\exists\, x_1, x_2$ such that $x_1 \leq y \leq x_2$.
Now x_1 becomes comparable to x_2. But $x_1, x_2 \in A$ which is anti-chain.
$\Rightarrow x_1 = x_2 = y$
$\Rightarrow y \in A$
Suppose $|X_1| < |X|$ & $|X_2| < |X|$ We can apply induction hypothesis on P_1 and P_2 to get chains $C_1, C_2, C_3, \ldots C_w$ and $C'_1, C'_2, C'_3, \ldots C'_w$ each of length w.
We know,

$$A = min(P_1) = max(P_2)$$

We can join the corresponding chains to get chains of poset P. Let the elements of set $A = \{a_1, a_2, a_3, \ldots, a_w\}$.
Without loss of generality, let's assume that C_1 ends at a_1, C_2 ends at a_2 and so on upto C_w ends at a_w. Similarly C'_1 starts as a_1, C'_2 starts at a_2 and so on upto C'_w starts at a_w. Now partition of X

for P can be $C_1 \cdot C'_1,\ C_2 \cdot C'_2$ and so on upto $C_w \cdot C'_w$.

We need to handle the case when $|X_1| = |X|$ or $|X_2| = |X|$.
If $|X_1| = |X|$ that means $X_1 = X$, which in turn means $A = min(P)$. Similarly if we choose $A = max(P)$ then $X_2 = X$ and $|X_2| = |X|$. If there are anti-chains of size w which are not min(P) and max(P), then we can do the same like above.

But if it is the case that the only max sized anti-chains are max(P) or min(P) or both, we should look for alternate approach.

Now consider any max chain in P, and remove that chain C from P to get P'. So now,

$$max(P) \cap C \neq \phi \ \ \& \ \ min(P) \cap C \neq \phi$$

We can apply induction hypothesis to get a decomposition of P' in less than w many chains. Now put the C back to get decomposition into w many chains which partition X.

□

30.5 Applications of Dilworth's Theorem

Application 1: Proof of Erdős–Szekeres theorem

Theorem 30.5.1. *Every sequence of $rs + 1$ distinct integers, there must exist an increasing sequence of length $r + 1$ or decreasing sequence of length $s + 1$.*

Proof. Let $a_1, a_2, a_3, \ldots, a_n$ be the sequence of length n where $n = rs + 1$.
Define ordering of the sequence as $a_i \leq a_j$ if $i \leq j$ and $a_i \leq a_j$. It is transitive, reflexive and anti-symmetric. So it is a partial order. So we define chains and anti-chains in this poset. A chain in this poset means the elements are in the increasing order.
$\Rightarrow$ A chain in this poset $\rightarrow$ increasing sub-sequence.
Similarly an anti-chain in this poset means the elements are in the decreasing order.
$\Rightarrow$ An anti-chain in this poset $\rightarrow$ decreasing sub-sequence.
Suppose there is no anti-chain(decreasing sub-sequence) of size $s + 1$.

$$\Rightarrow w(P) \leq s$$

By Dilworth's theorem there is a decomposition of P into atmost s many chains. So there exists at least one chain with $r + 1$ elements, otherwise there will be only $r \times s$ elements in the ground set. But we have $rs + 1$ elements. Therefore there must exist a chain with $r + 1$ elements which is an increasing sub-sequence. □

.

Example for size of chain and anti-chain

We know there is a bijection between example 6 and example 7 in section 30.1 i.e., between the sets

$\Rightarrow$ subset poset of subsets of [n] $\rightarrow$ Boolean strings poset of length n.

The max length of the chain is $n+1$. Intutively we can say that maximum size of the anti-chain is $\binom{n}{\frac{n}{2}}$. Let's look how to prove it in the next lecture by Sperner's theorem.

Theorem 30.5.2. *The maximum size of any anti-chain in the subset poset(Example 6 of 30.1) is* $\binom{n}{\frac{n}{2}}$.

Proof. The subset poset is equivalent to boolean strings of length n poset. Now let's represent boolean string poset as B_n. We need to prove width(B_n) = $\binom{n}{\frac{n}{2}}$.

Let us first show that width(B_n) is atleast $\binom{n}{\frac{n}{2}}$. We can show one anti-chain of size $\binom{n}{\frac{n}{2}}$, that is subsets of size $\frac{n}{2}$.

Now we need to show that any anti-chain in B_n must have size $\leq \binom{n}{\frac{n}{2}}$

Let F be any anti-chain in B_n. We need to show $|F| \leq \binom{n}{\frac{n}{2}}$. Let us say,

A permutation $\pi \in S_n$ is said to meet $A \subseteq \{1, 2, \ldots, n\}$ if A forms prefix of π. This statement meaning is, Let's say $|A| = k$ then π said to meet A if $A = \{\pi(1), \pi(2), \ldots, \pi(k)\}$.

Consider each subset in F and consider permutations meeting them, As we are taking subsets from F, they are incomparable. Hence a single permutation can't meet both A and B.Now let's count the size of

$$\sum_{A \in F} \Big| \{\pi | \pi \; meets \; A\} \Big|$$

As single permutation can meet only one subset of F,

$$\sum_{A \in F} \Big| \{\pi | \pi \; meets \; A\} \Big| \leq n!$$

Now number of permutations that can meet set A of size k is $k! \times (n-k)!$.So,

$$\sum_{A \in F} |A|! \times (n - |A|)! \quad \leq \quad n!$$

Bring that RHS term to LHS, now

$$\sum_{A \in F} \frac{1}{\frac{n!}{|A|! \times (n-|A|)!}} \quad \leq \quad 1$$

$$\sum_{A \in F} \frac{1}{\binom{n}{|A|}} \quad \leq \quad 1$$

We can substitute $\binom{n}{\frac{n}{2}}$ in place of $|A|$ and the inequality still holds.

$$\sum_{A \in F} \frac{1}{\binom{n}{\frac{n}{2}}} \quad \leq \quad 1$$

$$\sum_{A \in F} 1 \quad \leq \quad \binom{n}{\frac{n}{2}}$$

$$|F| \quad \leq \quad \binom{n}{\frac{n}{2}}$$

We showed that,

$$|F| \quad \leq \quad \binom{n}{\frac{n}{2}} \;\; \& \;\; |F| \quad \geq \quad \binom{n}{\frac{n}{2}}$$

Hence the max size of the anti-chain F is

$$|F| \quad = \quad \binom{n}{\frac{n}{2}}$$

Hence proved. □

Instructor : Jayalal Sarma
Scribe : Kaushik Arcot (*TA:* JS)
Date : 16 November, 2020
Status : α

Lecture
32

Incidence Algebra and Mobius Inversion Over Posets

32.1 Recall

Theorem 32.1.1 (Stronger PIE). *Let $f, g : 2^{[n]} \longrightarrow \mathbb{R}$ are functions assigning real numbers to subsets of $[n]$ with the property that for any $A \subseteq [n]$*

$$g(A) = \sum_{S \subseteq A} f(S)$$

Then,

$$f(A) = \sum_{S \subseteq A} (-1)^{|A|-|S|} g(S)$$

Mobius Inversion of Functions
$f, g : \mathbb{N} \to \mathbb{R}$ $satisfying, \forall n\ g(n) = \sum_{d|n} f(d)$ $then,$

$$\forall n\ f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$$

$$\mu(d) = \begin{cases} +1, & if\ d\ is\ a\ square-free\ positive\ integer\ with\ an\ even\ number\ of\ prime\ factors \\ -1, & if\ d\ is\ a\ square-free\ positive\ integer\ with\ an\ odd\ number\ of\ prime\ factors \\ 0, & otherwise \end{cases}$$

We can see in both cases that, there is an underlying poset for both the functions. For the first pair of functions, the poset is the Subset Poset, and for the second, it is the divisibilty poset. Our endeavour in this lecture is to further abstract this concept to any poset and acquire tools for algebra within poset functions, and then for Mobius Inversion of functions over posets.

32.2 Incidence Algebra of Posets

Let $P = (X, \leq)$ be a poset. Let

$$A(P) = \{f : X \times X \to \mathbb{R} | f(x, y) = 0, \forall x, y \in X s.t x || y\}$$

Here $x||y$, indicates that x is incomparable to y in the Poset P.

Example functions :

Zero Function

$$O(x, y) = 0 \forall x, y \in X$$

Kronecker Delta Function

$$\delta(x, y) = \begin{cases} 1, & if \ \ x \ = \ y \\ 0, & otherwise \end{cases}$$

Characteristic Function of Poset

$$\zeta(x, y) = \begin{cases} 1, & if \ \ x \ \leq \ y \\ 0, & otherwise \end{cases}$$

Addition Operator
Given $f \in A(P)$, $g \in A(P)$, the '+' operator

$$(f + g)(x, y) = f(x, y) + g(x, y)$$

If $x||y$, then $f(x, y) = 0$, $g(x, y) = 0$, and hence $(f + g)(x, y) = 0$. Thus $(f + g) \in A(P)$
Remark : A(P) forms a group with '+' operator as addition.

Scalar Multiplication
Given $f \in A(P)$, $c \in \mathbb{R}$,

$$(cf)(x, y) = c * f(x, y)$$

If $x||y$, then $f(x, y) = 0$, and so $(cf)(x, y) = 0$, Hence $(cf) \in A(P)$
Remark : $A(P)$ is closed under addition and scalar multiplication. Thus, $A(P)$ forms a vector space.

Convolution Operator
We define the operator '*' over $A(P)$. Given two functions, $f, g \in A(P)$, the convolution operator is defined as,

$$(f * g)(x, y) = \begin{cases} \sum_{z:x \leq z \leq y} f(x, z)g(z, y), & if \ \ x \ \ \leq \ \ y \\ 0, & otherwise \end{cases}$$

We find if the following properties of the convolution operator hold or not.

Commutative

Convolution operator is not commutative. Assume $x, y \in X$, such that $x \leq y$ and there exists no such z such that $x \leq z \leq y$. Then,

$$(f * g)(x, y) = f(x, x)g(x, y) + f(x, y)g(y, y)$$

$$(g * f)(x, y) = g(x, x)f(x, y) + g(x, y)f(y, y)$$

These two expressions are not always equal. Assume $f(x, x) = 1$, $g(x, y) = 1$, and $f(x, y) = f(y, y) = 0$, $g(x, x) = g(y, y) = 0$. Then, we have

$(f * g)(x, y) = 1$ and $(g * f)(x, y) = 0$. Therefore, convolution is not commutative.

Associative

The convolution operator is associative. To prove, assume $f, g, h \in A(P)$. Then,

$$((f * g) * h)(x, y) = \sum_{z:x \leq z \leq y} (f * g)(x, z)h(z, y)$$

$$= \sum_{z:x \leq z \leq y} (\sum_{w:x \leq w \leq z} f(x, w)g(w, z))h(z, y)$$

By changing the order of the summations, we get,

$$\sum_{w:x \leq w \leq z} f(x, w)(\sum_{z:w \leq z \leq y} g(w, z)h(z, y))$$

$$= \sum_{w:x \leq w \leq z} f(x, w)(g * h)(w, y)$$

$$= (f * (g * h))(x, y)$$

Hence, convolution is associative.

Identity

Claim : The Kronecker Delta function is the identity function of A(P)

Proof. For $f \in A(P)$, if $x \leq y$,

$$(f * \delta)(x, y) = \sum_{z:x \leq z \leq y} f(x, z)\delta(z, y)$$

$$= \sum_{z:x \leq z < y} f(x, z)\delta(z, y) + f(x, y)\delta(y, y)$$

Given that $z \neq y$, we have $\delta(z, y) = 0$. Thus, $(f * \delta)(x, y)$

$$= f(x, y)\delta(y, y)$$

$\delta(y, y) = 1$, So

$$= f(x, y)$$

Thus, Kronecker Delta function(δ) is the identity function of A(P).

□

32.3 Inverse of a Function

The inverse of a function $f \in A(P)$, is a function g, such that

$$(f * g)(x, y) = \delta(x, y)$$

Does the inverse of any $f \in A(P)$ exist ? No. In fact, we check for O(x,y). Let us assume there exists an inverse, Q(x,y) for the zero function. Then,

$$(O * Q)(x, x) = \sum_{z:x \leq z \leq x} O(x, z)Q(z, x)$$

$$= O(x, x)Q(x, x) = 0$$

But $\delta(x, x)$ = 1. Thus, O(x) (zero function) does not have an inverse. Can inverse exist for any other functions ? Yes, we see from this argument that for inverse to exist for $f \in A(P)$, there exists no $x \in X$, such that $f(x, x) = 0$. Infact, we prove next that for $f \in A(P)$, such that $\forall x \in X, f(x, x) \neq 0$, then there exists a unique inverse of f.

32.4 Mobius Inversion over Posets

Lemma 32.4.1. *For any $f \in \mathbb{A}(P)$ such that $\forall x \in X, f(x, x) \neq 0$, there exists $g \in \mathbb{A}(P)$ (which we will call f^{-1}) such that $\forall x, y \in X, g \star f = \delta$ where δ is the Kronecker delta function.*

Proof. We will directly write down the function g based on f. For incomparable pairs (x, y) we can define $g(x, y) = 0$. This ensures that $g \in \mathbb{A}(P)$.

For comparable pairs, the function g on input (x, y) is defined based on an induction on a parameter of $\ell(x, y) \in X$. The distance between x and y, denoted by $\ell(x, y)$ is said to be k, if $\exists z_1, z_2, \ldots z_{k-1}$ such that $x < z_1 < z_2 < \ldots < z_{k-1} < y$ and $\nexists w_1, w_2, \ldots w_k$ such that $x < w_1 < w_2 < \ldots < w_{k-1} < w_k < y$. In other words, this is the length of the longest directed path from x to y (or vice versa).

Now we are ready to describe the definition of g on comparable pairs (x, y).

As the base case, when $\ell(x, y) = 0$, we know that, $x = y$, hence we define:

$$g(x, x) = \frac{1}{f(x, x)}$$

Let us quickly check that this indeed satisfies the property that we wanted for inputs of the kind (x, x). That is,

$$(g \star f)(x, x) = \sum_{x \leq z \leq y} g(x, z) f(z, y) = g(x, x) f(x, x) = 1 = \delta(x, x)$$

To do the definition inductively: let us assume that $g(x, y)$ is defined when $\ell(x, y) \leq k$, and we consider a pair (x, y) with distance $k + 1$. We define :

$$g(x, y) = \frac{-1}{f(y, y)} \sum_{x \leq z < y} g(x, z) f(z, y)$$

Note that this is well-defined since $g(x, z)$ is used in the RHS only for pairs (x, z) with $\ell(x, z) \leq k$ and that $f(y, y) \neq 0$ for every $y \in X$. With this definition :

$$\begin{aligned}
(g \star f)(x, y) &= \sum_{x \leq z \leq y} g(x, z) f(z, y) \\
&= \sum_{x \leq z < y} g(x, z) f(z, y) + g(x, y) f(y, y) \\
&= \sum_{x \leq z < y} g(x, z) f(z, y) + \left(\frac{-1}{f(y, y)} \sum_{x \leq z < y} g(x, z) f(z, y) \right) f(y, y) \\
&= 0 = \delta(x, y)
\end{aligned}$$

Since $g \in \mathbb{A}(P)$ we have completed the proof. ∎

Instructor : Jayalal Sarma
Scribe : Abhishek Aladahalli (*TA:* JS)
Date : 18 November, 2020
Status : α

Lecture
33

Mobius Inversion Theorem for Posets and Corollaries

In particular the **zeta function** (ζ)

$$\zeta(x,y) = \begin{cases} 1 & \text{if } x \leq y \\ 0 & \text{otherwise} \end{cases}$$

has an inverse called the **Mobius Function** (μ) of the poset.

From the lemma proved above we define Mobius Function as,
For $x = y$,

$$g(x,x) = \mu(x,x) = \frac{1}{\zeta(x,x)} = 1$$

$$=> \boxed{\mu(x,x) = 1 \ \ (\text{Since } \zeta(x,x) = 1)}$$

For $x \mid\mid y$, (i.e. when x and y are incomparable)

$$g(x,y) = \mu(x,y) = \frac{-1}{\zeta(y,y)} \sum_{x \leq z < y} \mu(x,z)\zeta(z,y)$$

$$=> \mu(x,y) = -1 \sum_{x \leq z < y} \mu(x,z)\zeta(z,y)$$

$$=> \mu(x,y) = -1 \sum_{x \leq z < y} \mu(x,z)(0)$$

(Since, zeta function (ζ) is 0 for x and y which are incomparable)

$$=> \boxed{\mu(x,y) = 0}$$

For $x \leq y$,

$$g(x,y) = \mu(x,y) = \frac{-1}{\zeta(y,y)} \sum_{x \leq z < y} \mu(x,z)\zeta(z,y)$$

$$=> \mu(x,y) = -1 \sum_{x \le z < y} \mu(x,z)\zeta(z,y)$$

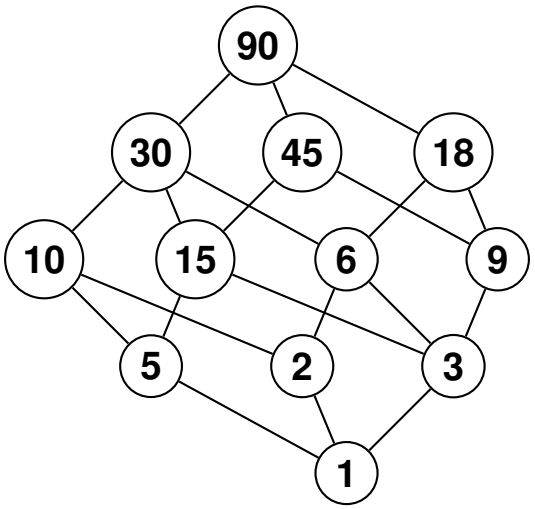
$$=> \mu(x,y) = -1 \sum_{x \le z < y} \mu(x,z)(1) \quad \text{(Since } \zeta(z,y) = 1 \text{ for } z < y)$$

$$=> \boxed{\mu(x,y) = -\sum_{x \le z < y} \mu(x,z)}$$

Hence, Mobius Function is defined as

$$\mu(x,y) = \begin{cases} -\sum_{x \le z < y} \mu(x,z) & \text{if } x < y \\ 1 & \text{if } x = y \\ 0 & \text{if x and y are incomparable i.e. } x \,||\, y \end{cases} \tag{33.89}$$

Now, Let's consider an example of Divisibility Poset and apply the mobius function on it,



For $(x, y) = (1, 1)$,

$$\mu(x, y) = \mu(1, 1)$$
$$\Rightarrow \mu(1, 1) = 1 \qquad (\because x = y)$$

For $(x, y) = (1, 2)$,

$$\mu(x, y) = \mu(1, 2)$$
$$\Rightarrow \mu(1, 2) = -\sum_{1 \le z < 2} \mu(1, z) \qquad \text{(By definition of mobius function)}$$
$$= -\mu(1, 1)$$
$$\Rightarrow \mu(1, 2) = -1$$

Similarly for $(x, y) = (1, 3)$,

$$\Rightarrow \mu(1, 3) = -1$$

Similarly for $(x, y) = (1, 5)$,

$$\Rightarrow \mu(1, 5) = -1$$

Thus, In general for a prime number p,

$$\mu(1, p) = -1$$

Now,

$$\begin{aligned}
\text{For } (x,y) &= (1,10), \\
\mu(x,y) &= \mu(1,10) \\
\Rightarrow \mu(1,10) &= -\sum_{1\le z<10} \mu(1,z) \qquad \text{(By definition of mobius function)} \\
&= -(\mu(1,1)+\mu(1,2)+\mu(1,5)) \\
\Rightarrow \mu(1,10) &= 1
\end{aligned}$$

$$\begin{aligned}
\text{Similarly for } (x,y) &= (1,15), \\
\Rightarrow \mu(1,15) &= 1
\end{aligned}$$

$$\begin{aligned}
\text{Similarly for } (x,y) &= (1,6), \\
\Rightarrow \mu(1,6) &= 1
\end{aligned}$$

Thus, In general for prime numbers p and q ,

$$\begin{aligned}
\mu(1,pq) &= -(\mu(1,1)+\mu(1,p)+\mu(1,q)) \\
\Rightarrow \mu(1,pq) &= 1
\end{aligned}$$

Now,

$$\begin{aligned}
\text{For } (x,y) &= (1,9), \\
\mu(x,y) &= \mu(1,9) \\
\Rightarrow \mu(1,9) &= -\sum_{1\le z<9} \mu(1,z) \qquad \text{(By definition of mobius function)} \\
&= -(\mu(1,1)+\mu(1,3)) \\
\Rightarrow \mu(1,9) &= 0
\end{aligned}$$

Thus, In general for a prime number p,

$$\mu(1,p^2) = 0$$

Now,

$$\begin{aligned}
\text{For } (x,y) &= (1,45), \\
\mu(x,y) &= \mu(1,45) \\
\Rightarrow \mu(1,45) &= -\sum_{1\le z<45} \mu(1,z) \qquad \text{(By definition of mobius function)} \\
&= -(\mu(1,1)+\mu(1,3)+\mu(1,5)+\mu(1,9)+\mu(1,15)) \\
\Rightarrow \mu(1,45) &= 0
\end{aligned}$$

$$\begin{aligned}
\text{Similarly for } (x,y) &= (1,18), \\
\Rightarrow \mu(1,18) &= 0
\end{aligned}$$

Thus, In general for prime numbers p and q,

$$\begin{aligned}
\mu(1,p^2q) &= -(\mu(1,1)+\mu(1,p)+\mu(1,q)+\mu(1,pq)+\mu(1,p^2)) \\
\Rightarrow \mu(1,p^2q) &= 0
\end{aligned}$$

Now,

$$\begin{aligned}
\text{For } (x,y) &= (1,30), \\
\mu(x,y) &= \mu(1,30) \\
\Rightarrow \mu(1,30) &= -\sum_{1\le z<30} \mu(1,z) \qquad \text{(By definition of mobius function)} \\
&= -(\mu(1,1)+\mu(1,3)+\mu(1,5)+\mu(1,2)+\mu(1,6)+\mu(1,10)+\mu(1,15)) \\
\Rightarrow \mu(1,30) &= -1
\end{aligned}$$

Thus, In general for prime numbers p, q and r,

$$\begin{aligned}
\mu(1,pqr) &= -(\mu(1,1)+\mu(1,p)+\mu(1,q)+\mu(1,pq)+\mu(1,qr)+\mu(1,pr)) \\
\Rightarrow \mu(1,pqr) &= 1
\end{aligned}$$

Therefore, in general, The mobius function for the divisibility poset turns out to be,

$$\mu(d)\begin{cases} = +1 & \text{If } d \text{ is a product of even number of primes} \\ = -1 & \text{If } d \text{ is a product of odd number of primes} \\ = 0 & \text{Otherwise} \end{cases}$$

33.1 Mobius Inversion theorem over Posets

Assumption :
In the poset X, there is a unique m such that $\forall x \in X, m \leq x$

Theorem 33.1.1. *For a poset X, if f is a function $f : X \to \mathbb{R}$ and g is a function $g : X \to \mathbb{R}$ such that,*

$$\forall a \in X, \qquad g(a) = \sum_{x \leq a} f(x)$$

then

$$\boxed{\forall a \in X, \qquad f(a) = \sum_{x \leq a} \mu(x, a) g(x)}$$

where μ is the mobius function of the poset.

Proof. As from the assumption, let m be the unique minimal element of the poset X.
And let f and g be the functions defined as above such that

$$\forall a \in X, \;\; g(a) = \sum_{x \leq a} f(x) \qquad (1)$$

Now, we define two functions $F(x, y)$ and $G(x, y)$ such that,

$\forall a \in X,$	For all other x and y where $x \neq m$,
$F(m, a) = f(a)$	$F(x, y) = 0$
$G(m, a) = g(a)$	$G(x, y) = 0$

Thus, By Incidence Algebra $F, G \in A(P)$ for $P(X, \leq)$.

Claim :

$$\boxed{G = F \star \zeta \;\text{ where } \zeta \text{ is the zeta function.}}$$

Note: Through this claim we can show that $F = G \star \mu$ (where μ is the mobius function) and thus proving the theorem.

Proof for the claim :

Consider $G(x, y)$,

Case 1 : $\forall a \in X$

$$\begin{aligned} G(m,a) &= g(a) \\ &= \sum_{x \le a} f(x) \qquad (\because \text{ from (1)}) \\ &= \sum_{m \le x \le a} F(m,x) \qquad (\because \text{ from definition of } F(x,y)) \\ &= \sum_{m \le x \le a} F(m,x)\zeta(x,a) \qquad (\because \zeta(x,a) = 1, \forall x \le a\ ) \end{aligned}$$

$$=> \boxed{G(m,a) = F \star \zeta(m,a)} \qquad (\because \text{ By defintion of convolution } (\star))$$

Case 2 : For all other x and y where $x \neq m$

$$\begin{aligned} G(x,y) &= 0 \\ &= \sum_{x \le z \le y} F(x,z)\zeta(z,y) \qquad (\because F(x,z) = 0, \forall x \neq m\ ) \end{aligned}$$

$$=> \boxed{G(x,y) = F \star \zeta(x,y)} \qquad (\because \text{ By defintion of convolution } (\star))$$

Hence, The claim $G = F \star \zeta$ is true.

Thus, By definition

$$\boxed{F = G \star \mu}$$

Therefore, $\forall a \in X$,

$$F(m,a) = \sum_{m \le x \le a} G(m,x)\mu(x,a) \qquad (\because \text{ By defintion of convolution } (\star))$$

$$=> f(a) = \sum_{x \le a} g(x)\mu(x,a) \qquad (\because \text{ From defintion of } F(m,a) = f(a), G(m,x) = g(x))$$

Thus,

$$\forall a \in X, \qquad f(a) = \sum_{x \le a} \mu(x,a)g(x)$$

Hence Proved.

□

33.1.1 Corollary

Application of Mobius Inversion theorem on Subset Poset

For the subset poset we will show, if f and g are functions defined from subsets to real numbers (i.e. $f : 2^{[n]} \to \mathsf{R}$, $g : 2^{[n]} \to \mathsf{R}$) such that

$$\forall A \subseteq [n], \quad g(A) = \sum_{S \subseteq A} f(S)$$

then

$$\boxed{\forall A \subseteq [n], \quad f(A) = \sum_{S \subseteq A} (-1)^{|A|-|S|} g(S)}$$

Claim : For $X \subseteq [n]$ and $Y \subseteq [n]$,

$$\mu(X,Y) = \begin{cases} 0 & \text{if } X \not\subseteq Y \\ (-1)^{|Y|-|X|} & \text{if } X \subseteq Y \end{cases}$$

Note : If we prove the claim to be true then the above subset poset can directly be shown as a corollary of the mobius inversion theorem by substituting the value of μ.

Proof for the claim :
We will apply Induction on $|Y| - |X|$ for $X \subseteq Y$.

Base step, For $|Y| - |X| = 0$ i.e. $X = Y$

$$\begin{aligned} & \mu(X,Y) = \mu(X,X) \\ \Rightarrow & \mu(X,Y) = 1 \qquad (\because X \subseteq X \text{ and } \mu(X,X) = 1\ ) \\ \Rightarrow & \mu(X,Y) = (-1)^0 = (-1)^{|Y|-|X|} \end{aligned}$$

Induction step, Assume it's true for $|Y| - |X| \leq k$. Now, we need to prove it's also true for $|Y| - |X| = k + 1$.

Thus, Consider $\mu(X,Y)$ for $|Y| - |X| = k + 1$,

$$\mu(X,Y) = -\sum_{X \subseteq Z \subset Y} \mu(X,Z) \qquad (\because X < Y \text{ and by definition of mobius function })$$

$$\Rightarrow \mu(X,Y) = -\sum_{X \subseteq Z \subset Y} (-1)^{|Z|-|X|} \qquad (\because |Z| - |X| \leq k \text{ and it's assumed true for } |Y| - |X| \leq k)$$

$$\Rightarrow \mu(X,Y) = -\sum_{X \subseteq Z \subseteq Y} (-1)^{|Z|-|X|} + (-1)^{|Y|-|X|} \qquad (\because \text{ Adding and subtracting the subset } Y)$$

$$\Rightarrow \boxed{\mu(X,Y) = -\sum_{X \subseteq Z \subseteq Y} (-1)^{|Z|-|X|} + (-1)^{|Y|-|X|}} \qquad (1)$$

Now, we will show that 1st term in the R.H.S goes to 0 by using a combinatorial argument.

So, For given $X, Y \subseteq [n]$ and $X \subseteq Y$,

$$\sum_{X \subseteq Z \subseteq Y} (-1)^{|Z|-|X|} = \sum_{k} \sum_{\substack{X \subseteq Z \subseteq Y \\ |Z|-|X|=k}} (-1)^k \quad \text{(By rewriting the summation based on the size of } |Z| - |X|)$$

$$= \sum_{k} (-1)^k \binom{n}{k} \qquad (\because \text{ Number of ways of choosing such a subset } |Z| \text{ is } \binom{n}{k})$$

$$= 0 \qquad (\because \text{ Signed summation of binomial coefficients is } 0)$$

$$\Rightarrow \sum_{X \subseteq Z \subseteq Y} (-1)^{|Z|-|X|} = 0$$

Therefore, Equation (1) becomes,

$$\mu(X, Y) = (-1)^{|Y|-|X|}$$

Hence Proved.

Thus, from this definition of μ and the theorem of Mobius Inversion, the corollary on the subset poset follows that ,

Corollary : If f and g are functions defined from subsets to real numbers (i.e. $f : 2^{[n]} \to \mathsf{R}$, $g : 2^{[n]} \to \mathsf{R}$) such that

$$\forall A \subseteq [n], \quad g(A) = \sum_{S \subseteq A} f(S)$$

then

$$\forall A \subseteq [n], \quad f(A) = \sum_{S \subseteq A} (-1)^{|A|-|S|} g(S)$$

Instructor : Jayalal Sarma
Scribe : Kaushik Arcot, Abhishek Aladahalli (*TA:* JS)
Date : 19 November, 2020
Status : α

Lecture
34

More Applications of Structure of Partial Orders, Fixed Point Theorems

34.1 Equinumerous Sets and Bijections

We define Cardinality using the concept of Bijections and Equinumerous sets.

Theorem 34.1.1. *Two sets A, B are equinumerous or equal in cardinality iff there exists a bijection $f : A \to B$. Or,*

$|A| = |B| \Leftrightarrow \exists$ *bijection* $f : A \to B$

Example of Equinumerous sets and Bijections

Even Numbers and $\mathbb{N}$

$f : \mathbb{E} \to \mathbb{N}$, $f(x) = x/2$
Is a bijection from even numbers to Natural Numbers.

The Noton of Cardinality arises from the fact that these Equinumerous sets divide the Subset Partial Order into different equivalence classes and each of those classes correspond to different cardinalities.

So to prove that two sets are equinumerous sets, we need to prove there exists a bijection between the two sets. To prove that there exists a bijection between two sets, we can just prove that there exists an injection in both directons.

Theorem 34.1.2 (Cantor Schroeder Bernstein Theorem)**.** *$A, B \subseteq U$,$\exists f : A \to B, g : B \to A$ are injections $\Rightarrow \exists h : A \to B$ which is a bijection*

This theorem is intuitive in finite sets, but to prove for infinite sets, we need some more tools that concern posets and cardinality.

34.2 Knaster-Tarski Fixed point theorem

To prove this theorem, we need to understand some properties.

Fixed Point of a Function

Let $f : X \to X$, be a function. Then, a point $x \in X$, is said to be a fixed point of function f if $f(x) = x$.

Preserving Order of Posets

Let $P(X, \leq)$ be a poset. Then any function $f : X \to X$ is said to preserve order if

$$\forall x, y \in X, x \leq y \Rightarrow f(x) \leq f(y)$$

Upper Bound of a Set

Let $P(X, \leq)$ be a poset, and $A \subseteq X$, then the upper bound of set A is defined as

$$UB(A) = \{x \in X | \forall y \in A, y \leq x\}$$

Least Upper Bound of a Set

Let $P(X, \leq)$ be a poset, and $A \subseteq X$, then the least upper bound of set A is defined from the upper bound set, as the least element in the upper bound set of A.

$$LUB(A) = \{x | \forall y \in UB(A), x \leq y\}$$

Complete Partial Order

A partial order $P(X, \leq)$ is set to be a complete partial order, if $\forall A \subseteq X$, $\exists LUB(A)$

We can understand the notion of a complete partial order using the subsets partial order. Let $P(X, \leq)$, be the subsets partial order, where $X = 2^{[n]}$. Then, let $A \subseteq X$, be a subset of X, which is a set of subsets of $[n]$. Assume, $A = \{A_1, A_2, ...A_k\}$, and S = $\bigcup_{i=1}^{k} A_i$ forms the LUB of the set A. We know that $\forall i \in [k], A_i \leq S$, (because A_i is a subset of S, S is the union of all A_i's). And it is the lowest upper bound, as any element missing from S, will be present in one of the A_i's.

Now, we're ready to prove the Knaster-Tarski Theorem.

Theorem 34.2.1 (Knaster-Tarski Fixed point theorem)**.** *Let $P(X, \leq)$ be a complete partial order, and let $f : X \to X$, be a function that preserves the order on the partial order P. Then f has a fixed point.*

Proof. Consider the set $A = \{x | x \leq f(x)\}$. Assume that A is non-empty. This is possible when X has a least element in P. Then, for that least element $x \in X$, $\forall y \in X, x \leq y$. And $f(x) \in X$, thus, $x \leq f(x)$, and therefore $x \in A$.

Observation If $x \in A$, then $f(x) \in A$.
$x \in A$. $\Rightarrow x \leq f(x)$. As f preserves order,
$\Rightarrow f(x) \leq f(f(x))$. Let f(x) = z, then

$z \leq f(z)$. Thus, $z \in A. \Rightarrow f(x) \in A$.

Since the partial order is complete, and $A \subseteq X$, there exists an LUB(A). Let

$$y = LUB(A)$$

Consider, $\forall x \in A$. As y is LUB,
$x \leq y$, As f preserves order
$f(x) \leq f(y)$. Becasue $x \in A$,

$x \leq f(x) \leq f(y), \forall x \in A$

This implies that $f(y)$ is an upper bound of A. Since y is the LUB of A,

$$y \leq f(y)$$

By the property of A, it is clear that $y \in A$. And because $y \in A$, and from the observation proven above, we have that $f(y) \in A$.

Since $f(y) \leq A$, and y is LUB(A) of A, we have that

$$f(y) \leq y$$

So, we have,

$$f(y) \leq y \ \ \& \ \ y \leq f(y)$$

.

By the anti-symmetry of the relation $\leq$ in the partial order, we have

$$f(y) = y$$

So, we have y as the fixed point.

Hence proved.

□

34.3 Cantor-Schroeder-Bernstein Theorem

Theorem 34.3.1 (Cantor Schroeder Bernstein Theorem)**.** *$A, B \subseteq U$,$\exists f : A \to B, g : B \to A$ that are injections $\Rightarrow \exists h : A \to B$ which is a bijection.*

Proof. We find a $H \subseteq A$, and we build a function h, such that

$$h|_H = f \ \ \& \ \ h|_{\overline{H}} = g$$

Then, we prove that H is a bijection.
Claim For $H \subseteq A$, if $g(\overline{f(H)}) = \overline{H}$ then by the above definition, h is a bijection.

Or, we have to find an H such that $H = \overline{g(\overline{f(H)})}$

First, we find an H such that this claim is satisfied, and then we prove the claim.

We define the following function on the subset partial order of A.

$\tau : 2^{[A]} \to 2^{[A]}$, such that for any $T \subset A$,

$$\tau(T) = \overline{g(\overline{f(T)})}$$

We will prove the properties of preserving order and completeness of this Partial Order.

We know that the partial order is complete, as it is a subset poset.

For preserving order, assume $S \subset T$. . By applying f on both sides, we have $f(S) \subset f(T)$.

Taking complement, we have $\overline{f(T)} \subset \overline{f(S)}$.

As g is a function from B to A, and $f(x) \in B \forall x \in A$, applying g on both sides, we get

$$g(\overline{f(T)}) \subset g(\overline{f(S)})$$

Again taking complement, we get

$$\overline{g(\overline{f(S)})} \subset \overline{g(\overline{f(T)})}$$

So, $\tau(S) \subset \tau(T)$. Hence τ preserves order.

Because τ preserves order and and $P = ([A], \leq)$ is a complete poset, we have that there exists a fixed point for τ. Therefore

$$\exists H \subset A, \overline{g(\overline{f(H)})} = H$$

Now that we have arrived at an H, we now need to prove that h is a bijection. We need to

prove three parts.

Well-defined

h is well defined. $\forall x \in A$, if $x \in H$, the output of h is f(x). Otherwise, as g is injective, and $\overline{H} = g(\overline{f(H)})$, and so $\overline{H} \subseteq g(B)$, and $g^{-1}(x)$ is defined $\forall x \in g(B)$, and subsequently in $\overline{H}$. So $\forall x \in A$, h(x) is well defined.

Injective

We need to prove $\forall x, y \in A, x \neq y \Rightarrow h(x) \neq h(y)$.

Case 1 : $x \in H \ \ \& \ \ y \in H$

$\forall x \in H, h(x) = f(x)$. Therefore, $x \neq y \Rightarrow f(x) \neq f(y) \Rightarrow h(x) \neq h(y)$

Case 2: $x \in \overline{H} \ \ \& \ \ y \in \overline{H}$

$\forall x \in \overline{H}, h(x) = g^{-1}(x)$. Since g is injective, g^{-1} is well-defined, and thus $g^{-1}(x) \neq g^{-1}(y) \Rightarrow h(x) \neq h(y)$

Case 3 : $x \in H \ \ \& \ \ y \in \overline{H}$ For $x \in H$, $h(x) = f(x)$
For $y \in \overline{H}$, $h(y) = g^{-1}(y)$

We need to prove $h(x) \neq g^{-1}(y)$

We know, $g(\overline{f(H)}) = \overline{H}$. As g^{-1} is well defined, $\Rightarrow g^{-1}(\overline{H}) \subseteq \overline{f(H)}$
. Therefore, $g^{-1}(H) \nsubseteq f(H)$. Moreover, as $g^{-1}(\overline{H}) \subseteq \overline{f(H)}$, $\nexists u \in \overline{H}$, such that $g^{-1}(u) \in f(H)$. Thus, for $x \in H \ \ \& \ \ y \in \overline{H}$, $g^{-1}(y) \neq f(x)$. Hence proved.

Surjective

To prove, $range(h) = B$. That is, $\forall y \in B, \exists x \in A$, such that $h(x) = y$. Assume, $y \in f(H)$. Given that $\forall x in H, h(x) = f(x)$, and because $y \in f(H)$, $\exists x, f(x) = y$.

Now, for $x \in \overline{f(H)}$. We know,

$$\overline{H} = g(\overline{f(H)}) \tag{34.90}$$

And that $g^{-1}(x)$ is defined $\forall x \in \overline{H}$ (already proved). Since g^{-1} is obviously injective (if $x \neq y$ and $g^{-1}(x) = g^{-1}(y) = a$, then $g(a)$ is not defined), we can apply g^{-1} on both sides of 34.90, to get

$$g^{-1}(\overline{H}) \subseteq \overline{f(H)}$$

As $g{-}1$ is injective, and we know that $|\overline{H}| = g(\overline{f(H)})$, both the sets are of the same size, thus,

$$g^{-1}(\overline{H}) = \overline{f(H)}$$

.

$\forall x \in \overline{f(H)}$, we have a pre-image in $g^{-1}(\overline{H})$. Hence, h is surjective.

From the three parts, we have proven that $h : A \to B$, is a bijective function, constructed from $f : A \to B$ and $g : B \to A$, two injective functions.

□

Instructor : Jayalal Sarma
Scribe : Mohit Singla (*TA:* JS)
Date : Nov 23, 2020
Status : α

Lecture
34

Extremal Set Theory

34.1 Recall Sperner Theorem

Theorem 34.1.1. *Let F be the family of subsets of $[n] \mid \forall\ A, B \in F$, $A \nsubseteq B$.*

$$|F| \leq \binom{n}{n/2}$$

The size is the width of subset boolean poset.

Proof. **Tightness:-** The bound is tight as we have example $F = \{A \subseteq [n] \mid |A| = n/2\}$

A permutation $\pi \in S_n$ is said to meet $A \subseteq \{1, 2, \ldots, n\}$ if A forms prefix of π. Let's say $|A| = k$ then π said to meet A if $A = \{\pi(1), \pi(2), \ldots, \pi(k)\}$.

Consider each subset in F and consider permutations meeting them, As we are taking subsets from F, they are incomparable. Hence a single permutation can not meet both A and B. So,

$$\sum_{A \in F} \left| \{\pi | \pi\ meets\ A\} \right| \leq n!$$

Now number of permutations that can meet set A of size k is $k! \times (n-k)!$.So,

$$\sum_{A \in F} |A|! \times (n - |A|)! \quad \leq \quad n!$$

$$\boxed{\sum_{A \in F} \frac{1}{\binom{n}{|A|}} \quad \leq \quad 1}$$

The above inequality is known as **LYM Inequality - Lubell–Yamamoto–Meshalkin Inequality,**

We can substitute $\binom{n}{\frac{n}{2}}$ in place of $|A|$ and the inequality still holds.

$$\begin{aligned}\sum_{A\in F}\frac{1}{\binom{n}{\frac{n}{2}}} &\leq 1\\ \sum_{A\in F}1 &\leq \binom{n}{\frac{n}{2}}\\ |F| &\leq \binom{n}{\frac{n}{2}}\end{aligned}$$

□

34.2 Disussing family of subsets with certain intersection properties

The **Sperner theorem** we did is sample of family of subsets with intersection properties : for any pair $A, B \subseteq F \mid A \cap B \neq A$

Question:- Consider family of subsets of $[n]$ such that for any pair $A, B \subseteq [n]$, $A \cap B \neq \phi$. How large can F be?

Building up:- The size can be as large a 2^n but will not be equal to 2^n as if we take all singleton sets, their pairwise intersection is empty.
The size can be 2^{n-1}, $F = \{B \cup \{n\} \mid B \subseteq [n-1]\}$. Example for $n = 3$: $F = \{\{3\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. Can it be larger than 2^{n-1} ?

Theorem 34.2.1. *The size of intersection family is atmost 2^{n-1}. And this bound is tight as we already have an example for any n.*

Proof. By the property of family of subsets, its clear that if any subset $A \in F \Rightarrow A^{\complement} \notin F$. If both A and $A^{\complement}$ are present then their intersection is empty. So for every subset in F there is subset not present in F. Hence $|F| \leq 2^{n-1}$. □

Special cases of above family:-

1. The intersection size is always λ i.e. $A, B \subseteq F \mid |A \cap B| = \lambda$. Claim : $|F| \leq n$.
2. The family is k-uniform.

We will answer above two cases using **Linear Algebra** techniques. Before proving above claims lets take a look at some other problem that uses similar proof techniques.

34.2.1 Odd Town Problem

- n people in an odd town form m clubs $C_1, C_2, \ldots, C_m$.
- Each club has an odd number of members.
- Each pair of clubs have an even number of common members.
- No two clubs have same set of members.

Theorem 34.2.2. *In Odd Town problem $m \leq n$.*

Proof. Associate a n-sized 0-1 vector v_i to each club C_i, such that $v_i[j] = 1$ if j is member of club C_i else 0. It is now sufficient to prove that we cannot have more than n different vectors. Theses vectors are defined over field $\mathbb{F}_2^n$. The field $\mathbb{F}_2^n$ can be considered as structure where both addition and multiplication is modulo 2 and every element is either 0 or 1.

If we can show that the set of vectors $v_1, v_2, \ldots, v_m$ are linearly independent over $\mathbb{F}_2^n$, then it's implied that $m \leq n$ as number of independent vectors are always less than or equal to dimension.

Consider the inner product $\langle v_i, v_j \rangle$. In $\mathbb{F}_2^n$, $\langle a, b \rangle = (\sum_1^n a_i b_i)\%2$.

Case 1: $i \neq j$, $\langle v_i, v_j \rangle = \sum_{k=1}^n v_i[k]v_j[k] = |C_i \cap C_j|\%2 = 0$. As the size of intersection is always $even$.

Case 2: $i = j$, $\langle v_i, v_j \rangle = \sum_{k=1}^n v_i[k]v_i[k] = (\sum_{k=1}^n v_i[k])\%2 = 1$. As the size of each club is *odd*.

Suppose the set of vectors $v_1, v_2, \ldots, v_m$ are not linearly independent. Then these exist non-trivial solution to the equation: $\sum \lambda_i v_i = 0$. If we can show that only solution to above equation is when all λ_i is **0**, then we are done with proof.

Take inner product of $\sum \lambda_i v_i$ with v_j for every j. As $\sum \lambda_i v_i$ is **0** vector.

$$\left\langle \sum \lambda_i v_i, v_j \right\rangle = 0$$

$$\sum \langle \lambda_i v_i, v_j \rangle = 0$$

$$\sum \lambda_i \langle v_i, v_j \rangle = 0$$

As we saw earlier, when $i \neq j$ $\langle v_i, v_j \rangle = 0$. And when $i = j$, $\langle v_i, v_j \rangle = 1$. So the above equation can be written as:

$$\lambda_j \langle v_j, v_j \rangle = 0$$

For above equation to satisfy $\lambda_j = 0$, this can be shown for all λs. Hence proved $m \leq n$. □

In next lecture we will analyse the special cases of intersection family.

Instructor : Jayalal Sarma
Scribe : Mohit Singla (*TA:* JS)
Date : Nov 25, 2020
Status : α

Lecture
35

More on Linear Algebra Techniques

35.1 Recall some intersection families

The family F such that for any two subsets $A, B \subseteq F \mid A \cap B \neq \phi$, then $|F| \leq 2^{n-1}$. Then we questioned two special cases of this intersection family.

1. The intersection size is always λ i.e. $A, B \subseteq F \mid |A \cap B| = \lambda$. Claim : $\boxed{|F| \leq n}$. This inequality is knows as **Fisher's Inequality**.
2. The family is k-uniform λ i.e. $A \subseteq F \mid |A| = k$. Claim : $\boxed{|F| \leq \binom{n-1}{k-1}}$. This is knows as **Edrös Ko-Rado Theorem**.

We saw **Odd-Town Theorem** which states that if:

- n people in an odd town form m clubs $C_1, C_2, \ldots, C_m$.
- Each club has an odd number of members.
- Each pair of clubs have an even number of common members.
- No two clubs have same set of members.

Then $m \leq n$. We proved this inequality using **Linear Algebra**. We associated one vector with each club and showed that all the vectors are linearly independent. As the dimension is n, there can not be more that n linearly independent vectors.

35.2 Fisher's Inequality (1940s)

We will look at proof by **Babai Frankl** in 1992.

Theorem 35.2.1. *The family F such that intersection size is always λ i.e. $A, B \subseteq F \mid |A \cap B| = k$. then $|F| \leq n$.*

Proof. Associate a n-sized 0-1 vector v_i to each club C_i, such that $v_i[j] = 1$ if j is member of club C_i else 0. Each $v_i \in \mathbb{R}^n$.

Consider the inner product $\langle v_i, v_j \rangle$. In $\mathbb{R}^n$, $\langle a, b \rangle = (\sum_1^n a_i b_i)$.

Case 1: $i \neq j$, $\langle v_i, v_j \rangle = \sum_{k=1}^n v_i[k]v_j[k] = |C_i \cap C_j| = k$. As the size of intersection is always k.

Case 2: $i = j$, $\langle v_i, v_j \rangle = \sum_{k=1}^n v_i[k]v_i[k] = \sum_{k=1}^n v_i[k] = |C_i|$.

We will show the vectors are linearly independent. Suppose the set of vectors $v_1, v_2, \ldots, v_m$ are not linearly independent. Then these exist non-trivial solution to the equation: $\sum \lambda_i v_i = \mathbf{0}$. We can write

$$\left\langle \sum_1^m \lambda_i v_i, \sum_1^m \lambda_i v_i \right\rangle = 0$$

$$\Rightarrow \quad \sum_1^m \lambda_i^2 \langle v_i, v_i \rangle + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j \langle v_i, v_j \rangle = 0$$

$$\Rightarrow \quad \sum_1^m \lambda_i^2 |C_i| + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j k = 0$$

$$\Rightarrow \quad \sum_1^m \lambda_i^2 (|C_i| - k) + \sum_1^m \lambda_i^2 k + \sum_{1 \leq i \neq j \leq m} \lambda_i \lambda_j k = 0$$

$$\Rightarrow \quad \sum_1^m \lambda_i^2 (|C_i| - k) + (\sum_1^m \lambda_i)^2 k = 0$$

Suppose there exist a C_i such that $|C_i| = k$, then no other club size can be k. If there are two clubs with size k and their intersection is also of size k, then both the clubs have to be equal. so at-most one club can have size k. Now as the intersection size is always k, for all j, $C_i \subseteq C_j$ must hold as the size of C_i is k and $|C_i \cap C_j| = k$. Note for all C_i, $|C_i| \geq k$ as the intersection size with any other club is of size k.

So in the expression $\sum_1^m \lambda_i^2 (|C_i| - k) + (\sum_1^m \lambda_i)^2 k$, both the parts in summation are non-negative. For right part to be zero, $\sum_1^m \lambda_i = 0$. Not all λs are zero but their summation is, so there are atleast 2 λs which are non-zero.

Now lets focus on left part. Each term $\lambda_i^2 (|C_i| - k)$ is non-negative. There are atleast 2 λs

which are non-zero but atmost one $(|C_i| - k)$ can be zero. So the summation is always positive. So if there are non-zero λs then summation cannot be equated to zero. This leads to contradiction in assumption that there exists non-zero λs which satisfy above equation.

Hence proved that vectors $v_1, v_2, \ldots, v_m$ are linearly independent. So $m \leq n$. □

35.3 Application of Fisher Inequality and Odd Town Theorem

35.3.1 Ramsey Number

Definition:$R(s,t)$ is minimum number (n) of vertices required in complete graph such that 2-edge coloring (red and blue colors) of this K_n produces either red K_s or blue K_t.

Earlier we have proved $R(t,t) > 2^t$ i.e. there exist a 2-edge coloring of K_{2^t} such that there is no red K_t or blue K_t. We proved this using probabilistic method. We chose color of each edge uniformly at random and observed that the probability of graph having either red K_t or blue K_t is strictly less than 1. So there exist a graph with neither has red K_t nor blue K_t, we did not explicitly drew thew the graph. This proof was **non-constructive**.

If we want a constructive example for lower-bound, we have much weaker lower bound.

35.3.2 Constructive lower bound for diagonal Ramsey number

Claim 35.3.1. $R(t+1, t+1) > \binom{t}{3}$

We will be able to show a construction to prove this claim.

Proof. We need to show there exist a 2-edge coloring of $K_{\binom{t}{3}}$ such that there is no red K_{t+1} or blue K_{t+1}.

$n = \binom{t}{3}$. Interpret each vertex as 3-sized subset of set $\{1, 2, \ldots, t\}$. Let $A, B \in V$, then $A, B \subseteq [t]$ and $|A| = |B| = 3$. Color edge AB red if $|A \cap B| = 0$ or 2. As size of each subset is 3 and all are pairwise distinct, the intersection size can only be 0, 1 or 2. Color edge AB blue if $|A \cap B| = 1$.

Lets look for blue K_{t+1}. Consider F as family consisting 3-sized subsets of $[t]$ such that intersection size is 1. These subsets in F will represent the vertices corresponding to blue edges as described earlier. By Fishers theorem we know $|F| \leq t$. There are atmost t vertices available so there cannot be K_{t+1}.

Lets look for red K_{t+1}. Consider F as family consisting 3-sized subsets of $[t]$ such that intersection size is even. These subsets in F will represent the vertices corresponding to red

edges as described earlier. Now we have all subsets of odd size and intersection size even. All conditions required in Odd Town theorem are satisfied, so by the theorem $|F| \leq t$. There are atmost t vertices available so there cannot be K_{t+1}.

Hence proved. □

35.4 Edrös Ko-Rado Theorem (Discovered-1938, Presented-1962)

Lemma 35.4.1. *Let C be a cycle of length n (n edges and n vertices). Let H be family of paths in C of fixed length k where $k \leq \frac{n}{2}$. Assume any paths in H have an common edge. Then $|H| \leq k$.*

Proof. Pick a path $p = (v_1, v_2, \ldots v_{k+1})$. All other paths have to intersect with this path. A path here is contiguous set of edges in cycle. Lets analyse how other paths look like. No other path can start from v_1, as it will end up being the same path p. No path can start at v_{k+1}, as $k \leq \frac{n}{2}$ and path starting at v_{k+1} will not have any edge common with p. Similarly no path can end at v_1 and v_{k+1}. So paths can start or end at $v_2, v_3 \ldots v_k$. Note if there is a path that starts at v_j, we cannot include path ending at v_j as these two paths will not have any common edge. So there can at-most be $k-1$ other paths. Hence $|H| \leq k$. □

Theorem 35.4.2 (Erdös-Ko-Rado Theorem). *F is k-uniform where $k \leq \frac{n}{2}$, family of subsets of $[n]$ such that for every $A, B \subseteq F$, $A \cap B \neq \phi$. Note if $k > \frac{n}{2}$, then every pair of subsets trivially has non-empty intersection. Then $|F| \leq \binom{n-1}{k-1}$*

Proof. Before we prove the theorem, to get a feel, we construct an example first. And this example also will prove that the above theorem is tight.

Tightness: Consider the family.

$$F_k = \{\{n\} \cup B \mid B \subseteq [n-1], |B| = k-1\}$$

Since n is there in every set in the family, the family is an intersecting family. All sets have size k and hence it is k-uniform. By definition, $|F_k| = \binom{n-1}{k-1}$. Thus the claim is tight as we have an example for any k. It turns out that these are the only tight examples when $k < \frac{n}{2}$.

When n is even and $k = n/2$, there is one more tight example. We can take F_k such that for every $\frac{n}{2}$-sized subset of $[n]$, we take either that subset or its complement in F.

$$|F_k| = \binom{n}{n/2} * \frac{1}{2} = \frac{n}{n/2} * \binom{n-1}{n/2-1} * \frac{1}{2} = \binom{n-1}{n/2-1}$$

Proof of the Erdös-Ko-Rado Theorem: We will discuss the proof by **Katona (1972)** using cycle permutation argument.

Assume someone invited all of the n people from the town to a party. These n people are members of clubs $C_1, C_2, \ldots, C_m$ where each club is of size k and every pair of intersection is non-empty. The party has round table with n labelled chairs. Host wants to seat the club members contiguously. But of course he may not be able to since there may be contradictory requirements across clubs since members can be common.

However, in an attempt to maximise the seating satisfaction of the club members, he decided to try all $n!$ permutations. Lets define a Matrix H with $n!$ rows indexing the permutation number which represents seating arrangement. The columns are indexed by club $C_1, C_2, \ldots, C_m$, so total m columns. The entries of the matrix defined as follows. For $\sigma \in S_n, j \in [m]$:

$$H(\sigma, j) = \begin{cases} 1 & \text{if } \sigma \text{ seats members of club } C_j \text{ contiguously} \\ 0 & \text{otherwise} \end{cases}$$

Let c be the number of ones in matrix H. we will count c in two different ways.

Count 1 - Row-wise first: For a given permutation, each club seated contiguously is a path in the cycle. The guests correspond to edges. As the family of clubs is an intersecting family, by above lemma we know that in each row there can be atmost k ones. so $c \leq k * n!$

Count 2 : Column-wise first: As we are considering all the permutations possible, the number of times each club appears contiguously will be the same. In fact a club will appear contiguously in $nk!(n-k)!$ permutations. First choose the starting index from n positions, then permute the members inside group, and then permute the members outside group. There are m columns, so $c = mnk!(n-k)!$.

Using the above two counts,

$$\begin{aligned} m\ n\ k!\ (n-k)! &\leq k\ n! \\ m &\leq \frac{kn!}{nk!(n-k)!} \leq \frac{(n-1)!}{(k-1)!(n-k)!} \leq \binom{n-1}{k-1} \end{aligned}$$

□

Instructor : Jayalal Sarma
Scribe : Banavath Tarun (*TA:* JS)
Date : Nov 27, 2020
Status : α

Lecture
37

Generalization of linear algebraic method

37.1 Running problems

1. **Intersecting family** : Let $\mathcal{F}$ be family of subsets of $\{1, 2, 3, ..., n\}$ and is called Intersecting family, if every two subsets in these family intersect (i.e. $\forall A, B \in \mathcal{F}, \quad A \cap B \neq \phi$), and we have seen that $|\mathcal{F}| \leq 2^{n-1}$.

2. **Intersecting family with fixed size λ (Fisher's Inequality)** : Similarly, when $\mathcal{F}$ is a family of subsets of $\{1, 2, 3, ..., n\}$ such that $\forall A, B \in \mathcal{F}, \quad |A \cap B| = \lambda$, then size of family is not too large and is given as $|\mathcal{F}| \leq n$

   techniques used in Fisher's inequality : Odd town problem, linear algebra method.

In this lecture, we discuss the theorems involving polynomial methods (or) function space methods.

proof techniques for polynomial method (or) function space methods includes 3 steps:

1. Associate a polynomial in n-variables with each element
2. prove that polynomials are linearly independent
3. Bound the dimensions of space of polynomials

37.2 Independence criterion Tool and Two-distance set

Lemma 37.2.1. *(**Independence criterion Tool**)* $\forall\ 1 \leq i \leq m$, *let* $f_i : \Omega \longrightarrow \mathbb{F}$ *be a function,* $v_i \in \Omega$ *such that it satisfies the following two conditions :*

1. $f_i(v_i) \neq 0,\ \forall\ i$
2. $f_i(v_j) = 0,\ \forall\ 1 \leq i < j \leq m$

then $\{f_1, f_2, f_3, ..., f_m\}$ are linearly independent in $\mathbb{F}^\Omega$. (Here each function f_i is a element in $\mathbb{F}^\Omega$ i.e. a vector)

Proof. Suppose $\exists \lambda_1, \lambda_2, \lambda_3, ..., \lambda_m \in \mathbb{F}$ such that $F = \sum_{i=1}^{m} \lambda_i f_i = 0$ and suppose there are dependent, where not all $\lambda_i = 0$, then there is a contradiction. Let j be the largest index (rightmost) such that $\lambda_j \neq 0$. Substitute v_j to the above function F. We then have $F(v_j) = \sum_{i=1}^{m} \lambda_i f_i(v_j) = \lambda_j f_j(v_j)$ (because $\forall i > j \ \lambda_i = 0$ by choice of j and $\forall i < j$ the term $f_i(v_j) = 0$ by second condition) then $\lambda_j f_j(v_j) = 0$. Since $f_j(v_j) \neq 0$, λ_j should be zero, but $\lambda_j \neq 0$ from above assumption. Thus it contradicts the fact that $\exists \ \lambda_1, \lambda_2, \lambda_3, ..., \lambda_m \in \mathbb{F}$ that are dependent. □

Claim 37.2.2. *Let $a_1, a_2, ..., a_m$ be m points in $\mathbb{R}^n$, such that all pair-wise distances are unique, them relation between m and n is given as : $m \leq n + 1$*

What if we relax the condition in above claim and require that there are two possible distances c, d, so that any pairwise distance is either c or d? Such a set is called a two-distance set.
Below theorem is an example of demonstration of a polynomial method (or) function space method.

Theorem 37.2.3. *(**Two-distance set**) Consider a two-distance set, a set $S = \{a_1, a_2, a_3, ..., a_m\}$ is said to two-distance set, if $\exists \ d_1, d_2$ (two fixed distances) such that $\forall a_i, a_j \in S$, satisfy the relation $dist(a_i, a_j) = d_1$ or $dist(a_i, a_j) = d_2$ (where $dist(a_i, a_j)$ is the distance between the two points a_i, a_j in $\mathbb{R}^n$). Then the relation between m (size of two-distance set) and n (dimension of elements in two-distance set) is given as : $m \leq \binom{n}{2} + 3n + 2$.*

Proof. We Solve it using polynomial method (or) function space methods that follows the three steps as already mentioned.

step1 (Associate a polynomial) : Associate a polynomial $P_i(x_1, x_2, x_3, ..., x_n)$ for each element a_i in $S = \{a_1, a_2, a_3, ..., a_m\}$ with some properties, so that we can prove independence in these polynomials. As seen in above lemma the functions f_i's are polynomial P_i's here and $\Omega = \mathbb{R}^n$ in this case (since $\forall i, \ a_i \in \mathbb{R}^n$). Let $x = (x_1, x_2, x_3, ..., x_n)$ be a n-vector then polynomial : $\forall \ 1 \leq i \leq m \ P_i(x) = \left(||x - a_i||^2 - {d_1}^2\right)\left(||x - a_i||^2 - {d_2}^2\right)$.

step2 (prove that polynomials are linearly independent) : The above polynomials defined satisfies the two conditions of independent criterion tool. i.e.

1. $P_i(a_i) \neq 0, \ \forall i$. P_i satisfy the first condition because $P_i(a_i) = \left(||a_i - a_i||^2 - {d_1}^2\right)\left(||a_i - a_i||^2 - {d_2}^2\right) = {d_1}^2{d_2}^2 \neq 0$ (since $d_1, d_2 \neq 0$), So $P_i(a_i) \neq 0, \ \forall i$
2. $P_i(a_j) = 0, \forall 1 \leq i < j \leq m$. P_i also satisfy the second condition because $P_i(a_j) = \left(||a_j - a_i||^2 - {d_1}^2\right)\left(||a_j - a_i||^2 - {d_2}^2\right)$ and also $||a_j - a_i||^2 = {d_1}^2$ (or) $||a_j - a_i||^2 = {d_2}^2$ from definition of two-distance set. So $P_i(a_j) = \left(||a_j - a_i||^2 - {d_1}^2\right)\left(||a_j - a_i||^2 - {d_2}^2\right) = 0, \forall 1 \leq i < j \leq m$

step3 (Bound the dimension of space of polynomials) : The polynomial that we have constructed has a property that we wanted and all these polynomials are now independent by independent criteria. Also after expanding the polynomial $P_i(x = (x_1, x_2, ...x_n)) = \left(||x - a_i||^2 - {d_1}^2\right)\left(||x - a_i||^2 - {d_2}^2\right)$, we can see that the polynomial have only following type of terms:

$$(\sum_{i=1}^{n} {x_i}^2)^2, \sum_i {x_i}^2 x_j, \sum_{1 \leq i \leq j \leq n} x_i x_j, \sum_{i=1}^{n} x_i, 1$$

. i.e.

- Number of terms of form $(\sum_{i=1}^{n} {x_i}^2)^2$ are 1.
- Number of terms of form $\sum_i {x_i}^2 x_j$ are n.
- Number of terms of form $\sum_{1 \leq i \leq j \leq n} x_i x_j$ are $\binom{n}{2} + n$.
- Number of terms of form $\sum_{i=1}^{n} x_i$ are n.
- Number of constant terms are 1.

So in total we have $1 + n + \binom{n}{2} + n + n + 1 = \binom{n}{2} + 3n + 2$ number of terms i.e. any polynomial in our family can be expressed as a linear combination in $\binom{n}{2} + 3n + 2$ number of terms, which means that dimensions of set of polynomials that we are looking cannot be greater than $\binom{n}{2} + 3n + 2$ because these are the simplified polynomials using which we can express all the polynomials in our family. So, the dimension of underline space is bounded by $\binom{n}{2} + 3n + 2$ and hence

$$m \leq \binom{n}{2} + 3n + 2$$

because there cannot be more than $\binom{n}{2} + 3n + 2$ number of independent polynomials (or) vectors. □

37.3 Frankl-Wilson Theorem

Theorem 37.3.1. *Let $\mathcal{F}$ be family of subsets of $[n]$ and let L be subset of $[n]$ ($L \subseteq \{1, 2, 3, ..., n\}$) such that $\forall A, B \in \mathcal{F}$, $|A \cap B| \in L$, then $|\mathcal{F}| \leq \sum_{i=1}^{|L|} \binom{n}{i}$. This theorem is also known as **Frankl-Wilson Theorem**, which is a Generalization of **Fisher's theorem**.*

Proof. Let $\mathcal{F} = \{A_1, A_2, ..., A_m\}$ be family of subsets of $[n]$, $L = l_1, l_2, ..., l_s$ be a subset of $[n]$ such that $\forall i, j$ $(1 \leq i, j \leq n)$ $\exists$ k $(1 \leq k \leq s)$ such that $|A_i \cap A_j| = l_k$. Let v_i be the characteristic vector of A_i, $v_i \in \Omega = \mathbb{R}^n$ $\left(\text{where} < v_i, v_i >= |A_i| \text{ and} < v_i, v_j >= |A_i \cap A_j|\right)$ and we can assume that A_1 to A_m is ordered such that sizes are non-decreasing order (or) rename them accordingly. We then have

$$|A_1| \leq |A_2| \leq |A_3| ..... \leq |A_m|.$$

Now We Solve the proof using polynomial method (or) function space methods that follows the three steps as already mentioned.

step1 (Associate a polynomial) : Associate a polynomial $P_i(x_1, x_2, ..., x_n)$ for each element A_i. So the polynomial that we are going to define is as follows:

$$P_i\big(x = (x_1, x_2, ..., x_n)\big) = \prod_{k\,:\,l_k<|A_i|} \big(< v_i, x > -l_k\big)$$

where $x = (x_1, x_2, ..., x_n)$ is a n-vector.

step2 (prove that polynomials are linearly independent : The above polynomials defined satisfies the two conditions of independent criterion tool.

1. when $x = v_i$, we have:

$$P_i(v_i) = \prod_{k\,:\,l_k<|A_i|} \big(< v_i, v_i > -l_k\big) = \prod_{k:l_k<|A_i|} \Big(|A_i| - l_k\Big) \neq 0$$

   so, $P_i(v_i) \neq 0,\ \forall i$

2. when $x = v_j$ and $i < j$, we have:

$$P_i(v_j) = \prod_{k\,:\,l_k<|A_i|} \big(< v_i, v_j > -l_k\big) = \prod_{k:l_k<|A_i|} \big(|A_i \cap A_j| - l_k\big) = 0$$

   Since $|A_i \cap A_j|$ must be one of the $l_p \in L$ and this p must satisfy $l_p < |A_i|$, because the intersection size $|A_i \cap A_j|$ cannot be more than A_i. So, $P_i(v_j) = 0, \forall 1 \leq i < j \leq m$ Now we have this polynomial $P_i\big(x = (x_1, x_2, ..., x_n)\big) = \prod_{k\,:\,l_k<|A_i|} \big(< v_i, x > -l_k\big)$ that satisfies the two conditions of Independent criteria and hence $P_1, P_2, ..., P_n$ are linearly independent as polynomials (or) as coefficients of vectors.

step3 (Bound the dimension of space of polynomials) : Estimating the underlying dimensions (here, space of polynomials): We need to compute the dimension of space containing all these polynomials. Since we are using only $0/1$ vectors here we can reduce the dimension by replacing the higher powers ${x_i}^k$ with x_i, this process does not change the linear dependence property and we still get same conditions. Now each term monomial looks like $x_1x_2x_3$..... Polynomials with these properties (i.e. each monomial with every individual variable degree to be at most one) are called as multilinear polynomials. So the polynomials under consideration lives in the space of multilinear polynomials of degree at most s.
Let us look at the example on multilinear polynomials when $n = 3$ and degree=2, the only terms correspond to these multilinear polynomials looks like:

$$x_1x_2,\ x_2x_3,\ x_1x_3,\ x_1,\ x_2,\ x_3,\ 1$$

there are 7 terms and an example of these multilinear polynomial with real coefficients looks like: $5x_1x_2 + 6x_1x_3 + 5x_2x_3 + 3x_1 + 2x_2 + x_3 + 6$ and dimension of this multilinear polynomial example is 7. The number of monomials we can have with that much degree is the bound for dimension. So in general when degree=k and number of variables is n, then number of monomials in this multilinear polynomial is $\binom{n}{k}$ (i.e. select k elements from $\{1, 2, 3, ..., n\}$ and associate a monomial with corresponding variables). But now we have that degree is at most s, so we need to sum the result $\binom{n}{k}$ overall values of k (i.e. $1 \leq k \leq s$). So,

$$Dimension\ of\ space = \#\ of\ subsets\ of\ \{1, 2, 3, ..., n\}\ of\ size\ \leq s = \sum_{k=1}^{s} \binom{n}{k}$$

and hence

$$m \leq Dimension \leq \sum_{k=1}^{|L|} \binom{n}{k}$$

□

Theorem 37.3.2. *Let $\mathcal{F}$ be family of subsets of $[n]$, p be a prime and L be subset of $\{0, 1, 2, 3, ..., p-1\}$, ($L \in \{0, 1, 2, 3, ..., p-1\}$) such that $\forall A, B \in F, \quad |A \cap B| \in L(mod\ p)$ and $|A| \notin L(mod\ p)$, then $|\mathcal{F}| \leq \sum_{i=1}^{|L|} \binom{n}{i}$. This theorem is proved by **Ray-choudhuri Wilson**, which is a Generalization of **odd-town problem**.*

Theorem 37.3.3. *Let $\mathcal{F}$ be a k-Uniform family of subsets of $[n]$ and let L be subset of $[n]$, ($L \subseteq \{1, 2, 3, ..., n\}$) such that $\mathcal{F}$ is $L-$intersecting (i.e. $\forall A, B \in F, \quad |A \cap B| \in L$), then the size of $\mathcal{F}$ is given as : $|\mathcal{F}| \leq \binom{n}{|L|}$. This theorem is proved by **Ray-choudhuri Wilson***

The above two theorems are also applications of polynomial method and process involved in proving them is similar to that we have done before.

Chapter 38

Supplementary Material

38.1 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 38.1.1. 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 38.1.2. 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 38.1.3 (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 38.1.4 (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".

38.2 Exercises

Exercise 38.3. 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 38.4. Prove the following identities using double counting method:

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

Exercise 38.5. 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

Exercise 38.6. 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.

Exercise 38.7. Prove the following by combinatorial arguments

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

Exercise 38.8.

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.

38.9 Problem Sets

38.9.1 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 :

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