
Lecture Notes on

Algorithmic Algebra

Jayalal Sarma
Department of Computer Science and Engineering
IIT Madras, Chennai 600036

Draft—August 9, 2015 and forever

List of Scribes

Lecture 1	<i>K Dinesh</i>	1
Lecture 2	<i>K Dinesh</i>	4
Lecture 3	<i>K Dinesh</i>	7
Lecture 4	<i>Ramya C</i>	10

Table of Contents

Lecture 1	Introduction, Motivation and the Language	1
1.1	Overview of the course. Administrative, Academic policies	1
1.2	Introduction and Motivation	2
1.3	Overview of the course	3
Lecture 2	Algebraic Approach to Primality Testing	4
2.1	Application to Number Theory	4
Lecture 3	Algebraic Approach to finding Perfect Matchings in Graphs	7
3.1	Application to Graph algorithms	7
Lecture 4	Graphs, Groups and Generators	10
4.1	Graph Isomorphism	10

Preface

This lecture notes are produced as a part of the course *CS6842: Algorithmic Algebra* which was a course offered during August to November semester in 2013 and 2015 at the CSE Department of IIT Madras.

Acknowledgements

Thanks to Alexander Shrestov for creating a nice template for lecture notes which are being used in this document.

CS6842 – Algorithmic Algebra

Instructor: Jayalal Sarma

Scribe: K Dinesh

Date: Aug 3, 2015

LECTURE

1

Introduction, Motivation and the Language

1.1 Overview of the course. Administrative, Academic policies

1.2 Introduction and Motivation

Main theme of this course is to use algebra to solve computational problems. Let us consider the following two problems :

Plagiarism check Given two C programs P_1 and P_2 , check if they are the same under renaming of variables.

Molecule detection Given two chemical molecules check if they have the same structure.

Consider the following simpler variant of plagiarism checking where the program submitted has just its variables renamed and all other

Note that both these problems can be modelled using a graph. For example, in the second case one could view the given molecules as adjacency matrix. Our aim in both cases is to check if there is isomorphism between two graphs.

DEFINITION 1.1 (Graph Isomorphism). Two graphs $X_1(V_1, E_1)$, $X_2(V_2, E_2)$ are said to be isomorphic if there is a bijective map $\sigma : V_1 \rightarrow V_2$ such that $\forall (u, v) \in V_1 \times V_1$,

$$(u, v) \in E_1 \iff (\sigma(u), \sigma(v)) \in E_2$$

PROBLEM 1.2. The *graph isomorphism problem* is the decision problem of checking if given two graphs X_1, X_2 are isomorphic.

We are also interested in the following special case of the above problem called graph automorphism problem.

DEFINITION 1.3 (Graph Automorphism). For a graph $X(V, E)$, an automorphism of X is a renaming of the vertices of X given by a bijective map $\sigma : V \rightarrow V$ such that $\forall (u, v) \in V \times V$,

$$(u, v) \in E \iff (\sigma(u), \sigma(v)) \in E$$

We are interested in the set of all bijections such that they are automorphisms of X . We denote this by $Aut(X)$.

DEFINITION 1.4. For a graph X on n vertices, $Aut(X) = \{\sigma \mid \sigma : [n] \rightarrow [n], \sigma \text{ is an automorphism of } X\}$

Note that an identity map which takes a vertex to itself always belongs to $Aut(X)$ for all graphs X . Hence the question is : are there any bijections other than the identity map as automorphism of X .

PROBLEM 1.5 (Graph Automorphism Problem). Given a graph X does $Aut(X)$ has any element other than the identity element.

One way to see bijections is via permutations. This is because, every bijection define a permutation and vice versa.

Let X be an n vertex graph. Denote S_n to be the set of all permutations on n elements. Hence $Aut(X)$ can be defined as $\{\sigma \mid \sigma \in S_n \text{ and } \sigma \text{ is an automorphism of } G\}$.

We now show that the set $Aut(X)$ has some nice properties. Given $\sigma_1, \sigma_2 \in Aut(X)$, we can compose two permutations as $\sigma_1 \circ \sigma_2 = (\sigma_1(\sigma_2(1)), \sigma_1(\sigma_2(2)), \dots, \sigma_1(\sigma_2(n)))$. This is same as

applying σ_2 on identity permutation and then applying σ_1 to the result. We show that $Aut(X)$ along with the composition operation \circ gives us many nice properties.

- If $\sigma_1, \sigma_2 \in Aut(X)$, then $\sigma_1 \circ \sigma_2$ is also an automorphism of X . The reason is that for any $(u, v) \in X \times X$, $(u, v) \in E \iff (\sigma_2(u), \sigma_2(v)) \in E$. Now applying σ_1 on the previous tuple, we get that $(\sigma_2(u), \sigma_2(v)) \iff (\sigma_1 \circ \sigma_2(u), \sigma_1 \circ \sigma_2(v)) \in E$. Hence $(u, v) \in E \iff (\sigma_1 \circ \sigma_2(u), \sigma_1 \circ \sigma_2(v)) \in E$. This tells that $Aut(X)$ is *closed* under \circ .
- The composition operation is also *associative*.
- *Identity* permutation belongs to $Aut(X)$ as observed before.
- Since we are considering bijections, it is natural to consider *inverse* for a permutation σ denoted σ^{-1} with the property that $\sigma \circ \sigma^{-1}$ is identity permutation.

We gave a definition of inverse for an arbitrary permutation. But then a natural question is : given $\sigma \in Aut(X)$, is it true that σ^{-1} also belongs to $Aut(X)$. It turns out that it is true.

CLAIM 1.6. For the graph $X(V, E)$ $\sigma \in Aut(X) \iff \sigma^{-1} \in Aut(X)$

Proof. Recall that $\sigma \in Aut(G)$ iff $\forall (u, v) \in V \times V$, $(u, v) \in E \iff (\sigma(u), \sigma(v)) \in E$. In particular, this must be true for $(\sigma^{-1}(u), \sigma^{-1}(v))$ also. This means,

$$(\sigma^{-1}(u), \sigma^{-1}(v)) \in E \iff (\sigma(\sigma^{-1}(u)), \sigma(\sigma^{-1}(v))) \in E$$

By definition of σ^{-1} we get that $(\sigma^{-1}(u), \sigma^{-1}(v)) \in E \iff (u, v) \in E$. This shows that $\sigma^{-1} \in Aut(X)$ \square

Objects which satisfy these kind of properties are called groups.

1.3 Overview of the course

There are two major themes.

- Algorithms for permutation groups.
- Algorithms for polynomials.

Algebraic Approach to Primality Testing

In this lecture, we will see an algebraic approach to solving a fundamental problem in Number Theory.

2.1 Application to Number Theory

Following is an algorithmic question that we are interested.

PROBLEM 2.1. Given a number n in its binary representation, check if it is a prime or not in time $O(\text{poly}(\log N))$.

NOTE 2.2. *The trivial algorithms that we can think of will depend on n and hence takes time exponential in its input representation.*

Consider the following property about prime number proved by Fermat which is of interest in this context.

THEOREM 2.3 (Fermat's Little Theorem). *If N is a prime, then $\forall a, 1 \leq a \leq N - 1$,*

$$a^N = a \pmod{N}$$

Proof. Fix an $a \in \{1, 2, \dots, N - 1\}$. Now consider the sequence $a, 2a, \dots, (N - 1)a$. The question we ask is : can any two of the numbers in this sequence be the same modulo N . We claim that this cannot happen. We give a proof by contradiction : suppose that there are two distinct r, s with $1 \leq r < s \leq N - 1$ and $sa = ra \pmod{N}$. Then clearly $N|(s - r)a$ which means $N|a$ or $N|(s - r)$. But both cannot happen as $a, s - r$ are strictly smaller than N .

This gives that all the N numbers in our list modulo N are distinct. Hence all numbers from $1, 2, \dots, N - 1$ appear in the list when we go modulo N . Taking product of the list and the list modulo N , we get

$$(N - 1)!a^{N-1} = (N - 1)! \pmod{N}$$

By cancelling $(N - 1)!$, we get that $a^{N-1} = 1 \pmod{N}$. □

This tells that the above condition is necessary for a number to be prime. If this test is also sufficient (i.e, if the converse of the above theorem is true), we have a test for checking primality of

a number. But it turns out that this is not true due to the existence of Carmichael numbers which are not prime numbers but satisfy the above test.

So one wants a necessary and sufficient condition which can be used for primality testing. For this, we need the notion of polynomials.

DEFINITION 2.4. A polynomial $p(x) = \sum_{i=0}^d a_i x^i$ with $a_d \neq 0$ denotes a polynomial in one variable x of degree d . Here a_i s are called coefficients and each term excluding the coefficient is called a monomial. **A polynomial is said to be identically zero, if all the coefficients are zero.**

A polynomial time algorithm for this problem has been found in 2002 by Manindra Agarwal, Neeraj Kayal and Nitin Saxena (called as the AKS algorithm). In their result, they used the following polynomial characterisation for a prime number.

THEOREM 2.5 (Polynomial formulation (Agarwal-Biswas 1999)). *Let $N \geq 1$ be an integer. Define a polynomial $p_N(z) = (1+z)^N - 1 - z^N$. Then*

$$p_N(z) \equiv 0 \pmod{N} \iff N \text{ is prime}$$

By the notation $p_N(z) \equiv 0 \pmod{N}$, we mean that for all $a \in \{1, 2, \dots, N-1\}$, $p_N(a) \equiv 0 \pmod{N}$.

Hence checking if N is prime or not boils down to checking if $p_N(z)$ is identically 0 or not except for the fact that the underlying operations are done modulo N .

Proof of the theorem is as follows.

Proof. Note that $p_N(z) = \sum_{i=1}^{N-1} \binom{N}{i} z^i$ and $\binom{N}{i} = \frac{N(N-1)\dots(N-i+1)}{1 \cdot 2 \dots i}$ with $2 \leq i \leq N-1$. If N is prime, then $\binom{N}{i} = N \times k_i$ for some integer k_i as none of $1, 2, \dots, i$ divides N . Hence $\binom{N}{i} \pmod{N} = 0$ for every i and $p_N(z) \equiv 0 \pmod{N}$ since the polynomial has all coefficients as zero.

If N is composite, we need to show that $p_N(z) \not\equiv 0 \pmod{N}$ which means that we need to produce an $a \in \{1, 2, \dots, N-1\}$ such that $p_N(a) \not\equiv 0 \pmod{N}$. Suppose N is composite. Hence there exists a prime p such that $p \mid N$. Let $p^k \mid N$ where $k \geq 1$ is the largest exponent of p in the prime factorisation of n . Hence $p^{k+1} \nmid N$.

We now need to show that there is an $a \in \{1, 2, \dots, N-1\}$ such that $p_N(a) \not\equiv 0 \pmod{N}$. For this, we first show that $p_N(z)$ is a non zero polynomial by showing that the coefficient of z^i for $i = p$, which is $\binom{N}{p}$, is non zero modulo p^k showing¹ $p_N(z)$ is not a zero polynomial modulo N . As an exercise, the reader is asked to produce an a such that $p_N(a) \not\equiv 0 \pmod{N}$. We now proceed with the proof.

Let $N = g \times p^k$. In $\binom{N}{p}$, p of the denominator divides N . Note that p cannot divide g , for if it does, then $p^{k+1} \mid N$ which is not possible by choice of p and k .

$$\binom{N}{p} = \frac{g \times p^k (N-1) \dots (N-p+1)}{1 \cdot 2 \dots p} = \frac{g \times p^{k-1} (N-1) \dots (N-p+1)}{1 \cdot 2 \dots p-1} \quad (2.1)$$

Hence it must be that p^{k-1} divides $\binom{N}{p}$. This is because, there is no p left now in the denominator to divide N . Now $p^k \nmid \binom{N}{p}$ because, none of the terms $(N-1), \dots, (N-p+1)$ can have p as a factor since all these terms are obtained by subtracting at most $p-1$ times from N . Hence $\binom{N}{p} \not\equiv 0 \pmod{p^k}$. \square

¹Note that if $N \mid \binom{N}{i}$ then $p^k \mid \binom{N}{i}$. Taking contrapositive, we get that $\binom{N}{i} \not\equiv 0 \pmod{p^k}$ implies $\binom{N}{i} \not\equiv 0 \pmod{N}$

Note that Fermat's Little Theorem is a special case of Agarwal-Biswas formulation of primality testing.

EXERCISE 2.6. Derive Fermat's Little Theorem from Agarwal-Biswas theorem. (Hint : Use induction on a)

This shows that checking if the polynomial $p_N(z)$ is a zero polynomial is an if and only if check for primality of N . There are two naive ways to do it. One is to evaluate it at all the numbers from 1 to N or to expand out the polynomial and see if it is identically zero. But both operations are costly.

So checking primality of a number now boils down to checking if a polynomial is identically zero or not. This is a fundamental problem of polynomial identity testing. We will be discussing about polynomial identity testing and AKS algorithm in our next theme.

Algebraic Approach to finding Perfect Matchings in Graphs

3.1 Application to Graph algorithms

Consider the following problem of finding perfect matching.

DEFINITION 3.1 (Finding Perfect Matching). Given a bipartite graph $G(V_1, V_2, E)$, we need to come up with an $E' \subseteq E$ such that $\forall u \in V_1 \cup V_2$, there is exactly one edge incident to it in E' .

We shall give a polynomial formulation for the problem. Given $G(V_1, V_2, E)$ with vertex sets $|V_1| = |V_2| = n$. Define an $n \times n$ matrix A where $A(i, j) = 1$ if $(i, j) \in E$ and is 0 otherwise for all $(i, j) \in V_1 \times V_2$. Recall the determinant of A given by

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^n A_{i, \sigma(i)}$$

where

$$\text{sign}(\sigma) = \begin{cases} -1 & \text{if } \text{inv}(\sigma) \text{ is even} \\ 1 & \text{if } \text{inv}(\sigma) \text{ is odd} \end{cases}$$

and $\text{inv}(\sigma)$ is defined as $|\{(i, j) \mid i < j \text{ and } \sigma(i) > \sigma(j), 1 \leq i < j \leq n\}|$. We denote $f(x) \equiv 0$ to denote that polynomial $f(x)$ is the zero polynomial.

LEMMA 3.2. For the matrix A as defined as before, $\det(A) \neq 0 \Rightarrow G$ has a perfect matching

Proof. Let $\det(A) \neq 0$. Hence there exists a $\sigma \in S_n$ such that $\prod_{i=1}^n A_{i, \sigma(i)} \neq 0$. Hence the edge set $E' = \{(i, \sigma(i)) \mid 1 \leq i \leq n\}$ exists in G and since $\sigma(i) = \sigma(j)$ iff $i = j$ for every i, j , E' form a perfect matching.

□

Note that converse of this statement is not true. For example, consider the bipartite graph whose A matrix is $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. It can be verified that $\det(A) = 0$ but the bipartite graph associated has a perfect matching.

Hence the next natural question, similar to our primality testing problem, is to ask for some kind of modification so that converse of previous lemma (lemma 3.2) is true. In the example considered, there were two perfect matchings in G having opposite sign due to which the determinant became 0. So the modification should ensure that perfect matchings of opposite signs does not cancel off in the determinant.

One way to achieve this is as follows. Define a matrix T as

$$T(i, j) = \begin{cases} x_{ij} & (i, j) \in E \\ 0 & \text{otherwise} \end{cases}$$

where $(i, j) \in V_1 \times V_2$. This matrix is called as the Tutte matrix. Now, if we consider determinant of this matrix, we can see that the monomials corresponding a $\sigma \in S_n$ can be a product of at most n variables. Hence $\det(T)$ is a polynomial in n^2 variables with degree at most n .

Also in the expansion of determinant, we can observe that each term picks exactly one entry from every row and column meaning each of the entries picked is from a distinct row and column. Hence each of the them is a bijection and hence is a permutation on n elements. Also corresponding to any permutation on n elements, we can get a term. This gives us the following observation.

OBSERVATION 3.3. *Set of monomials in $\det(T)$ is in one-one correspondence with set of all permutations on n .*

We now give polynomial formulation for the problem of checking perfect matching in a bipartite graph.

CLAIM 3.4. *For the matrix T as defined before, $\det(T) \neq 0 \iff G$ has a perfect matching*

Proof. By $\det(T) \equiv 0$, we mean that the polynomial $\det(T)$ has all coefficients as zero. (\Rightarrow) Since $\det(T) \neq 0$, there exists a $\sigma \in S_n$ such that the monomial corresponding is non-zero and by definition of determinant it must be expressed as product of some n set of variables $\prod_i T(i, \sigma(i))$. The variable indices gives a matching and since there are n variables this is a perfect matching.

(\Leftarrow) Suppose G has a perfect matching given by a M . Let τ denote the permutation corresponding to M . We now need to show that $\det(T) \neq 0$. To prove this, it suffices to show that there is a substitution to $\det(T)$ which evaluates to a non-zero value.

Consider the following assignment, $\forall i, j$

$$a_{ij} = \begin{cases} 1 & \text{if } (i, j) \in M \\ 0 & \text{otherwise} \end{cases}$$

From the formula of determinant,

$$\begin{aligned} \det(T) &= \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^n T_{i, \sigma(i)} \\ &= \text{sign}(\tau) \prod_{i=1}^n a_{i, \tau(i)} + \sum_{\sigma \in S_n \setminus \{\tau\}} \text{sign}(\sigma) \prod_{i=1}^n T_{i, \sigma(i)} \end{aligned}$$

Now substituting $x_{ij} = a_{ij}$, we get that the first term evaluates to $\text{sign}(\tau)$ since all the entries are 1. The second term evaluates to 0 since for all $\sigma \neq \tau$, there must be a j such that $\sigma(j) \neq \tau(j)$. Hence it must be that $a_{j, \sigma(j)} = 0$ and hence the product corresponding to σ goes to 0. \square

Hence to check if the bipartite graph G has a perfect matching or not, it suffices to check if the polynomial $\det(T)$ is identically zero or not. Checking if a polynomial is identically zero or not is one of the fundamental question in this area.

Note that this problem becomes easy if the polynomial is given as sum of monomial form. In most of the cases, the polynomial will not be given this way. For example if we consider our problem, we are just given the T matrix and $\det(T)$ is the required polynomial. Trying to expand $\det(T)$ and simplifying will involve dealing with $n!$ monomials which is not feasible.

Hence the computational question again boils down to checking if a polynomial is identically zero or not.

Graphs, Groups and Generators

4.1 Graph Isomorphism

DEFINITION 4.1. (Graph Isomorphism.) Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be graphs. We say $G_1 \cong G_2$ (read as G_1 is *isomorphic to* G_2) if there exists a bijection $\sigma : V_1 \rightarrow V_2$ such that $\forall (u, v) \in V_1 \times V_2$ we have

$$(u, v) \in E_1 \iff (\sigma(u), \sigma(v)) \in E_2$$

In other words, we say a graph G_1 is isomorphic to G_2 if there exists a relabeling of the vertices in G_1 such that the adjacency and non-adjacency relationships in G_2 is preserved.

OBSERVATION 4.2. If $|V_1| \neq |V_2|$ we have that G_1 is not isomorphic to G_2 .

The graph isomorphism problem is stated as follows.

PROBLEM : GRAPH ISOMORPHISM

Input : $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$

Output : Decide if $G_1 \cong G_2$ or not.

A natural question to ask in this setting is that if there is an isomorphism from a graph G to itself.

Let $[n] = \{1, 2, \dots, n\}$. Let S_n denote the set of all permutations from the set $[n]$ to $[n]$.

DEFINITION 4.3. (Graph Automorphism.) Let $G = (V, E)$ be a graph. An automorphism of G is a bijection $\sigma : V \rightarrow V$ such that $\sigma(G) = G$. Let

$$\text{Aut}(G) = \{\sigma \mid \sigma \in S_n \text{ and } \sigma(G) = G\}$$

be the set of all automorphisms of G .

The graph automorphism problem is stated as follows.

PROBLEM : GRAPH AUTOMORPHISM

Input : A graph $G = (V, E)$

Output : Construct $\text{Aut}(G)$.

OBSERVATION 4.4. Let $\tau : [n] \rightarrow [n]$ be the identity permutation. That is, for all $i \in [n]$, $\tau(i) = i$. Then by definition $\tau \in \text{Aut}(G)$ for any graph $G = (V, E)$. This identity permutation τ is in $\text{Aut}(G)$.

Are there other permutations from $[n]$ to $[n]$ that are in the set $\text{Aut}(G)$? How large can the set $\text{Aut}(G)$ be?

Formally, the graph rigidity problem is stated as follows.

PROBLEM : GRAPH RIGIDITY

Input : A graph $G = (V, E)$

Output : Decide if $\text{Aut}(G)$ is trivial or not.

OBSERVATION 4.5. Let G be the complete graph on n vertices. Then $|\text{Aut}(G)| = n!$.

Is the set $\text{Aut}(G)$ just a set or does it have more algebraic structure?

DEFINITION 4.6. (Groups.) A set G together with a binary operation $*$ is said to be a group if the following four conditions are met

- **Closure :** $a, b \in G$, the element $a * b \in G$.
- **Associative :** For any $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.
- **existence of Identity :** For any $a \in G$ there exists a unique element $e \in G$ such that $a * e = e * a = a$.
- **existence of Inverse :** For any $a \in G$ there exists a unique element $b \in G$ (denoted by a^{-1}) such that $a * b = b * a = e$.

EXAMPLE 4.7. • S_n forms a group under composition.

- $(\mathbb{Z}_5, +)$ is a group.

From now on, we will use the letter X to denote a graph and G to denote a group.

REMARK 4.8. Let $(G, *)$ be a group. Let $H \subseteq G$ such that $(H, *)$ also forms a group. We say H is a *subgroup* of G and denote by $H \leq G$.

EXERCISE 4.9. For any graph X , the set $\text{Aut}(X)$ forms a group under the composition operation. That is, $\text{Aut}(G) \leq S_n$.

Let $(G, +)$ be a finite group and $g \in G$ be an element. Let $g^2 = g * g$, $g^3 = g * g * g$. Similarly $g^k = \underbrace{g * g * \dots * g}_{k \text{ times}}$. Now consider the set $H = \{g, g^2, g^3, \dots\}$. Since $(G, *)$ is a finite group there

must exist a k such that $g^k = g$.

LEMMA 4.10. Let $(G, +)$ be a finite group and $g \in G$ be an element. Let $H = \{g, g^2, g^3, \dots\}$ be a set of elements. The unique identity e of G is in H .

Proof. By definition, $g^k = g^{k-1} * g = g$.

As $(G, *)$ is a group, we have the inverse of g^{-1} in G .

Therefore

$$g^{k-1} * g * g^{-1} = g * g^{-1} = e$$

□

DEFINITION 4.11 (Generator). Let $(G, +)$ be a finite group and $g \in G$ be an element. We say an element $g \in G$ is a generator of the set H if $H = \{g, g^2, g^3, \dots\}$ (denoted by $H = \langle g \rangle$).

OBSERVATION 4.12. H is a subgroup of G . That is, $H \leq G$.

EXAMPLE 4.13. • $\langle 1 \rangle = (\mathbb{Z}_5, +)$

DEFINITION 4.14. An group $(G, *)$ that can be generated by a single element is called a *cyclic group*.
example : $(\mathbb{Z}_5, +)$.

Not every group is cyclic. For instance S_3 is not cyclic.

DEFINITION 4.15. (Generatin set.)