

---

---

Lecture Notes on

# Algorithmic Algebra

---

---

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

Draft—August 7, 2015 and forever

# List of Scribes

Lecture 1	<i>K Dinesh</i>	1
Lecture 2	<i>Student</i>	4
Lecture 3	<i>Student</i>	7
Lecture 4	<i>Ramya C</i>	10
Lecture 5	<i>stud</i>	13
Lecture 6	<i>stud</i>	14
Lecture 7	<i>stud</i>	15
Lecture 8	<i>stud</i>	16
Lecture 9	<i>stud</i>	17
Lecture 10	<i>stud</i>	18
Lecture 11	<i>stud</i>	19
Lecture 12	<i>stud</i>	20
Lecture 13	<i>stud</i>	21
Lecture 14	<i>stud</i>	22
Lecture 15	<i>stud</i>	23
Lecture 16	<i>stud</i>	24
Lecture 17	<i>stud</i>	27
Lecture 18	<i>stud</i>	28
Lecture 19	<i>stud</i>	29
Lecture 20	<i>stud</i>	30

# Table of Contents

<b>Lecture 1</b>	<b>Introduction, Motivation and the Language</b>	<b>1</b>
1.1	Overview of the course. Administrative, Academic policies . . . . .	1
1.2	Introduction and Motivation . . . . .	2
1.3	Overview of the course . . . . .	3
<b>Lecture 2</b>	<b>Algebraic Approach to Primality Testing</b>	<b>4</b>
2.1	Application to Number Theory . . . . .	4
<b>Lecture 3</b>	<b>Algebraic Approach to finding Perfect Matchings in Graphs</b>	<b>7</b>
3.1	Application to Graph algorithms . . . . .	7
<b>Lecture 4</b>	<b>Graphs, Groups and Generators</b>	<b>10</b>
4.1	Graph Isomorphism . . . . .	10
<b>Lecture 5</b>	<b>Multivariate Multipolynomial Division and Applications</b>	<b>13</b>
5.1	Another Example Application - Geometric Theorem Proving . . . . .	13
5.2	An Informal View . . . . .	13
5.3	Algebraic Preliminaries . . . . .	13
<b>Lecture 6</b>	<b>From Dickson's Lemma to Hilbert Basis Theorem</b>	<b>14</b>
6.1	From Multivariate Polynomial Division Algorithm to Ideal Membership Problem . .	14
6.2	Proof of Hilbert Basis Theorem . . . . .	14
6.3	Grobner Conditions for Basis . . . . .	14
6.4	Ideal Membership Problem with Grobner basis as Input . . . . .	14
<b>Lecture 7</b>	<b>Buchberger's Algorithm</b>	<b>15</b>
7.1	Constructing Counter-Examples to Grobner condition . . . . .	15
7.2	$S$ -polynomials and Buchberger's Criterion . . . . .	15
7.3	Buchberger's Algorithm - Correctness & Termination . . . . .	15
7.3.1	Ascending Chain Condition for Ideals . . . . .	15
7.4	Proof of Buchberger's criterion. . . . .	15
7.4.1	A structure Lemma for counter examples for Grobner condition . . . . .	15
<b>Lecture 8</b>	<b>Proof of Buchberger's criterion.</b>	<b>16</b>
8.1	A Structure Lemma . . . . .	16
8.2	A Proof by Contradiction . . . . .	16

<b>Lecture 9 Minimality, Elimination Theory</b>	<b>17</b>
9.1 Minimal and Reduced Grobner Basis . . . . .	17
9.2 Uniqueness of Reduced Grobner basis . . . . .	17
9.3 Elimination Theory and Elimination Ideals . . . . .	17
9.4 Grobner Basis for the Elimination Ideals . . . . .	17
<b>Lecture 10 An application of Monomial ordering</b>	<b>18</b>
10.1 Applications of Grobner Basis . . . . .	18
10.1.1 3-coloring via Grobner Basis . . . . .	18
10.2 Integer Programming . . . . .	18
10.2.1 Formulation as polynomials . . . . .	18
10.2.2 $\mathbb{F}$ -algebra homomorphism . . . . .	18
10.2.3 Kernel . . . . .	18
10.2.4 Testing membership in the image . . . . .	18
10.2.5 Bringing in optimisation . . . . .	18
<b>Lecture 11 Integer Programming using Grobner Basis</b>	<b>19</b>
11.1 Characterizing the Image . . . . .	19
11.2 Observations on the Grobner Basis . . . . .	19
11.3 Bringing in Optimality . . . . .	19
11.4 Remarks about generalizations . . . . .	19
<b>Lecture 12 From Root Finding to Factorization</b>	<b>20</b>
12.1 Number of Roots . . . . .	20
12.2 A Linear Algebraic Method - The companion Matrix . . . . .	20
12.3 From Roots to Factorization . . . . .	20
12.4 Informal Answers and the road ahead . . . . .	20
<b>Lecture 13 Unique Factorization Domains</b>	<b>21</b>
13.1 Irreducible vs Prime Elements of an Integral Domain . . . . .	21
13.2 A characterization of Unique Factorizability . . . . .	21
13.3 A Non-trivial Application - All Principal Ideal Domains are Unique Factorization Domains . . . . .	21
13.4 Gauss's Theorem . . . . .	21
13.4.1 All constant primes in $R$ are primes in $R[x]$ . . . . .	21
13.4.2 All non-constant irreducibles in $\mathbb{Z}[x]$ are irreducibles in $\mathbb{Q}[x]$ . . . . .	21
<b>Lecture 14 Irreducibility</b>	<b>22</b>
14.1 Completing Gauss's Theorem . . . . .	22
14.2 A Remark about Field of Fractions . . . . .	22
14.3 Eisenstein criterion for irreducibility . . . . .	22
<b>Lecture 15 Quotient Rings and First Isomorphism Theorem</b>	<b>23</b>
15.1 Quotient Rings and Irreducibility . . . . .	23
15.2 Quotient Rings and First Isomorphism Theorem . . . . .	23
15.3 Application 1 : Chinese Remaindering Theorem . . . . .	23

15.4 Application 2 : From Irreducibility to Field Extensions . . . . .	23
<b>Lecture 16 More on Fields</b>	<b>24</b>
16.1 Field Extensions as Vector Spaces . . . . .	24
16.1.1 Linear Independence, Basis, and Dimension . . . . .	24
16.1.2 Minimal Polynomials - viewing adjoining as a vector space . . . . .	25
16.2 Characteristic of Rings & Fields . . . . .	25
16.3 Sizes of Finite Fields . . . . .	25
16.4 Constructing Field Extensions . . . . .	26
16.5 Uniqueness of Fields up to isomorphism . . . . .	26
<b>Lecture 17 Warming up to Berlekamp's Factorization Algorithm</b>	<b>27</b>
<b>Lecture 18 Berlekamp's Lemma</b>	<b>28</b>
<b>Lecture 19 Berlekamp's Factorization Algorithm</b>	<b>29</b>
<b>Lecture 20 Berlekamp's Factorization Algorithm</b>	<b>30</b>
20.1 The Berlekamp Subalgebra $\mathbb{W}$ . . . . .	30
20.2 From Number of Irreducible Factors to Dimension . . . . .	30
20.3 Using $\mathbb{W}$ for factorization . . . . .	30
20.4 Constructing a basis for $\mathbb{W}$ - a linear algebraic approach . . . . .	30

# 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 at 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 M.N.

*Scribe:* K Dinesh

*Date:* July 31, 2013

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 :

**Plagarism 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.

Note that both these problems can be modelled using a graph. For example, in the second case one could view the molecule being given as adjacency matrix. Our aim in both cases are similar which 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 follows :  $\sigma_1 \circ \sigma_2 = (\sigma_1(\sigma_2(1)), \sigma_1(\sigma_2(2)), \dots, \sigma_1(\sigma_2(n)))$ . This is same as applying  $\sigma_2$  on identity permutation and then applying  $\sigma_1$  to the result. We show that  $Aut(X)$  along with the composition operation  $\circ$  gives us many nice properties.



- If  $\sigma_1, \sigma_2 \in \text{Aut}(X)$ , 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  $\sigma_1$  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  $\text{Aut}(X)$  is *closed* under  $\circ$ .
- The composition operation is also *associative*.
- *Identity* permutation belongs to  $\text{Aut}(X)$  as observed before.
- Since we are considering bijections, it is natural to consider *inverse* for a permutation  $\sigma$  denoted  $\sigma^{-1}$  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  $\sigma \in \text{Aut}(X)$ , is it true that  $\sigma^{-1}$  also belongs to  $\text{Aut}(X)$ . It turns out that it is true.

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

*Proof.* Recall that  $\sigma \in \text{Aut}(G)$  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  $\sigma^{-1}$  we get that  $(\sigma^{-1}(u), \sigma^{-1}(v)) \in E \iff (u, v) \in E$ . This shows that  $\sigma^{-1} \in \text{Aut}(X)$  □

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.

An algorithm for this problem has been found in 2002 by Manindra Agarwal, Neeraj Kayal and Nitin Saxena (which is now called as 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  $N$  be composite. Hence there exists a prime  $p$  such that  $p \mid N$ . Let  $p^a \nmid N$  where  $a \geq 1$  is the largest exponent of  $p$  in the prime factorisation of  $N$ . Hence  $p^{a+1} \nmid N$ .

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 in this case, we show that the coefficient of  $z^i$  for  $i = p$ , which is  $\binom{N}{p}$ , is non zero modulo  $p^a$  showing<sup>1</sup>  $p_N(z)$  is not a zero polynomial. 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  $\binom{N}{p} \not\equiv 0 \pmod{p^k}$ .  $\square$

---

<sup>1</sup>Note that if  $N \mid \binom{N}{i}$  then  $p^a \mid \binom{N}{i}$ . Taking contrapositive, we get that  $\binom{N}{i} \not\equiv 0 \pmod{p^a}$  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

Preamble

### 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  $|\{(i, j) \mid i < j \text{ and } \sigma(i) > \sigma(j), 1 \leq i < j \leq n\}|^2$ .

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.

□

---

<sup>2</sup>Every permutation can be decomposed to disjoint cycles. It can also be shown that  $\text{sign}(\sigma) = (-1)^{(n - \# \text{ of odd cycles})}$

Note that converse of this statement is not true. For example, consider the bipartite graph

whose  $A$  matrix is  $A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$ . It can be verified that  $\det(A) = 0$  but the bipartite graph associated has a perfect matching.

Hence the next natural question to ask is what kind of modification to the 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  $(i, j) \in V_1 \times V_2$ . 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  $n$  variables at most. Hence  $\det(T)$  is a polynomial in  $n^2$  variables with degree at most  $n$ . We now give polynomial formulation for the problem of checking perfect matching in a bipartite graph.

**CLAIM 3.3.** *For the matrix  $T$  as defined before,  $\det(T) \neq 0 \iff G$  has a perfect matching*

*Proof.* ( $\Rightarrow$ ) 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  $\sigma$  and it appears in  $\det(T)$  as  $m$ . Only way the term associated with this perfect matching can vanishes from  $\det(T)$  is via another perfect matching which appear as  $-m$  in  $\det(T)$

But note that for any two different perfect matchings in  $G$  if we look at the permutations associated, they must differ in at least one edge. Hence the associated terms must differ in some variable. Hence there does not exists another matching which can vanish  $m$  from  $\det(T)$  showing  $\det(T) \neq 0$ .  $\square$

Hence to check if the bipartite graph  $G$  has a perfect matching or not, it suffices to check if the polynomial  $\det(A)$  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.

So far we have spoken about finding perfect matching in bipartite graphs. A similar result holds for general graphs also.

THEOREM 3.4. *Given a graph  $G(V, E)$  and for  $i, j \in V$ ,  $i \neq j$ , define an  $n \times n$  matrix  $T$  as*

$$T_{i,j} = \begin{cases} x_{ij} & (i, j) \in E, i < j \\ -x_{ji} & (i, j) \in E, i > j \\ 0 & \text{otherwise} \end{cases}$$

*Then,  $\det(T) \neq 0 \iff G$  has a perfect matching.*

## 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 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  $\tau$  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*.  
exercise example :  $(\mathbb{Z}_5, +)$ .

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

DEFINITION 4.15. (Generatin set.)

CS6842 – Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Aug 13, 2013

LECTURE

5

## Multivariate Multipolynomial Division and Applications

Preamble

**5.1 Another Example Application - Geometric Theorem Proving**

**5.2 An Informal View**

**5.3 Algebraic Preliminaries**

## From Dickson's Lemma to Hilbert Basis Theorem

Preamble

- 6.1 From Multivariate Polynomial Division Algorithm to Ideal Membership Problem
- 6.2 Proof of Hilbert Basis Theorem
- 6.3 Grobner Conditions for Basis
- 6.4 Ideal Membership Problem with Grobner basis as Input

## Buchberger's Algorithm

Preamble

**7.1 Constructing Counter-Examples to Grobner condition**

**7.2  $S$ -polynomials and Buchberger's Criterion**

**7.3 Buchberger's Algorithm - Correctness & Termination**

**7.3.1 Ascending Chain Condition for Ideals**

**7.4 Proof of Buchberger's criterion.**

**7.4.1 A structure Lemma for counter examples for Grobner condition**

CS6842 – Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Feb 6, 2013

LECTURE

8

## Proof of Buchberger's criterion.

Preamble

**8.1 A Structure Lemma**

**8.2 A Proof by Contradiction**

## Minimality, Elimination Theory

### Preamble

Minimal and Reduced Grobner Basis. Ideal Equality Problem. Uniqueness of Reduced Grobner basis. Elimination Theory and Elimination Ideals. Grobner Basis for the Elimination Ideals. Relating to the Robotics Arms problem.

### 9.1 Minimal and Reduced Grobner Basis

### 9.2 Uniqueness of Reduced Grobner basis

### 9.3 Elimination Theory and Elimination Ideals

### 9.4 Grobner Basis for the Elimination Ideals

## An application of Monomial ordering

### Preamble

Applications of Grobner Basis. 3-coloring via Grobner basis. Testing membership in Kernel and Image of Ring Homomorphisms. Applications to Integer Programming.

### 10.1 Applications of Grobner Basis

#### 10.1.1 3-coloring via Grobner Basis

### 10.2 Integer Programming

#### 10.2.1 Formulation as polynomials

#### 10.2.2 $\mathbb{F}$ -algebra homomorphism

#### 10.2.3 Kernel

#### 10.2.4 Testing membership in the image

#### 10.2.5 Bringing in optimisation



## Integer Programming using Grobner Basis

Proof of the characterization of the Image of the  $k$ -algebra homomorphism. Observation about the Grobner basis in the special case of integer programming. Defining the monomial ordering to bring in optimization. Proof of optimality of the solution.

### 11.1 Characterizing the Image

### 11.2 Observations on the Grobner Basis

### 11.3 Bringing in Optimality

### 11.4 Remarks about generalizations

## From Root Finding to Factorization

*Shorter Lecture:* From Root finding to factorization of polynomials. Why or when is a polynomial completely factorizable over the underlying ring/field? Why should they be unique factorizable? Informal answers, and directions to explore.

### 12.1 Number of Roots

### 12.2 A Linear Algebraic Method - The companion Matrix

### 12.3 From Roots to Factorization

### 12.4 Informal Answers and the road ahead

## Unique Factorization Domains

Irreducible and Prime Elements in an Integral Domain. Primes are irreducible. When is it that all irreducibles are primes? A proof that this is exactly when the domain is a UFD. A field is a UFD. Every principal Ideal Domain (example:  $F[x]$  and  $\mathbb{Z}$ ) is a UFD. What about rings like  $F[x_1, x_2]$ , and  $\mathbb{Z}[x]$ ? Gauss's theorem : If  $R$  is a UFD, then so is  $R[x]$ . Proof of the theorem using the characterization about irreducibles in  $R[x]$ . The case when the irreducibles are from  $R$  itself (Gauss's Lemma).

### 13.1 Irreducible vs Prime Elements of an Integral Domain

### 13.2 A characterization of Unique Factorizability

### 13.3 A Non-trivial Application - All Principal Ideal Domains are Unique Factorization Domains

### 13.4 Gauss's Theorem

#### 13.4.1 All constant primes in $R$ are primes in $R[x]$

#### 13.4.2 All non-constant irreducibles in $\mathbb{Z}[x]$ are irreducibles in $\mathbb{Q}[x]$

All primes in  $\mathbb{Q}[x]$  are primes in  $\mathbb{Z}[x]$

## Irreducibility

Continuing the proof of Gauss's theorem : The case when the irreducibles are from the  $\mathbb{R}[x]$ . Moving the argument to the Field of Fractions. Conclusion : Two tasks are well-framed.

- How do we detect irreducibility?
- How do we factorize into irreducible factors?

Eisenstein criterion for irreducibility.

### 14.1 Completing Gauss's Theorem

### 14.2 A Remark about Field of Fractions

### 14.3 Eisenstein criterion for irreducibility

## **Quotient Rings and First Isomorphism Theorem**

Quotient Rings. Irreducibility and Quotient Rings. First Isomorphism Theorem for the Quotient Ring. Application 1 : Chinese remaindering theorem. Application 2 : From Quotient Rings of Irreducible polynomials to Field extensions.

### **15.1 Quotient Rings and Irreducibility**

### **15.2 Quotient Rings and First Isomorphism Theorem**

### **15.3 Application 1 : Chinese Remaindering Theorem**

### **15.4 Application 2 : From Irreducibility to Field Extensions**

## More on Fields

Quick introduction to vector spaces. Viewing field extensions as vector spaces. Characteristic of a field. Sizes of fields. Constructing extensions and uniqueness of fields of a given size (up to isomorphism).

### 16.1 Field Extensions as Vector Spaces

A vector space over a field  $\mathbb{F}$  is a set  $V$  with two kinds of operations - addition and scalar multiplications - satisfying the following properties. Elements of  $V$  are called vectors and elements of  $\mathbb{F}$  are called scalars.

- $(V, +)$  forms an abelian group.
- If  $\alpha$  is a scalar, and  $v$  is a vector, then  $\alpha v$  is a vector.
- If  $\alpha$  is a scalar, and  $u$  and  $v$  are vectors, then  $\alpha(u + v)$  is the same vector as  $\alpha u + \alpha v$ .
- If  $\alpha_1, \alpha_2$  are scalars, and  $v$  is a vector, then  $\alpha_1(\alpha_2 v)$  is the same vector as  $(\alpha_1 \alpha_2)v$  where  $\alpha_1 \alpha_2$  is the multiplication in  $\mathbb{F}$ .

Some easy examples are the set of points in  $\mathbb{R} \times \mathbb{R}$ . Set of polynomials of degree  $d$  over a field  $\mathbb{F}$  forms a vector space with the natural notion of addition and multiplication.

Let  $E$  be a field and  $F$  be a subfield of it. One can view  $E$  as a vector space over  $F$ . To see this, view the elements of  $F$  as scalars and the elements of  $E$  as vectors in the above definition.

#### 16.1.1 Linear Independence, Basis, and Dimension

DEFINITION 16.1. A set of vectors  $v_1, v_2, \dots, v_k$  are said to be *linearly independent*, if:

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_k v_k = 0 \implies \alpha_1 = 0 \wedge \alpha_2 = 0 \wedge \dots \wedge \alpha_k = 0$$

For any set  $S$  of vectors, the set of vectors spanned by it, denoted by  $\text{SPAN}(S)$  is the set of vectors that can be expressed as the linear combination of vectors in  $S$ . A set  $S$  is said to be a basis of a vector space, if  $S$  itself is linearly independent and the  $\text{SPAN}(S)$  is the whole space.

We need two observations about the basis of a vector spaces and basis.

All basis of a vector space are of the same size. Suppose there is an  $S$  and an  $S'$  which forms the basis of the same vector space  $V$ , and  $|S| > |S'|$ . Since  $S$  and  $S'$  are subsets of  $V$  itself, the elements of  $S'$  **Jayalal says: This needs to be completed.**

Since all basis of a vector space are of the same size - it must be the case that.

### 16.1.2 Minimal Polynomials - viewing adjoining as a vector space

## 16.2 Characteristic of Rings & Fields

Consider the following Ring homomorphism from  $\mathbb{Z}$  to a ring  $R$ .

$$\phi : \mathbb{Z} \rightarrow R$$

where,  $\forall a \in \mathbb{Z}$ ,  $\phi(a) = |a|.1$  if  $a > 0$ , and  $\phi(a) = |a|.(-1)$  if  $a < 0$ . where  $n.1$  is simply a notation for adding the identity of the ring  $R$ ,  $n$  times to itself.

We will first check that it is a ring homomorphism. **Jayalal says: Yet to be written**

Let  $I$  be the kernel of this map. Since  $\mathbb{Z}$  is a principal ideal domain,  $I$  is singly generated and the generator is simply the least number in absolute value. Let  $\ell$  be the generator of the ideal. We know that the ideal  $I$  is simply  $\ell\mathbb{Z}$ . This  $\ell$  is called the characteristic of the ring  $R$ . In other words, *characteristic of a ring  $R$  with identity is simply the smallest number of times one needs to add 1 to get to 0*. Indeed, it is possible that adding the identity to itself never gets to 0 of the ring. In this case  $I = 0$  and  $\ell = 0$  - we say that the characteristic of the ring is 0.

We explore more properties that can be derived from this  $\ell$ . Let  $R'$  be the image of this homomorphism. We know that  $R'$  is a subring of  $R$ . Consider the quotient ring  $\mathbb{Z}/\ell\mathbb{Z}$  which is same as  $\mathbb{Z}_\ell$ . By the first isomorphism theorem we have the following:  $\mathbb{Z}_\ell \cong R'$ . In other words, if the characteristic of a ring  $R$  is  $\ell$ , then there is an isomorphic copy of  $\mathbb{Z}_\ell$  sitting inside  $R$  as a subring.

Now we turn to characteristic of a field. First of all let us argue that it can only be zero or a prime number.

**LEMMA 16.2.** *The characteristic of a field is either a prime number or zero.*

*Proof.* Let  $F$  be a field. Suppose the characteristic is not a prime and is  $\ell \in \mathbb{Z}$ . Assume for the contradiction that  $\ell$  is not prime.  $\ell = p.q$  where  $p, q < n$ . Indeed,  $\ell$  is least integer such that  $\ell.n = 0$ . Hence  $p.1 \neq 0$  and  $q.1 \neq 0$ . Since  $\phi$  is a homomorphism, associated with the  $\ell$  that we discussed above,  $\phi(pq) = \phi(p)\phi(q)$ . Since the LHS is 0,  $\phi(p)$  and  $\phi(q)$  forms zero divisors in  $\mathbb{F}$ . Thus, we have arrived at a contradiction and hence the lemma.  $\square$

**COROLLARY 16.3.** *Any finite field must have a subfield whose order is a prime number.*

*Proof.* Let  $F$  be a finite field. We first argue that the characteristic cannot be zero. If it is zero, then we know that the ideal  $I$  in the above discussion is the zero ideal and hence the quotient ring is  $\mathbb{Z}$  itself. Hence,  $\exists R' \subseteq F$  such that  $\mathbb{Z} \cong R'$ , which implies that  $\mathbb{F}$  must have infinite cardinality. Thus, characteristic can only be a prime number. Thus, an isomorphic copy of  $\mathbb{Z}_p$  for some prime  $p$  must be present in every field.  $\square$

## 16.3 Sizes of Finite Fields

We combine the ideas developed in the previous two sections to conclude that the sizes of finite fields cannot be arbitrary.

**LEMMA 16.4.** *The size of any finite field is always of the form  $p^d$  for some prime  $p$  and a non-negative integer  $d$ .*

*Proof.*  $\mathbb{Z}_p$  (for some prime  $p$ ) appears a subfield (up to isomorphism) of any finite field. Let  $d$  be the dimension of  $F$  as a vector space over  $\mathbb{Z}_p$ . That is, there is a subset  $S \subseteq F$  with  $|S| = d$ , which forms the basis of  $F$  over  $\mathbb{Z}_p$ . Let us say that  $S = \{a_1, a_2, \dots, a_d\}$ . Indeed, each vector (each element of  $a \in \mathbb{F}$ ) can be viewed as a  $d$ -tuple  $(\alpha_1, \alpha_2, \dots, \alpha_d)$  such that  $a = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_d a_d$ . Can two tuples represent the same  $a$ ? No, because it would mean then that  $\sum_i \alpha_i a_i = \sum_i \alpha' a_i$ . This contradicts the fact that  $S$  is linearly independent (since it forms a basis of  $\mathbb{F}$ ). Hence there are precisely  $p^d$  tuples possible, each of them representing distinct elements of  $\mathbb{F}$  as a vector space over  $\mathbb{Z}_p$ . Hence the size of the field  $\mathbb{F}$  must be exactly  $p^d$ .  $\square$

## 16.4 Constructing Field Extensions

For any  $p$  and  $d$ , is there a field of size  $p^d$ . We will answer this question positively.

Consider a polynomial  $p(x)$  of degree  $d$  that is irreducible over  $\mathbb{Z}_p$ . Let  $a$  be a root of such a polynomial. Clearly  $a \notin \mathbb{Z}_p$ . Consider the field  $\mathbb{Z}_p/\langle p \rangle$ . This is isomorphic to  $\mathbb{Z}_p(a)$  which also is a vector space over  $\mathbb{Z}_p$ .

We argue that the size of this finite field is precisely  $p^d$ . First of all, we argue that any element of the space  $\mathbb{Z}_p(a)$  can be viewed as a linear combination of elements in  $\{1, a, a^2, \dots, a^{d-1}\}$ . We do not need an  $a^d$  in this expression - indeed, it can be written as a combination of the other elements of lesser power since  $p(a) = 0$ . Suppose there is a linear combination of  $(1, a, a^2, \dots, a^{d-1})$  that goes to zero, that is  $a$  is a root of the polynomial of lesser degree than  $p(a)$ . But then there is a polynomial of degree less than  $p(x)$  which has  $a$  as the root.

## 16.5 Uniqueness of Fields up to isomorphism

We will be greedy, for any  $p$  and  $d$ , are there two non-isomorphic fields of size  $p^d$ ? We will answer this question negatively. So, we can always talk about *the* field of size  $p^d$ . **Jayalal says: Define splitting field etc.**

LEMMA 16.5. *The splitting field of a polynomial are always isomorphic to each other.*

*Proof.* **Jayalal says: Yet to be written**  $\square$

LEMMA 16.6. *For any field  $\mathbb{F}$ , there is a polynomial whose splitting field is  $\mathbb{F}$ .*

*Proof.* Let  $|\mathbb{F}| = k$ . Consider the multiplicative group  $\mathbb{F} - \{0\}$ . Let  $g$  be an element in this group. We know by Lagrange's theorem,  $g^{k-1} = 1$  where 1 is the multiplicative identity. Thus for all  $g \in \mathbb{F}$ ,  $g^k = g$ . Thus all of them are roots of the polynomial  $x^k - x$ , as a polynomial in  $\mathbb{F}[x]$ . Since this polynomial can have at most  $k$  roots, the polynomial completely splits in  $\mathbb{F}$  and it does not split in any subfield of  $\mathbb{F}$ . Hence  $\mathbb{F}$  is the splitting field of the polynomial  $x^k - x$ .  $\square$

By combining the above two lemmas, we get the main point of this section. That finite fields of a fixed size must be isomorphic.



CS6842 – Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Sep 18, 2013

# LECTURE 17

## Warming up to Berlekamp's Factorization Algorithm

Back to Factorization problem. A starting idea to use Fermat's little theorem to extract product of linear factors. Reduction to Squarefree case. Frobenius map ( $x^q = x$ ) and the sub-algebra of the quotient ring  $F[x]/f$ . Dimension of the sub-algebra when  $f$  is irreducible.

CS6842 – Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Sep 10, 2013

# LECTURE 18

## Berlekamp's Lemma

Chinese remaindering. Berlekamp algebra  $W$  and its dimension. From an element in  $W$  to factorization - Berlekamp's Lemma.

CS6842 – Algorithmic Algebra

*Instructor:* Jayalal Sarma M.N.

*Scribe:* stud

*Date:* Sep 25, 2013

# LECTURE 19

## Berlekamp's Factorization Algorithm

Writing a set of linear equations and the Berlekamp Matrix. The  $O((qn^3)(n^2)(qn^2))$  time algorithm. Reducing the first factor of  $q$  by faster exponentiation. Removing the second factor of  $q$ . Identifying the minimal polynomial for the  $g(x)$ .

## Berlekamp's Factorization Algorithm

Computing the minimal polynomial of  $g(x)$ . Factorizing the minimal polynomial by Rabin's factorization method. Discussions on effect of choosing  $g(x)$  in  $\mathbb{W}$ , at random.

Berlekamp's Algorithm.

**20.1 The Berlekamp Subalgebra  $\mathbb{W}$**

**20.2 From Number of Irreducible Factors to Dimension**

**20.3 Using  $\mathbb{W}$  for factorization**

**20.4 Constructing a basis for  $\mathbb{W}$  - a linear algebraic approach**