6.966 Algebra and Computation	September 9, 1998

Lecture 1

Lecturer: Madhu Sudan — *Scribe: John Dunagan*

1 Course Overview

In this course we will investigate the relationship between algebra and computation. Towards this end, we will survey computational results in algebra and some notions and results from algebraic models of computation. A historical goal of algebra has been to find explicit computational solutions to algebraic problems (i.e., Euclid's algorithm). Algebra has also had a very strong influence on our thinking about algorithms.

Some of the sub-areas we will focus on are: Algorithms from algebra; algebraic models of computation; and algebraic tools for dealing with complexity. We won't cover all the interesting algebraic problems and algorithms, but we'll hit a lot of the high points. Let us start by comparing algebraic problems and algorithms against the more general class of combinatorial problems and algorithms.

2 Two Flavors of Algorithms

Combinatorial problems typically assume an unstructured input. This typically leads to intractability relatively quickly. Algebra assumes a much greater amount of structure. To study this contrast more formally, let us look at a basic framework which captures many combinatorial and algebraic problems — namely "constraint satisfaction." In this framework, we typically describe a space of solutions, impose a collection of constraints, and then ask for a solution satisfying all the constraints. Combinatorial problems such as sorting, max flow, linear programming, and 3SAT can all be expressed in this way. E.g.:

Sorting: Given $X = \{x_1, x_2, ...x_n\}$ find $\pi : \{1, \ldots, n\} \rightarrow \{1, \ldots, n\}$ such that for every pair of indices $i, j \in \{1, \ldots, n\}$ with $i < j$, $\pi(i) \neq \pi(j)$ and $x_{\pi(i)} < x_{\pi(j)}$.

3SAT: Given $X = \{x_1, x_2, ...x_n\}$, and a series of functions of three variables, $x_i \vee x_j \vee x_k$, does there exist an assignment of the $\{x_i\}$ such that all the functions evaluate to true?

Similarly central algebraic problems are also "constraint satisfaction problems". Consider, for example, the classical problem of solving linear systems.

System of linear equations: Find x, y such that $ax + by = c$ and $dx + ey = f$.

Another common problem is that of finding integer solutions to the above linear system, which gives an example of a Diophantine problem. And, if the equalities in the linear system are replaced by inequalities, we obtain the problem of linear programming. All these provide examples of cosntraint satisfaction problems.

A constraint satisfaction problem of a somewhat different flavor is that of finding roots of polynomials.

Roots of quadratic polynomials: Find x such that $ax^2 + bx + c = 0$.

This problem of solving a polynomial equation can be generalized in many ways. We can look at systems of many polynomials, polynomials of higher degree, polynomials of many variables, and replacing the equalities by inequalities. A familiar system of polynomials in many variables is given below.

System of polynomial equations Given the variables $x_1, x_2, ...x_n$, the equations $x_i(1 - x_i) = 0$ for every i, and the additional equations, $x_1x_2(1 - x_3) = 0$, $x_3(1 - x_2)x_5 = 0$, ..., is there a solution?

Remark: Notice that this captures 3SAT!

These problems lead to two of the most fundamental problems in algebra: polynomial factorization and quantifier elimination. These two shall be the focus of much of this course. Since at times, the problems will look repetitive (and more so the solutions), there will occasionally be a hint of applications.

The bigger goal here is to learn about the algebraic theory of the words that end with **-ant**. These include the **determinant, permanent, discriminant, resultant, continuant, alternant,** etc. In general they are covered by the unifying word: **invariant**. Algebra is most fortunate in that not only can it solve systems when they can be solved, it can also provide simple algebraic expressions that tell you whether or not a solution exists. Classical examples of this are the **determinant** and the **discriminant**. Understanding this underlying algebra should enhance your understanding of why things work.

3 Complexity

A lot of recent work in complexity theory has relied on an algebraic setting for the problems of complexity theory. An example problem that is often used is:

System of degree 2 polynomials Given m polynomials of degree 2 in n variables, do they have a common zero.

Exercise: Prove above is NP-hard.

Since we often move well-known combinatorial problems to an algebraic setting, it seems worthwhile to study these problems directly in an algebraic setting. This leads to the issue of whether there is a direct way to study algebraic problems in an algebraic model of computation.

A number of algebraic models have been proposed in the past to study computation; notable examples are due to Valiant, and more recently, to Blum, Shub and Smale. These models lead to natural generalizations of the P vs. NP question. They have natural complete problems, and (under some restrictions) a separation of P from NP in these models yields some useful information about the P=NP question.

Unfortunately, we must conclude with the same observation so often made in other complexity courses; we know how to prove precious little. However, some weak separations are possible in some weak models of computation, and we will give a brief survey of some of the methods used to lower bound the algebraic complexity of computations in some of these models.

4 References

There are a number of books that are closely related to the topic of this course. The ones we will follow closely are:

1. Polynomial Factorization:
   Cohen: Computational Algebraic Number Theory.

2. Elimination:
   Cox, Little, O'Shea: Ideals, Varieties and Algorithms.

3. Algebraic Models of Computation:
   Blum, Cucker, Shub and Smale: Complexity and Real Computation.

4. Non-uniform methods:
   Burgisser, Clausen, Shokrollahi: Algebraic Complexity Theory.

5 Administrivia

There will be some obligation to scribe notes for this course and to both read and write papers based on it. The lecturer hopes that anyone[1] who meets any of the following criteria will both enjoy and benefit from this course.

1. interested in complexity theory
2. interested in number theory
3. interested in coding theory
4. very interested in algebraic methods

6 A Review of Some Algebra

Let's review some useful things from algebra. Fields are objects which possess both the operators $+$ and $*$, both of which are associative, commutative, and both of which possess both identities and inverses, except that 0 does not have a multiplicative inverse. Also, $*$ distributes over $+$.

Some common examples of fields are the rational numbers $\mathbb{Q}$, the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$, the integers modulo p for any prime p ($\mathbb{Z}_p$ - we will shortly show this is a field), and rational functions[2] over a field $\mathbb{F}$.

Commutative rings are like fields, except that we drop the restriction that multiplicative inverses must exist. Examples of commutative rings are the integers ($\mathbb{Z}$), and polynomials over a ring ($R[x]$ where R is a ring).

Groups only possess the operation plus. Groups are not necessarily commutative. For our purposes, the only interesting result for finite groups relates to the order of an element. The **order** of an element a is the least positive integer i (if one exists) such that the sum of i copies of a is the identity element.

Theorem 1 *For every finite group, the order of any element of the group divides the order of the group.*

One immediate consequence of this theorem is that $a^p = a$ (mod p) where p is a prime, which is also referred to as Fermat's Little Theorem.[3]

Between commutative rings and fields, it is possible to come up with a number of interesting axioms, all of which try to capture some property of the integers. To start, let us consider the question of factorization.

Define an integral domain to be a ring R such that no two non-zero elements yield zero when multiplied. Formally:

A ring R is an **integral domain** iff $\forall a, b \in R : ab = 0 \Rightarrow a = 0 \vee b = 0$.

A unit in an integral domain is any element with an inverse. Formally

$u \in R$ is a **unit** iff $\exists v : uv = 1$.

It is useful to create equivalence classes in integral domains using multiplication by units. Two elements belonging to the same equivalence class under multiplication by a unit are said to be associates. Formally,

a and b are **associates** iff $\exists u$ such that u is a unit and $au = b$.

It may be verified "association" yields an equivalence relation. Relating this to our reference ring, the integers, this means that a and $-a$ are associates for every a.

With this in hand, we can now express the notion of irreducibility.

[1] Unless you are the type of person who wants to argue over whether zero is an ideal. In this case, you should have a long talk with Madhu.

[2] Rational functions are formally described as a ratio of two formal polynomials over with coefficients from the field.

[3] We prove this using that $\mathbb{Z}_p$ is a field. This property does not hold in general for arbitrary p. Consider $p = 4, a = 2$.

An element $a \in R$ is **irreducible** iff $\forall b, c \in R, bc = a$ implies b is a unit or c is a unit.

This definition does correspond to our notion of an irreducible. Since in the integers, irreducibles are primes and vice versa, let us examine a prime, such as two. $2 = 2 * 1 = -2 * -1$ are both true. In both cases, one of the factors is a unit.

We are now ready to define unique factorization domains:

An integral domain R is a **unique factorization domain** (UFD) iff every element is expressible uniquely as a product of finitely many irreducibles (up to associates).

It is worthwhile to pause to note that in an arbitrary integral domain, not every element has a unique factorization. A common example is the ring $\mathbb{Z}[x, y]/(x^2 - y^3)$ (i.e., polynomials with integer coefficients in x and y with the relation $x^2 = y^3$). In this case, we can factor x^2 as $x * x$ or (since $x^2 = y^3$) as $y * y * y$. (Of course, to verify the example one should also check that x and y are irreducible in this domain.) Similarly, there are integral domains where some elements are reducible but are not units and are not expressible as the product of finitely many irreducible elements. We conclude that our definition is "tight." We will mostly work with unique factorization domains, and this is good for us, because irreducibles and primes are synonymous in a unique factorization domain. This is a good time to pause to introduce primes formally.

An element $p \in R$ is **prime** iff $\forall b, c \in R, p$ divides bc implies p divides b or p divides c.

Both integers and polynomials over an integral domain satisfy the above properties, and so are unique factorization domains. In general, integral domains have nearly all the nice properties of fields. We extract these properties in the next two lemmas.

Lemma 2 *Every finite integral domain R is a field.*

Proof We need to show that every non-zero element $a \in R$ has a multiplicative inverse. Consider the sequence $1, a, a^2, a^3, \ldots, a^n, \ldots$ Since R is finite, the sequence will eventually repeat elements. I.e., $\exists i < j$ s.t. $a^i = a^j$. Thus $a^j - a^i = 0 \Leftrightarrow a^i \cdot (a^{j-i} - 1) = 0$. Since $a \neq 0$, we have $a^i \neq 0$ (using R is integral) and hence $a^{j-i} - 1 = 0$ (again using R is integral). Thus we have that a^{j-i-1} satisfies the properties required of a^{-1}. ■

If an integral domain R is not finite, then to get a field from R we work with the field of fractions over R. Formally

For an integral domain R, the **field of fractions**, denoted $\tilde{R}$, has as elements, pairs from $R \times (R - \{0\})$, under the equivalence $(a, b) \sim (c, d)$ if there exist $\lambda_1, \lambda_2 \in R - \{0\}$ such that $\lambda_1 a = \lambda_2 c$ and $\lambda_1 b = \lambda_2 d$. Addition and multiplication over $\tilde{R}$ are defined as: $(a, b) + (c, d) = (ad + bc, bd)$ and $(a, b) \cdot (c, d) = (ac, bd)$.

Proposition 3 *The field of fractions $\tilde{R}$ forms a field.*

The canonical application of this proposition is the creation of field of the rationals, $\mathbb{Q}$, from the domain of the integers, $\mathbb{Z}$. Finally we define the notion of an ideal that are additively closed subsets of rings that are closed under multiplication with any element of the ring. Formally:

$I \subseteq R$ is an **ideal** if $a, b \in I \Rightarrow a + b \in I$ and $a \in I, c \in R \Rightarrow ac \in I$.

An example of an ideal are multiples of m over integers (written (m)). Ideals will play a significant role in algorithms for quantifier elimination.