Geometric Complexity and Applications CIS 6930 August 26 - September 4, 2008

Lecture 1 through 4

Lecturer: Dr. Meera Sitharam Scribe: Venkatakrishnan Ramaswamy

1 Introduction

Geometric Complexity is a term that is used in a wide variety of contexts to mean different things. We will use this term to broadly refer to the study of computational complexity using different geometric techniques.

Geometry, historically was a study of measurement. *Analytic Geometry* is the study of geometry using the principles of algebra. We have studied Analytic Geometry in middle/high school and it enables us to answer questions such as, where does the tangent to a curve at some point intersect a certain other line.

Algebraic Geometry is the more modern avatar, in which we study zeros of polynomials defined over rings.

Example 1 *Consider the polynomials* $x^2 + y^2 + z^2 - r^2$ *and* $ax + by + cz + d$. *The ideal generated by these polynomials is the set of points on which both these polynomials go to zero. In this case, geometrically, it is the points of intersection of the sphere* $x^2 + y^2 + z^2 - r^2 = 0$ *with the plane* $ax + by + cz + d = 0$

While algebraic geometry deals with polynomial equations, *Semi-Algebraic Geometry* deals with polynomial inequalities. This involves tools from Real Analysis, Functional analysis and measure theory.

2 Klein's Erlangen program

Felix Klein with his Erlangen program in 1872 showed the link between Geometry and Abstract Algebra. This program looked at geometry as the study of properties of a space invariant under a given group of transformations. Thus geometric properties could be described by the group of transformations, under the action of which the properties would remain invariant.

Example 2 *Euclidean distance between two points is a property that is invariant under the action of the Euclidean group (which is the group of rigid body motions in Euclidean space). So in* $\mathbb{R}^2$, *for example, the distance between two points* (x_1, y_1) *and* (x_2, y_2) *is given by* $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$. *Now suppose we perform the translations given by:*
$x' = x + a$
$y' = y + b$,

the new distance is $\sqrt{(x_2' - x_1')^2 + (y_2' - y_1')^2}$
$= \sqrt{(x_2 + a - x_1 - a)^2 + (y_2 + b - y_1 - b)^2}$
$=\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$,

which is the same as the distance between the pair of points before performing the co-ordinate transformations.

Angles, for example, are preserved, under rigid body motions and scaling.

2.1 Geometric Theorem Proving

In the Erlangen program, the hypothesis and the conclusions of a geometric theorem can be written down as polynomials, and a proof of the theorem would be equivalent to showing that if the polynomials corresponding to the hypothesis evaluate to zero, then the polynomial(s) corresponding to the conclusion evaluate to zero. This is the problem of ideal membership for polynomials in a ring of invariants for a geometric group. In general, determining ideal membership for polynomials turns out to be a hard problem (triple-exponential?). However, in this case, we also have the property that the polynomials are invariant under the action of certain groups. The Wu-Ritt decomposition algorithm gives an efficient way to determine ideal membership in this case.

3 Hilbert's Nullstellensatz

Hilbert's Nullstellensatz (German for "theorem of zeros") is a theorem in algebraic geometry that is useful in coming up with algorithms for determining ideal membership for polynomials.

Theorem 1 *$P_t \in \mathcal{I}(P_1, \ldots, P_k)$ if and only if there exist an integer m and multiplying polynomials $Q_1, Q_2, \ldots, Q_k$ such that $P_t^m = \sum_{i=1}^{k} Q_i P_i$.*

Now given a polynomial P_t, it is straightforward to verify if it is in the ideal generated by $P_1, \ldots, P_k$: Suppose we knew the degrees of the multiplying polynomials $Q_1, Q_2, \ldots, Q_k$, then constructing the multiplying polynomials would be sufficient to show membership of P_t in the ideal. To construct the multiplying polynomials, we need to determine coefficients of each of the terms for each multiplying polynomial. Taking these as variables, simplifying $\sum_{i=1}^{k} Q_i P_i$ to group like terms and equating coefficients of corresponding terms on the right and left hand sides, we observe that we need to solve a system of linear equations, in order to find the coefficients of the multiplying polynomials, which is an easy problem. However, in practice, the coefficients of the multiplying polynomials are not known. Brownawell [1] derived upper bounds on the degrees of $Q_1, \ldots, Q_k$ in terms of the degrees of $P_1, \ldots, P_k$. This immediately gives us an algorithm for checking ideal membership. For each possible degree (up to the Brownawell bound), we get a system of linear equations. If atleast one of these systems is consistent, then P_t lies in the ideal generated by $P_1, \ldots, P_k$, otherwise it does not. We illustrate this with an example:

Example 3 *Let*

$P_1 : x^2 + x + 1$
$P_2 : 2x + 3$
and

$P_t : 5x^2 + 11x + 7.$

We wish to determine if P_t is in the ideal generated by P_1 and P_2. Further, let us assume that the multiplying polynomials have degree atmost 1. Thus let,

$Q_1 : a_1x + b_1$
$Q_2 : a_2x + b_2.$

Now from Hilbert's Nullstellensatz, P_t is in the required ideal iff,
$P_t = Q_1P_1 + Q_2P_2$
$\Leftrightarrow 5x^2 + 11x + 7 = (a_1x + b_1)(x^2 + x + 1) + (a_2x + b_2)(2x + 3)$
$\Leftrightarrow 5x^2 + 11x + 7 = a_1x^3 + (a_1 + b_1 + 2a_2)x^2 + (a_1 + b_1 + 3a_2 + 2b_2)x + (b_1 + 3b_2)$

Equating coefficients on the left and right-hand-side, we get the following system of linear equations:

$a_1 = 0$
$a_1 + b_1 + 2a_2 = 5$
$a_1 + b_1 + 3a_2 + 2b_2 = 11$
$b_1 + 3b_2 = 7.$

This system turns out to have the unique solution: $a_1 = 0, b_1 = 1, a_2 = 2, b_2 = 2$. Thus P_t lies in the ideal generated by P_1 and P_2.

3.1 Checking if a set of polynomials does not have a common zero

It turns out that this problem can also be easily posed as an ideal membership problem.

Proposition 2 *A set of polynomials do not have a common zero if and only if the constant polynomial* 1 *is in the ideal generated by the set.*

4 Reducing Unsatisfiability to Ideal Membership

It turns out that several other problems can be reduced to ideal membership for polynomials. Here is one:

Problem 1 (Unsatisfiability) *Given a propositional formula, determine if no truth assignment to its variables makes the formula satisfiable.*

Unsatisfiability is known to be in co-$\mathcal{NP}$.

To reduce unsatisfiability to ideal membership,for each propositional variable, we construct a polynomial
$P_i : x_i^2 - x_i$.

From the propositional formula, we construct the polynomial P_t by replacing each conjunction with multiplication, each disjunction with addition, and replace each negation $\neg x_i$ with $(1 - x_i)$. The formula is unsatisfiable iff P_t, is

in the ideal generated by $P_1, P_2, \ldots, P_n$. We can verify if this is so by using Hilbert's Nullstellensatz along with the Brownawell bounds to generate a sequence of linear systems of equations and check if any of them is consistent. We illustrate this reduction with an example:

Example 4 *Consider the 3-SAT formula* $(x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_2 \vee x_3 \vee x_4)$.

As described before we have four polynomials $P_1, \ldots, P_4$, *with* $P_i : x_i^2 - x_i$.
This polynomial has two roots 0 *and* 1, 0 *corresponding to* F *and* 1 *corresponding to* T, *and the polynomial* P_t *is constructed such that* P_t *evaluates to zero for a particular assignment of 0s and 1s to the* x_i*s iff the propositional formula evaluates to false for the corresponding truth assignment to the propositional variables.*

Thus, the polynomial P_t *corresponding to the above propositional formula is:* $P_t : (x_1 + x_2 + (1 - x_3)).((1 - x_2) + x_3 + x_4)$

The idea is that a literal evaluates to False iff the corresponding expression evaluates to zero. Thus a disjunction of literals evaluates to false, iff in the polynomial, each term in the sum is zero, which makes the sum equal to zero. Similarly, a conjunction is false iff atleast one of the operands is false, and equivalently, the product of expressions evaluates to zero, iff atleast one of them is zero.

From the perspective of complexity theory, this reduction enables us to transfer upper bounds for Unsatisfiability from the problem of ideal membership and transfer lower bounds to ideal membership from Unsatisfiability.

5 Complexity Themes

The study of complexity usually has two different kinds of fields. One is the study of complexity measures related to computation and information. The other is the study of what are called complex systems.

5.1 Complexity measures related to computation and information

Computational Complexity encompasses the following broad themes:

1. **P vs. NP**: Some problems don't have fast algorithms (unless P=NP).
2. **NP vs. co-NP**: Some problems don't have short proofs.
3. **P vs. BPP**: Some problems cannot be derandomized.

This can be contrasted with the usual mathematical notions of complexity:

1. Dimension of representation.
2. Sparseness of representation.

5.1.1 Mulmuley's program

Ketan Mulmuley's program [2] to prove P≠NP involves proving lower bounds on some algebraic complexity measure, which would imply P≠NP.

5.1.2 An example of a problem for P vs. NP lower bounds

Problem 2 *Consider n points in $\mathbb{R}^d$. For $d = 2$,*
maximize $|S|$
such that
$\exists$ a set S of points
$\exists$ a set L of lines
such that any pair of points in S is separated by exactly half the lines in L.

5.1.3 Automated Geometry Theorem Proving

The problem of automated geometry theorem proving may be posed in Euclidean Geometry, Projective Geometry or Similarity Geometry. This is an example of a problem in the theme of NP vs. co-NP upper bounds. [3] is a good starting point for analytic approaches to this problem and [4] is a good reference for combinatorial and algebraic approaches.

5.2 Complex systems

Complex systems is a field that consists of problems from disparate fields. These problems have some common characteristics such as being *indecomposable* and having the property of *emergence*. They include problems from

1. Markets
2. Biological processes such as evolution
3. Weather
4. Dynamical systems
5. Iterated function systems
6. Games
7. Distributed systems

6 Sparse Representations

Here is an example of a sparseness question related to analysis:

Problem 3 (Interpolation) *Given certain points in a function f, pick a small number of basis function from a family of bases, and show that for a small number of bases (defined appropriately), the function cannot be exactly represented by interpolation when*

- *Each basis function is independent.*
- *When the basis functions are not independent.*

The field of *Wavelet Analysis* in particular, and in general *Nonlinear Approximation Theory* are interested in such questions.

The field of *Geometric Function Theory* (starting with Dvoretzky's Theorem) is interested in the following type of problem:

Problem 4 (Low-dimension and low-distortion embeddings) *Given a high dimensional set of points, does there exist a projection onto lower dimensions, which distorts it to a small extent?*

This type of problem is also tackled by Principal Components Analysis in Statistics and Machine Learning.

The Duality Theorem in Geometric Functional Analysis allows us to make non-existence results imply existence results.

7 Algebraic and Analytic approaches to complexity

We will consider analytic and algebraic approaches to the study of complexity and look at the similarities between the two approaches.

7.1 Analytic approach

We study boolean functions, which can be written using as few basis functions as possible,
$f = \sum_{b \in M \subseteq B} a_b b$

That is, we use as few basis functions as possible in M. B is a set of simple basis functions

If we cannot exactly represent the function with the basis, we try to approximate it:
$||f - \sum_{b \in M \subseteq B} a_b b|| < \epsilon$

7.2 Algebraic approaches

In the algebraic geometry approach, we treat sets as the zero set of a system of polynomial equations of low complexity. We might quantify low complexity by specifying bounds on number of equations, degree, number of variables or number of terms. We can also use semi-algebraic sets or a union of semi-algebraic sets.

The strength of the algebraic approach for complexity theory is that we can ask the the *input* $\in$ *set* and the *set* $\in$ *complexity class* questions in the same way.

Here is one way to algebrize:
Elements: linear programs (lps), geometric constraint systems (gcs) (systems of polynomial equalities and inequalities $g(x)$ which are somehow special; for example belong to an invariant ring of a geometric group or something else)
Sets: Set of lps/gcss that have a common zero/do not have a common zero.

Find a system of polynomials S (whose variables are coefficients of gcs g)
s.t. $S(g) = 0$ iff $\exists x \in F$ s.t.$g(x) = 0$
(F is some field, say the reals)

Note that this is a family of systems S_m, since their number of variables (coefficients of g) is unbounded since input set of g's is infinite.

Now to show g is not in the set, we need to show g do not have a common zero, which can be converted to an existential statement via Hilberts nullstellensatz, so then we can again get a system of polynomials
$\bar{S}$ s.t.
$\bar{S}(g) = 0$ iff there is no x s.t. $g(x) = 0$.

Complexity class: set of polynomial system-families S_m for which there is a "few, sparse, lowdegree" set of polynomials P_m
s.t. $S_m(g) = 0$ iff $P_m(g) = 0$ over a field F
i.e. $S =_F P$

Find a family of polynomial systems C_{S_m}
s.t.
$\exists P$ s.t. $C_S(P) = 0$ iff $\exists P$ (few/sparse/low-degree)
s.t. $S =_F P$

To show a lower bound, show C_S do not have a common zero. Which we can try to convert into an existential statement and then use the trick from earlier to find a polynomial system
B s.t.
$B(S) = 0$ iff C_S does not have a common zero iff S is not in the complexity class.

Algebrization is a hurdle to proving complexity lower bounds. See [5] for more.

References

[1] W.D. Brownawell, *Bounds for the Degrees in the Nullstellensatz*, Annals of Mathematics, **126** (1987), pp. 571-591.

[2] K. Mulmuley, M. Sohoni, *Geometric complexity theory I: An approach to the P vs. NP and related problems*, SIAM J. Comput., 31(2), pp. 496-526, (2001).

[3] I. J. Schoenberg, *Metric Spaces and Positive Definite Functions*, Transactions of the American Mathematical Society, Vol. 44, No. 3 (Nov., 1938), pp. 522-536.

[4] L.M. Blumenthal, *Theory and Applications of Distance Geometry*, Oxford, 1953.

[5] S. Aaronson, A. Wigderson, *Algebrization: a new barrier in complexity theory*, Proc. STOC 2008.

[6] C.H. Papadimitriou, *Computational Complexity*, Addison Wesley, 1993.

[7] J. Bourgain, *Harmonic Analysis and Combinatorics: How Much May They Contribute to Each Other?*, in Mathematics: Frontiers and Perspectives, V. Arnold, M. Atiyah, P. Lax, B. Mazur, eds., AMS 2000.

[8] I. Laba, *The Kakeya problem, and connections to harmonic analysis*, At `http://www.math.ubc.ca/ ilaba/kakeya.html`.

[9] N.H. Katz, T. Tao, *BOUNDS ON ARITHMETIC PROJECTIONS, AND APPLICATIONS TO THE KAKEYA CONJECTURE*, Mathematical Research Letters 6, 625-630 (1999).

[10] A. Samorodnitsky, L. Trevisan. *Gowers Uniformity, Influence of Variables, and PCPs*, In Proc. of 38th STOC, ACM, 2006.

[11] S. Arora, B. Barak, *Complexity Theory: A Modern Approach*, Cambridge University Press, expected in 2009. (A draft is available at `http://www.cs.princeton.edu/theory/complexity/` .

[12] T. Tao, *The dichotomy between structure and randomness*, International Congress of Mathematicians presentation, At `http://www.math.ucla.edu/ tao/preprints/Slides/icmslides2.pdf`

[13] S. Khot, A. Naor, *Nonembeddability theorems via Fourier analysis*, Mathematische Annalen 334, number 4, 821-852 (2006).

[14] `http://in-theory.blogspot.com/2006/06/gowers-uniformity.html`

[15] `http://in-theory.blogspot.com/2006/06/analytical-approaches-to-szemeredis_08.html`

[16] `http://lucatrevisan.wordpress.com/tag/additive-combinatorics/`

[17] `http://boolean-analysis.blogspot.com/2007/02/whats-new-in-fourier-analysis.html`

[18] A. A. Razborov, A. A. Sherstov, *The sign-rank of AC^0*, FOCS 2008.

[19] A. A. Sherstov, *The unbounded-error communication complexity of symmetric functions*, FOCS 2008.

[20] A. A. Sherstov, *Communication lower bounds using dual polynomials.*, Bulletin of the EATCS, 95:59-93, 2008. (Invited survey).

[21] P. Indyk, J. Matousek, *Low-distortion embeddings of finite metric spaces*, Handbook of Discrete and Computational Geometry.