CPSC 506 NOTES ON GEOMETRIC COMPLEXITY THEORY

JOEL FRIEDMAN

Abstract. These are my notes on the Mulmuley-Sohoni approach to lower bounds, designed for my CPSC 506 class, for students without a background in algebraic geometry, but who understand the interest in circuit and formula lower bounds and the permanent versus determinant question. These notes are a work in progress; use at your own risk: the material is probably incomplete, and may contain errors, jokes, inaccuracies, and worse.

0. Introduction: GCT and Permanent versus Determinant

This article describes some of the Mulmuley-Sohoni approach to lower bounds in [MS01] (henceforth GCT1); sequels include [MS06, MS05, MS07, Mul12]). "Geometric Complexity Theory" aims to attack many problems in algebraic and Boolean complexity theory with tools from geometric invariant theory.

We begin, as does GCT1, with their ideas on the Superpolynomial Permanent-Determinant conjecture, that the permanent does not have a polynomial size formula, or, equivalently, cannot be written as a determinant of a polynomial sized matrix, each entry of which is either a variable or a constant. This is an exciting question, which has received much attention and is open at present. P vs. NP is related to *circuit* size lower bounds (rather than formula size) in *Boolean* (rather than algebraic) complexity theory; we'll worry about that later. The work of Valiant (see [Val79a, Val79b]) lead to the question of expressing a permanent as a determinant; Valiant showed that the computing the determinant is complete for the class of quasi-polynomially sized formulas, and that the permanent is complete for a class that is an algebraic analog of NP; we shall refer to the Superpolynomial Permanent-Determinant conjecture as Valiant's conjecture, even though it is not clear to us where/if Valiant made this conjecture explicitly, and sometimes people quote Valiant's conjecture with a Super-quasi-polynomial lower bound.

The approach in GCT1 begins with a very simple and clever strengthening of Valiant's notion of reduction ([Val79a]), and requires nothing but calculus and linear algebra. Then GCT1 proceeds to pursue their strengthened conjecture via geometric invariant theory. We'll see how far we get...

1. The General Setup

Mulmuley-Sohoni formulate a more lenient notion of Valiant's reducibility. Let $f(X) = f(X_1, \ldots, X_N)$ and $g(Y) = (Y_1, \ldots, Y_M)$ be polynomials over $\mathbb{C}$, the complex numbers. We say that f *is reducible to* g if there is an $A \in \mathbb{C}^{M \times N}$, i.e., an

Date: Wednesday 12th February, 2014, at 10:09(remove currenttime eventually).

Research supported in part by an NSERC grant. Research done in part at the Banff International Research Station for Mathematical Innovation and Discovery.

$M \times N$ matrix with entries in $\mathbb{C}$, for which

$$f(X) = g(AX). \tag{1.1}$$

The approach of Mulmuley-Sohoni is roughly that if g has very different "symmetry" than f, then you should (or may) be able to refute (1.1).

To be precise, a *symmetry* in Y of $g(Y)$ is a $S \in \mathrm{GL}_M$, i.e., an invertible $S \in \mathbb{C}^{M\times M}$, for which $g(SY) = g(Y)$ for all Y; the set of all symmetries of g forms a subgroup of GL_M. In the simple case $M = N$ and $A \in \mathbb{C}^{M\times N}$ is invertible, then each symmetry, S, of $g(Y)$, gives rise to a symmetry, S', of $h(X) = g(AX)$ via conjugation in A, namely $S' = A^{-1}SA$. So in case f can be reduced to g by an invertible linear transformation, the symmetry group of g and that of f are conjugates.

The case of interest to us will be where $M > N$, and $A \in \mathbb{C}^{M\times N}$. In this case a symmetry of $g(Y)$ may not extend to a symmetry of $h(X) = g(AX)$. Consider the toy case of $M = 2$, $N = 1$, and $AX = (X_1, 2X_1)$; the polynomial $g(Y) = Y_1Y_2$ has the symmetry $SY = (3Y_1, Y_2/3)$ (in characteristic zero); there is no symmetry, S', of X such that S' multiplies X_1 by 3 and multiplies $2X_1$ by $1/3$.

Since the symmetries of $g(Y)$ can be lost in $g(AX)$, Mulmuley-Sohoni look elsewhere. This involves a gambit.

Let $\iota \in \mathbb{C}^{N\times M}$. Note that (1.1) implies that

$$(f \circ \iota)(Y) = f(\iota Y) = g(BY),$$

where $B = \iota A$. Define

$$\mathrm{Lin}(g) = \{g(BY) \mid B \in \mathbb{C}^{M\times M}\}; \tag{1.2}$$

Mulmuley-Sohoni seek to show that

$$f \circ \iota \notin \mathrm{Lin}(g) \tag{1.3}$$

for certain f and g. When $B = \iota A$ as above, then B has rank at most N; yet (1.2) does not limit B to being of rank at most N. Hence (1.3) seems like an extra leap of faith when $M > N$.

To discuss Mulmuley-Sohoni further, consider

$$\mathrm{Lin}^\circ(g) = \{g(BY) \mid B \in \mathrm{GL}_M\},$$

which a subset of $\mathrm{Lin}(g)$. Each element of $\mathrm{Lin}^\circ(g)$ has the same symmetries as g, up to conjugation. Hence, roughly speaking, if $B \in \mathbb{C}^{M\times M}$ is not invertible, then some "small perturbation" of B will be invertible and, hence, exhibit a symmetry conjugate to that of g. So if (1.3) holds, in any neighbourhood of $f \circ \iota$ we should see elements with g-type symmeties, or, perhaps equivalently, $f \circ \iota$ shoud experience some sort of degenerate g-type symmetry.

For example, Valiant's conjecture studies the case $M = m^2$, for a positive integer, m, where

$$g(Y) = \det([Y]), \quad Y = \{y_{ij}\}_{i,j=1,\dots,m}; \tag{1.4}$$

we write $[Y]$ to emphasize that we are viewing Y as an $m\times m$ matrix. If $[M_1], [M_2] \in \mathrm{SL}_m(\mathbb{C})$, i.e., $m \times m$ matrices in $\mathbb{C}$ of determinat one, then

$$S([Y]) = [M_1][Y][M_2] \tag{1.5}$$

is a symmetry of the determinant. We caution the reader that an expression such as BY as in (1.3) means an arbtrary linear transformation of the $M = m^2$ variables

of Y, whereas (1.5) refers to transformations obtained by matrix multiplication in $\mathbb{C}^{m\times m}$, unlike BY which represents, in a sense, an $M \times M$ matrix multiplied by an $M \times 1$ vector of indeterminates. For example

$$\det\left(\begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22}\end{bmatrix}\right) = \det\left(\begin{bmatrix} 5 & 0 \\ 0 & 1/5\end{bmatrix}\begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22}\end{bmatrix}\begin{bmatrix} 4 & 7 \\ -1/7 & 0\end{bmatrix}\right)$$

attests to the fact that $\det(Y)$ for $m = 2$ ($M = 4$) is invariant under

$$S((y_{11}, y_{12}, y_{21}, y_{22}) = \big(20y_{11} - (5/7)y_{12}, 35y_{11}, (4/5)y_{21} - (1/35)y_{22}, (7/5)y_{21}\big).$$

Valiant's conjecture concerns

$$f(X) = x_0^{m-n}\mathrm{perm}([X]), \quad X = \{x_0\} \cup \{x_{ij}\}_{i,j=1,\dots,n}, \tag{1.6}$$

where $N = n^2+1$, X consists of a single variable x_0 plus an $n\times n$ matrix of variables, and $[X]$ consists of the matrix variables of X, viewed as a matrix. The variable x_0 is an auxilliary, homogenizing variable used to boost the degree of f to that of g. Valiant conjectured that given n, the minimum value of m for which f can be reduced to g is a superpolynomial function of n (Valiant actually conjectured more, in slightly different terms, with $\mathbb{C}$ replaced with an arbitrary field of characteristic other than two.)

Let us return to the general situation with $g = g(Y)$ homogeneous and Y N-dimensional. The set of homogenous polynomials of degree D in Y, which we denote $\mathrm{Poly}(Y, D)$, is isomorphic to $\mathbb{C}^S$ as an $\mathbb{C}$-vector space for $S = \binom{N+D-1}{D}$; this gives a topology on $\mathrm{Poly}(Y, D)$ from the standard topology on $\mathbb{C}^S$.

Definition 1.1. Let $f(X) = f(X_1, \dots, X_N)$ and $g(Y) = g(Y_1, \dots, Y_M)$ be polynomials over $\mathbb{C}$, homogeneous of degree D. For $h \in \mathrm{Poly}(Y, D)$, let

$$\mathrm{Stab}(h) = \{A \in \mathrm{GL}_M \mid h(AY) = h(Y)\},$$

which is just the stabilizer of h under the natural action of GL_M on $\mathrm{Poly}(Y, D)$ (namely $(A, h(Y)) \mapsto h(AY)$). We say that that f is *Mulmuley-Sohoni-separated* from g (or simply *MS-separated*) if there is an $\iota \in \mathbb{F}^{M\times N}$ for which some neighbourhood of $f\iota$ has no elements with a stabilizer conjugate to that of g.

It is immediate that if f is MS-separated from to g, then f cannot be reduced to g. Let us finish with a strengthening of Valiant's conjecture.

Conjecture 1.2 (Mulmuley-Sohoni)**.** *For a positive integer, n, let $m = m(n)$ be the smallest integer for which the permanent in (1.6) is MS-separated from the determinant in (1.4) over $\mathbb{C}$. Then $m(n)$ is superpolynomial in n (i.e., for any constant, $c > 0$, there is an n_0 for which $m(n) \geq cn^c$ for all $n \geq n_0$).*

Mulmuley-Sohoni make a stronger and more specific conjecture, for $\mathbb{C}$ replaced with an arbitrary algebraically closed field, for the Zariski topology, (see Conjecture 4.3 and Proposition 4.2 of GCT1).

2. The Quotient

We seek to write view MS-separation, in Definition 1.1, in terms of quotients. Namely, with notation as in Definition 1.1, recall that GL_M acts on $\mathrm{Poly}(Y, D)$ via $(A, g(Y)) \mapsto g(AY)$. We therefore get a quotient space

$$\mathrm{QPoly}(Y, D) = \mathrm{Poly}(Y, D)/\mathrm{GL}_M,$$

whose elements are GL_M orbits, i.e., equivalence classes of polynomials under the GL_M action. Let

$$\mathcal{Q}\colon \mathrm{Poly}(Y,D) \to \mathrm{QPoly}(Y,D)$$

be natural map taking a polynomial to its GL_M orbit. There are a number of appealing aspects of working with $\mathrm{QPoly}(Y,D)$.

First, as mentioned before, if $g_1, g_2 \in \mathrm{Poly}(Y,D)$ are in the same GL_M orbit, i.e., $g_1(AY) = g_2(Y)$ for some $A \in \mathrm{GL}_M$, then the stabilizers of g_1 and g_2 are the same up to conjugation; hence one can view an element of $\mathrm{QPoly}(Y,D)$, i.e., a GL_M orbit in $\mathrm{Poly}(Y,D)$, as having a well-defined stabilizer, up to conjugation. Second, MS-separation is eloquently expressed in QPoly.

Theorem 2.1. *Let $f(X) = f(X_1,\dots,X_N)$ and $g(Y) = g(Y_1,\dots,Y_M)$ be polynomials over $\mathbb{C}$, homogeneous of degree D. Then f is MS-separated from g iff $\mathcal{Q}(f)$ does not lie in the closure of the points, $\mathcal{Q}(g')$ (in the induced topology on* QPoly*), over $g' \in \mathrm{Poly}(Y,D)$ that have the same symmetries as g.*

The proof of the above theorem is almost immediate from the definition of the induced topology. However, this natural and beautiful lower bound approach has produced, QPoly, which, as we've hinted at above, has points that are not closed subsets of the space. So let's consider this theorem carefully and give a toy example.

Proof. The main point is that a set in QPoly is open in the induced topology, by definition, iff its inverse image in Poly is open; in other words, the open sets in the induced topology come from GL_M-invariant open sets in Poly.

Let f be MS-separated from g, and $\mathcal{O}$ an open subset containing f in which no element has a stabilizer conjugate to that of g; then the same is true of any translate, $A\mathcal{O}$, of $\mathcal{O}$ by an $A \in GL_M$. union, $\mathcal{O}'$, of GL_M translates of $\mathcal{O}$, is an open set in $\mathrm{Poly}(Y,D)$ that is GL_M invariant and does not contain g. Hence the closure of $\mathcal{Q}(g)$ does not contain $\mathcal{Q}(f)$. The converse is similar, but easier. □

Example 2.2. Let

$$g(Y) = g(Y_1,Y_2,Y_3) = Y_2^2Y_3 - Y_1^3 - Y_1Y_3^2.$$

Then the orbit of g under GL_3 contains

$$Y_2^2Y_3 - Y_1^3 - \epsilon Y_1Y_3^2$$

for every $\epsilon \neq 0$, via

$$(Y_1,Y_2,Y_3) \mapsto (Y_1, Y_2\epsilon, Y_3\epsilon^2).$$

Hence the closure of $\mathcal{Q}(g)$ in $\mathrm{QPoly}(Y,3)$ contains the image under $\mathcal{Q}$ of

$$h(Y) = Y_2^2Y_3 - Y_1^3.$$

However, g and h do not have the same stabilizers; indeed, the stabilizer of g is finite, of order two, with the unique non-zero symmetry $(Y_1,Y_2,Y_3) \mapsto (Y_1,-Y_2,Y_3)$ (homework), while the stabilizer of h is infinite, containing $(Y_1,Y_2,Y_3) \mapsto (Y_1,Y_2c,Y_3/c^2)$ for any nonzero $c \in \mathbb{C}$ (homework).

The above example is based on the degeneration of the elliptic curve $y^2 = x^3 - \epsilon x$ to the genus zero curve $y^2 = x^3$. In general, we expect a "degenerate picture" at new points in the closure of a point; although the order two symmetry of g above persists, the degeneration may give a whole bunch of extra symmetry. Of course, any neighbourhood of h contains elements with the same symmetry as g, indeed in the same orbit as g.

GCT1 points out that the determinant is characterized by its symmetries; it follows that any element whose symmetries are the same as the determinant lies in the orbit of the determinant. This gives some evidence that their conjecture is not asking far more than Valiant's. Furthermore, if one replaces g by a polynomial that is not characterized by its symmetries, one could alter our definition of MS-separated so that in Theorem 2.1 we take only the closure of the single point $\mathcal{Q}(g)$

3. The Appeal of Geometric Invariant Theory

Determining basics facts about QPoly, such as whether one point is in the closure of another, generally seems to be a very difficult problem. The good news is that such questions are of vital importance in studying moduli spaces in algebraic geometry, and there are some significant tools concerning the foundations of such quotient spaces.

The bad news about QPoly is that we expect it to be difficult to understand. The question of permanent versus determinant and/or algebraic formula size has been around a long time, and the best progress toward Valiant's conjecture has been a very recent quadratic lower bound (see [Mignon-Ressayre]).

Yet, there is good news about QPoly. The GCT1 approach does not require you to take an $f(X)$, choose ι, and then try to prove that no neighbourhood of $f\iota$ has elements with the right kind of symmetry, at least not explicitly. Trying, brute force, to perturb $f\iota$ and claim it has no symmetry (or not enough or too much) is a bit like trying to show that a problem has no algorithm—given a symmetry or algorithm, it is often not hard to verify that it holds, but it is a lot harder to show that, say, no symmetry exists. For example, imagine that we perturb the 2×2 permanent, choose ι as the map $X_{ij} \mapsto Y_{ij}$ (with Y being a matrix of indeterminates of size at least that of X), and try to analyze the symmetries:

$$f\iota(Y, \epsilon) = Y_{11}Y_{22} + Y_{12}Y_{21} + \epsilon Q(Y),$$

where Q is some homogenous polynomial of degree two; you wish to argue that for any $Q \in \mathrm{Poly}(Y, 2)$, for sufficiently small ϵ, we do not see the same symmetry as g (for some g); can you exhaustively check all possible symmetries of $f\iota$?

Of course, you don't have to find all symmetries of neighbours of $f\iota$ and of g; it's enough to find one representation, that, say, occurs with higher multiplicity in the "polynomials on" (i.e., coordinate ring) of the permanent closure than on that of the determinant closure.

We recall that the theory of moduli spaces invovles equivalence classes in nice spaces where a quotient has some troublesome properties. TO DO: Examples: (1) $\mathbb{C}$ modulo $\mathbb{Z}$, as smooth functions and algebraic functions, (2) elliptic curves, with choices of x and y and without, etc.

Etc.

We intend to write more at some point, but at this point a good place to read would be [GR12].

References

[GR12] Joshua A. Grochow and Korben Rusek. Report on "mathematical aspects of p vs. np and its variants.". *CoRR*, abs/1203.2888, 2012. Available at http://arxiv.org/abs/1203.2888.

[MS01] Ketan Mulmuley and Milind A. Sohoni. Geometric Complexity Theory I: An Approach to the P vs. NP and Related Problems. *SIAM J. Comput.*, 31(2):496–526, 2001.

[MS05] Ketan Mulmuley and Milind A. Sohoni. Geometric Complexity III: on deciding positivity of Littlewood-Richardson coefficients. *CoRR*, abs/cs/0501076, 2005.

[MS06] Ketan Mulmuley and Milind A. Sohoni. Geometric Complexity Theory II: Towards explicit obstructions for embeddings among class varieties. *CoRR*, abs/cs/0612134, 2006.

[MS07] Ketan Mulmuley and Milind A. Sohoni. Geometric Complexity Theory IV: quantum group for the Kronecker problem. *CoRR*, abs/cs/0703110, 2007.

[Mul12] K. D. Mulmuley. Geometric Complexity Theory V: Equivalence between blackbox derandomization of polynomial identity testing and derandomization of Noether's Normalization Lemma. *ArXiv e-prints*, September 2012.

[Val79a] L. G. Valiant. Completeness classes in algebra. In *Proceedings of the eleventh annual ACM symposium on Theory of computing*, STOC '79, pages 249–261, New York, NY, USA, 1979. ACM.

[Val79b] L.G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189 – 201, 1979.

Department of Computer Science, University of British Columbia, Vancouver, BC V6T 1Z4, CANADA, and Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, CANADA.

E-mail address: jf@cs.ubc.ca or jf@math.ubc.ca