CS38600-1 Complexity Theory A **Spring 2003**

Lecture 1 : Geometric Complexity Theory Overview

Lecturer: Ketan Mulmuley *Scribe: Murali Krishnan Ganapathy*

Abstract

In this exposition, we give a overview of the GCT[1] approach to solve fundamental lower bound problems in algebraic models of computation.

1.1 Lower bound problems

Consider a polynomial $f(\vec{x}) \in \mathbb{Z}[\vec{x}]$ with integral coefficients. The non-uniform version of the P v/s NP problem, prescribes a specific such f and asks if it can be shown not to have polynomial size arithmetic circuits over $\mathbb{F}_2$. The characteristic zero version of the same problem asks whether we can prove that suitable f's do not have polynomial sized arithmetic circuits over $\mathbb{Z}$ (or equivalently $\mathbb{Q}$).

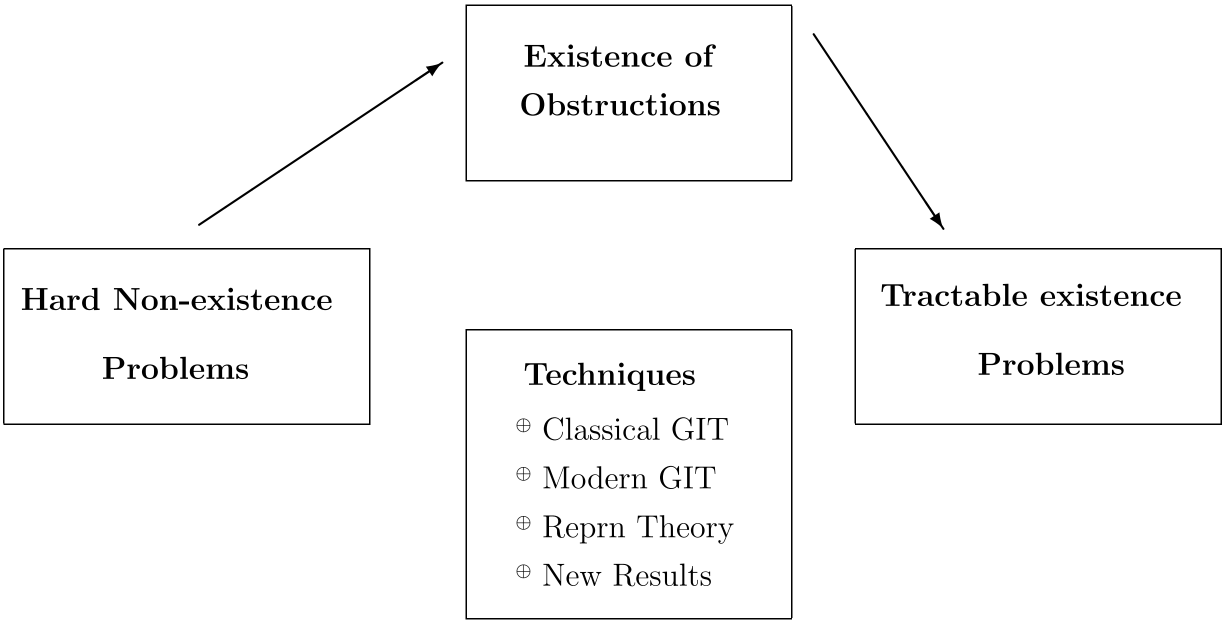
Clearly if an f has a polynomial sized circuit over $\mathbb{Z}$, then it can be transformed into a polynomial sized circuit over $\mathbb{F}_2$ to compute $f \mod 2$. Hence the characteristic zero version is an implication of the characteristic 2 version of the problem. Hence forth, we concentrate only on characteristic zero version of the problem.

In order to prove that a certain f does not have polynomial size circuits over $\mathbb{Z}$, we hope to prove a (possibly) stronger statement, viz. that it does not have polynomial size circuits over $\mathbb{C}$ (since $\mathbb{C}$ has more constants than $\mathbb{Z}$). Since $\mathbb{C}$ is an algebraically closed field with a well understood topology, we hope that results in Algebraic Geometry, Representation Theory and Geometric Invariant Theory will come to our rescue and help us solve the problem. What we will see is that the current state of knowledge in these areas is not sufficient to help us resolve the lower bound problems we are interested in. However, we will be able to show that knowing answers to certain mathematical questions (which have independent mathematical interest) will help us resolve our lower bound questions.

So what is so great about this approach? Lower bound problems are essentially problems of non-existence, and hence they are hard to solve. This approach reduces the hard non-existence problems into tractable existence problems. This is akin to the NP-characterization of primality, where the proof of primality of p is a generator of $\mathbb{Z}_p^*$. These existence problems are in the areas of Representation Theory and Algebraic Geometry. The primality reduction uses basic number theory and group theory, while the GCT reduction uses classical GIT[2] (due to Hilbert and Weyl), modern GIT (due to Mumford, Kempf and others), together with some new results.

[1] Geometric Complexity Theory

[2] Geometric Invariant Theory


Existence of Obstructions
Hard Non-existence Problems
Tractable existence Problems
Techniques
⊕ Classical GIT
⊕ Modern GIT
⊕ Reprn Theory
⊕ New Results

Before we explain some of the problems which need to be solved for a successful application of this GCT approach, lets pause to recall some basic results of representation theory. Some of the representation theoretic problem, encountered in this approach is outlined in §1.4.

1.2 Representation Theory - An Introduction

We start with a working definition of a reductive group.

Definition 1.1 *A group G is said to be **reductive** if*

1. *G is finite or $\mathbb{C}^*$,*
2. *(simple groups) $G = SL_n(\mathbb{C}), SO_n(\mathbb{C}), SP_{2n}(\mathbb{C})$,*
3. *G is an* exceptional *group or*
4. *G is a direct product of reductive groups.*

We will never encounter exceptional groups, so we don't bother defining it here. Recall that $SO_n(\mathbb{C})$ consists of matrices which preserve a symmetric bilinear form and $SP_{2n}(\mathbb{C})$ consists of matrices which preserve a skew-symmetric bilinear form. These definitions determine the group uniquely up to conjugation.

Definition 1.2 *A representation ρ of a group G is a homomorphism ρ from G to a $GL(V)$, where V is a finite dimensional complex vector space. Here $GL(V)$ denotes the group of all invertible linear transformations on V. Note that a representation should specify the vector space in addition to the homomorphism.*

A representation may also be viewed as equipping the vector space V with a $\mathbb{C}[G]$-module structure, i.e. a vector space with a G-action which is compatible with the linear structure. When the representation is obvious from context, we denote $\rho(g)(v)$ as gv, where $g \in G, v \in V$.

Definition 1.3 *Let V and W be two representations of G. A G-**equivariant map** or a homomorphism between the two representations, is a map φ between the two underlying vector spaces which commutes with the G-action on the two vector spaces, i.e. $\forall g \in G, \varphi(gv) = g\varphi(v)$.*

Definition 1.4 *Let V be a representation of G. A subspace W of V is called a **sub-representation** if W is invariant under G i.e. $\forall g \in G,\ gW \subseteq W$.*

Every representation has two trivial sub-representations, viz, itself and the null representation $\{0\}$. A representation V is called **irreducible** if has no non-trivial sub-representations, and otherwise called **reducible**.

Here are some examples of representations:

1. $G = SL_n(\mathbb{C}), V = \mathbb{C}^n$: action by left multiplication

2. $G = S_n, V = \mathbb{C}^n$: action by permuting coordinates.

3. Any G, any V: $g(v) = v$ (the trivial action).

4. If G is a finite group and X is a G-set (i.e. permits a G-action), then $V = \mathbb{C}^X$ is a representation of G. Here G acts on the basis ($\{e_x : x \in X\}$) by acting on the subscripts.

5. Special case of above, where $X = G$ and G acts on itself by left multiplication. This representation is called the **left regular representation** of G.

Lets see some ways by which new representations may be constructed from old. Let V and W be two representations. The **direct sum** $V \oplus W$ of the two representations is a G-representation through the action $g(v, w) = (g(v), g(w))$. Similarly the **tensor product** $V \otimes W$ is a G-representation through the action $g(v \otimes w) = g(v) \otimes g(w)$.

Let V, W be vector spaces and suppose V admits a G-action. Suppose also that $T : W \hookrightarrow V$, is an injection of vector spaces and $\mathrm{Im}(T)$ is G-invariant. Then T induces a G-action on W as well, since $W \cong \mathrm{Im}(T)$.

In particular if V is a G-representation, then it induces a G-action on the **n-fold alternating product** $\Lambda^n(V)$ via the map from

$$\Lambda^n(V) \mapsto V^{\otimes n} \text{ which sends } v_1 \wedge \cdots \wedge v_n \mapsto \sum_{\tau \in S_n} sgn(\tau)\ \ v_{\tau(1)} \otimes \cdots \otimes v_{\tau(n)}$$

Similarly the map from

$$Sym^n(V) \mapsto V^{\otimes n} \text{ which sends } v_1 \ldots v_n \mapsto \sum_{\tau \in S_n} v_{\tau(1)} \otimes \cdots \otimes v_{\tau(n)}$$

shows that the **n-fold symmetric product** $Sym^n(V)$ also admits a G-action.

If V is a G-representation, so is the **dual** V^*, via the action $g(f)(v) = f(g^{-1}v)$. Here $g \in G, f \in V^*, v \in V$. Finally, if V and W are G-representations, then $Hom(V, W)$ admits a G-action via $g(\varphi)(v) = g(\varphi(g^{-1}v))$. Here $Hom(V, W)$ is the (vector) space of all maps from V to W. Actually, the dual representation is a special case of this, since $V^* = Hom(V, \mathbb{C})$.

1.3 Complete reducibility

In this section, we prove Weyl's result on complete reducibility of representations of finite groups.

Proposition 1.5 *Let V be a G-representation and $W \subseteq V$ be a sub-representation. Then W has a complementary subspace $W^{\perp}$ which is also G-invariant.*

Proof: Let $\langle \cdot, \cdot \rangle$ be any hermitian inner product on V. Define a new hermitian inner product by $(x, y) = |G|^{-1} \sum_{g \in G} \langle gx, gy \rangle$. Now let $W^{\perp}$ be the orthogonal complement of W under $(\cdot, \cdot)$. Then it is easy to see that $W^{\perp}$ is also G-invariant. ■

Corollary 1.6 *Any representation is a direct sum of irreducible representations.*

Proof: If V is not irreducible, let W be a non-zero proper sub-representation of V. Then $V = W \oplus W^{\perp}$ by the above result. By induction on $\dim(V)$, both W and $W^{\perp}$ can be written as a direct sum of irreducible representations. ■

Note that we have not yet proved that the decomposition is unique. That is accomplished by

Lemma 1.7 ***(Schur's lemma)*** *Let V and W be irreducible G-representations, and $\varphi : V \mapsto W$, a G equi-variant map. Then*

1. *Either $\varphi = 0$ or an isomorphism.*
2. *If $V = W = \mathbb{C}^m$ and φ an isomorphism, then $\varphi = \lambda I$, for $\lambda \in \mathbb{C}$.*

Proof: Both $\ker(\varphi)$ and $\mathrm{Im}(\varphi)$ are G-invariant submodules of V and W respectively. If $\ker(\varphi) \neq \{0\}$ or $\mathrm{Im}(\varphi) = \{0\}$ then $\varphi = 0$. So, if $\varphi \neq 0$, then the only possibility is $\ker(\varphi) = \{0\}$ and $\mathrm{Im}(\varphi) = W$, i.e. φ is an isomorphism.

For the second claim, apply the previous result to $\varphi - \lambda I$, where λ is any eigenvalue of φ (exists since $\mathbb{C}$ is algebraically closed), and conclude that $\varphi = \lambda I$. ■

Theorem 1.8 ***(Complete Reducibility - Weyl)*** *If V is a representation of a finite group G, then V can be written as $\oplus_i V_i^{a_i}$, where V_i are irreducible G-representations and $a_i > 0$ are integers. Moreover this decomposition is unique.*

Proof: We have already shown the existence. Suppose $V = \oplus_i U_i = \oplus_j W_j$ are two decompositions, where the U_i's and W_j's are irreducible representations, not necessarily distinct. Let φ denote the identity map from $V = \oplus_i U_i$ to $V = \oplus_j W_j$, and θ_i be its restriction to U_i. Since $\theta_i \neq 0$, $\mathrm{Im}(\theta_i) \cap W_j \neq 0$ for some j, and by Schur's lemma $U_i \cong W_j$ for suitable j. Remove U_i and W_j from either side and continue. ■

1.4 Tractable Existence Problems

We have seen how all representations of a finite group, can be written as the direct sum of irreducible representations. The same is true for a larger class of groups, which includes compact lie groups. So the problem of classifying all representations for these groups, boils down to classifying all their irreducible representations. This has been done for many classes of groups, including

1. Simple groups – Weyl, Killing, Cartan,
2. S_n – Frobenious, Schur
3. Simple groups of Lie type (e.g. $SL_n(\mathbb{F}_q)$) – Deligne, Lusqtiq(?)

For example, every irreducible representation of $SL_n(\mathbb{C})$ can be tagged with a *Young Tableaux.* The same is true for S_n as well. In these cases, we can identify an irreducible representation with the Young tableaux associated with it. By $V_\mu(G)$, we denote the irreducible G-representation with tag μ.

Another important computational problem involving group representations is the following: Given a reductive group G, an irreducible representation $V_\mu(G)$ and a subgroup H, compute the decomposition of the $V_{\mu(G)}$ considered as a H-representation.

A decision version of the same problem is the **decomposition problem**: Given a reductive group G, an irreducible G-representation $V_\alpha(G)$, a subgroup H of G and an irreducible H-representation $V_\mu(H)$, decide whether $V_\mu(H)$ occurs in the decomposition of $V_\alpha(G)$ as a H-representation.

A special case is the **tensor product decomposition problem** obtained by setting $G = H \times H$, and taking the diagonal subgroup $\{(h,h) : h \in H\} \subseteq G \cong H$ as the subgroup. Let $V_\alpha(H), V_\beta(H)$ and $V_\mu(H)$ be three irreducible H-representations. Then $V_\alpha(H) \otimes V_\beta(H)$ is an irreducible G-representation. In this case, the problem is to decide whether $V_\mu(H)$ is a sub-representation of $V_\alpha(H) \otimes V_\beta(H)$.

The problem above has been solved for some special families of groups. For example, if $H = SL_n(\mathbb{C})$, then the Littlewood-Richardson rule gives a polynomial time (in input bit length) algorithm to find the complete decomposition of $V_\alpha(H) \otimes V_\beta(H)$. More generally, the Kashiwara-Littlemann rule can be used to settle the case where G is a simple group.

Conjecture 1 There exists a polynomial time algorithm to solve the Tensor product decomposition problem for $H = S_n$

The tensor product decomposition problem is in turn a special case of the **Plethysm Problem**. Here the problem is to describe the complete decomposition (into irreducible representations with multiplicities) of representations derived from a given representation. For e.g. $V \otimes V, V^*, Sym^k(V), \Lambda^k(\Lambda^l V)$. If V itself is a sum of two representations then these representations decompose accordingly, since if $V = U \oplus W$, then

1. $V \otimes V = (U \otimes U) \oplus (U \oplus W) \oplus (W \otimes U) \oplus (W \otimes W)$
2. $\Lambda^k(V^*) = \Lambda^k(V)^*$
3. $\Lambda^k(V) = \sum_{i+j=k} \Lambda^i(U) \otimes \Lambda^j(W)$

and so on.

Conjecture 2 The decision version of the Plethysm problem has a polynomial time (in input bit length) algorithm for representations of reductive groups.

1.5 Conclusion

The GCT approach provides a unified approach to attack many fundamental lower bound problems occurring in Algebraic models of computation. It provides a recipe for converting hard non-existence questions into "easy" existence problems. This approach also relates the P v/s NP and other lower bound questions to deep areas of mathematics like GIT, Representation theory and eventually to String theory through quantum groups!