CS 880: Complexity of Counting Problems 02/14/2012

Lecture 7: General Dichotomy

Instructor: Jin-Yi Cai Scribe: Chetan Rao

1 Introduction

In today's lecture, we will see a more general version of dichotomy theorem. In the previous lectures, we concentrated mainly on two techniques - Holographic transformation and interpolation. In particular, we proved the following dichotomy of single ternary signatures -

$$\text{Holant}^*([x_0, x_1, x_2, x_3]) \tag{1}$$

Instead of moving on and continuing to a full dichotomy of Holant$^*(\mathcal{F})$ (where $\mathcal{F}$ is an arbitrary set of functions), we branch to another topic in counting complexity which involves algebraic techniques that we have not seen in the earlier lectures.

Before we move on, we'll look into how holographic transformations are used to establish dichotomy for a set of signatures Holant$(\mathcal{F})$. For instance, consider the 2-3 regular bipartite graph ($G = (U, V, E)$ where $deg(u \in U) = 2$ and $deg(v \in V) = 3$) case:

$$\text{Holant}^*([y_0, y_1, y_2] | [x_0, x_1, x_2, x_3])$$

The main idea is to transform this form to Holant$^*([1, 0, 1] | [x_0', x_1', x_2', x_3'])$ where [1,0,1] is the Equality function of arity 2 ($=_2$). The Equality is absorbed on the LHS and reduces it to the case described in (1).

Exercise 1. *Determine conditions under which the above holographic transformation is possible -*

$$Holant^*([y_0, y_1, y_2] | [x_0, x_1, x_2, x_3]) \Longrightarrow Holant^*([1, 0, 1] | [x_0', x_1', x_2', x_3'])$$

Exercise 2. *Prove a dichotomy for Holant*$^*([y_0, y_1, y_2] | [a, 1, 0, 0])$ *for any* a.

Once we complete it for the 2-3 case, we can extend it further to a single function $f = [x_0, x_1, x_2, \ldots, x_n]$ of arity $n > 3$ and to set of functions $\mathcal{F}$.

The sub-signatures are obtained by the following unary functions - $[0, 1]$ or $[1, 0]$ akin to the constant 1 or 0 functions respectively i.e. if the external inputs to the unary functions are 1 or 0 respectively, they accept.

For example, if we have a signature of $[x_0, x_1, \ldots, x_n]$ and append 1 to it, it becomes a $[x_1, x_2, \ldots, x_n]$ signature as the weight increases by 1. On the other hand, if we append 0, we get $[x_0, x_1, \ldots, x_{n-1}]$. This way, we can construct arbitrary sub-signatures and obtain a restricted set of arity 3 sub-signatures for which we know the dichotomy.

However, there is still a problem in the case of arity 2 signatures (which are 'promiscuous'). We must ensure that the sub-signatures are of the same type to obtain the general dichotomy for all kinds of functions. The idea behind this is to glue the sub-signatures together with arity 2 sub-signatures and argue that they don't mix up. Once we have this, we can generalize it to the whole class by a similar argument.

Furthermore, in the Fibonacci signatures, there is a parameter (a, b) which could lead to two different families and hence it is to be proved that this is not the case.

$$ax_k + bx_{k+1} - ax_{k+2} = 0$$

In this case of generalized equality $[a, 0, 0, \ldots, b]$, if $a = 0$, then b is non-zero which in turn sets all the middle elements of the sub-signatures $([t, 0, \ldots, 0])$ as 0. This would imply that they are degenerate (rank < 2) and make them tractable.

2 Holant^c Dichotomy

Earlier, in the previous lectures we dealt with Holant$^*(\mathcal{F})$ which consists of a set of symmetric signatures $\mathcal{F}$ along with a set of unary relations $\mathcal{U}$. Here, instead of considering arbitrary unary signatures, we build on the classification of Holant$^*(\mathcal{F})$ use just two of them $\{[1, 0], [0, 1]\}$ and arrive at the following dichotomy for Holant$^c(\mathcal{F})(=$ Holant$(\mathcal{F} \cup \{[1, 0], [0, 1]\}))$ -

Theorem 1 (Holant^c dichotomy). *Given any set of symmetric signatures $\mathcal{F}$ which contains [0,1] and [1,0], we can construct a non-degenerate symmetric ternary signature $X = [x_0, x_1, x_2, x_3]$, except in the following two trivial cases:*

1. *Any non-degenerate signature in $\mathcal{F}$ is of arity at most 2;*
2. *In $\mathcal{F}$, all unary signatures are of form $[x, 0]$ or $[0, x]$; all binary signatures are of form $[x, 0, y]$ or $[0, x, 0]$; and all signatures of arity greater than 2 are of the form $[x, 0, \ldots, y]$.*

Building upon this are works on real symmetric functions [2] and arity k EQUALITY $(=_k)$, assymetric function [3].

Now, we move on to the paper by Bulatov and Dalmau [1] that proceeds towards a dichotomy for the counting CSP (Constraint Satisfaction Problem).

3 Dichotomy Theorem for Counting CSP

A Constraint Satisfaction Problem (CSP) is as follows: given a set of variables, a set of values that can be taken by the variables, and a set of constraints specifying some restrictions on the values that can be taken simultaneously by some variables, determine the if any assignment of values to variables that satisfy all the constraints. The Counting CSP (#CSP) counts the number of such possible satisfying assignments.

The model considered here is a bipartite graph $G = ((U, V); E)$ where U contains the set of all variables and V contains the constraints from the relation set.

A famous conjecture that gives a dichotomy for the decision version of CSP states that for every constraint set, CSP is either in P or NP-complete. Schaefer provides a dichotomy for a restricted version of CSP with 2 domain variables (0-1). Bulatov extends this result to 3 variables.

3.1 Definitions

Let A be a finite set (domain) and $R \subseteq A^r$ be an r-ary ($r \geq 1$) relation.

Definition 1. *The counting constraint satisfation problem (#CSP) is the combinatorial functional problem with*

INPUT: *a triple $(V; A; \mathcal{C})$ where V is a finite set of variables that take values in a finite domain A, $\mathcal{C}$ is a finite set of constraints. Each constraint $C \in \mathcal{C}$ is a pair (s, ρ) where*

- *$s = (v_1, v_2, \ldots, v_{m_C})$ is a tuple of variables of length m_C, called the constraint scope;*
- *ρ is an m_C-ary relation on A called the contraint relation.*

OBJECTIVE: *compute the number of solutions, i.e. functions f, from V to A such that for each constraint $(s, \rho) \in \mathcal{C}$, the tuple $(f(v_1), f(v_2), \ldots, f(v_m))$ belongs to ρ.*

Example:[#k-SAT] An instance of the #k-SAT problem is specified by giving a propositional logic formula in k-CNF, and asking how many assignments satisfy it. The domain of variable values $A = \{0, 1\}$. Let the variables and clause (constraint) be as follows -

$$(\bar{x}_1 \vee x_2 \vee x_3 \vee x_4 \vee \bar{x}_5)$$

The corresponding set of relations on A that satisfy the above constraint is defined by $\Gamma = \{a | a \in \{0, 1\}^5 - \{(1, 0, 0, 0, 1)\}\}$. The corresponding counting problem is referred by #CSP(Γ). ⊠

Definition 2 (constraint language Γ)**.** #CSP(Γ) *is called tractable if for every finite $\Gamma_0 \subseteq \Gamma$,* #CSP($\Gamma_0$) *is in polynomial time.*
#CSP(Γ) *is #P-Complete if there is a finite set $\Gamma_0 \subseteq \Gamma$ that is #P-Complete.*

Further, we can identify the following equivalence between #CSP and Holant problem:

$$\#\text{CSP}(\Gamma) = \text{Holant}(\Gamma \cup \{=_k |k \geq 1\}$$

3.2 Universal Algebra

A universal algebra is an algebraic system consists of a structure $\mathcal{A} = (A, \Gamma)$ where A is a set and Γ is a set of relations on A. We are going to deal with finite set A in this lecture.

Definition 3 (Polymorphism σ)**.** *A polymorphism σ is defined as $\sigma : A^n \rightarrow A$ is a function of arity n that commutes with every relation $R \in \Gamma$.*

If a column matrix $N = (a_{1,1}, a_{1,2}, \ldots, a_{1,r}), (a_{2,1}, a_{2,2}, \ldots, a_{2,r}), \ldots (a_{n,1}, a_{n,2}, \ldots, a_{n,r}) \in \Gamma$, then the tuple $(\sigma(a_{1,1}, a_{2,1}, \ldots, a_{n,1}), \sigma(a_{1,2}, a_{2,2}, \ldots, a_{n,2}), \ldots, \sigma(a_{1,r}, a_{2,r}, \ldots, a_{n,r})) \in \Gamma$ is a polymorphism and represented by $\sigma_{\rightarrow}(N)$.

Definition 4 (Partial polymorphism f)**.** *A partial polymorphism f is defined as $f : S \subseteq A^n \rightarrow A$ such that whenever rows are in the domain S, then $\forall R \in \Gamma, f_{\rightarrow}(N) \in \Gamma$.*

Definition 5 (Mal'tsev polymorphism σ_M)**.** *A Mal'tsev polymorphism σ_M is defined as $\sigma_M : A^3 \rightarrow A$ such that for all $x, y \in A$, $\sigma_M(x, x, y) = y$ and $\sigma_M(x, y, y) = x$.*

An example over vector spaces is the ternary operation called Mal'tsev operation σ and it is defined as $\sigma(x, y, z) = x - y + z$.

The class of relations in which these Mal'tsev's operations become a polymorphism is a set of all affine linear subspaces V:

$$V \subseteq S \qquad V = \{x | Mx = \alpha\} \quad M(x - y + z) = \alpha$$

In this line of work, Creignou and Hermann [4] arrived at the result that if R is not a set of affine linear subspaces, then #CSP over the boolean domain is #P-Hard. Therefore, the existence of Mal'tsev polymorphism is key to tractability over the boolean domain and we arrive at a dichotomy for the boolean domain. The same was conjectured for a 3-element domain by an earlier work of Bulatov et al. and later proved false.

A few properties to note in #CSP are:

- A permutation of variables is possible i.e. $R'(x, y, z) = R(y, z, x)$.
- Equality constraints can be replaced by using same variables for all elements in the equality.

Now let us get into some formal definitions of universal algebra which will be useful for the next few lectures - polymorphism and invariant.

For a given constraint language Γ, the set of all operations preserving each relation from Γ is denoted by $\mathsf{Pol}\ \Gamma$ (polymorphism). On the other hand, for a given set of functions $\mathcal{F}$, the set of all relations invariant under every function from $\mathcal{F}$ is denoted by $\mathsf{Inv}\ \mathcal{F}$.

By the definitions of Inv and Pol, we have the following relations:

$$\Gamma \xrightarrow{\mathsf{Pol}} \mathcal{F} \xrightarrow{\mathsf{Inv}} \Gamma' \quad \text{and} \quad \mathcal{F} \xrightarrow{\mathsf{Inv}} \Gamma_1 \xrightarrow{\mathsf{Pol}} \mathcal{F}'$$
$$\Gamma \longrightarrow \subseteq \longrightarrow \Gamma' \qquad \mathcal{F} \longrightarrow \subseteq \longrightarrow \mathcal{F}'$$

Definition 6 (Clone $\langle\Gamma\rangle$)**.** *For a constraint language Γ, the clone $\langle\Gamma\rangle$ consists of equality $(=_A)$ and all relations defined by existential quantifiers, conjunctions, extensions and repititions of variables over Γ.*

In the following lectures, we will look into a key theorem for clones ($\langle\Gamma\rangle \equiv \mathsf{Inv}(\mathsf{Pol}\ \Gamma)$) based on similar lines. We will also look into the properties satisfied by Inv and Pol. Before we conclude, we look into the relation between the existence of a Mal'tsev and congruences. Congruences are equivalence relations that are definable (by conjunctions, permutation on variables and existential quantifiers).

Suppose that α, β be two binary equivalence relations (congruences). The composition of the two relations is defined as:

$$\alpha \circ \beta = \{(a, c) | \exists b : (a, b) \in \alpha, (b, c) \in \beta\}$$

The question now is whether the congruences commute. If we are able to show that $\alpha \circ \beta \subseteq \beta \circ \alpha$ and vice-versa, we can show that they commute. This condition is true in the case of Mal'tsev operations.

Let $(a, c) \in \alpha \circ \beta$. Then there exists a b such that $(a, b) \in \alpha$ and $(b, c) \in \beta$ by the definition of $\alpha \circ \beta$. We also note that $(a, a) \in \alpha, \beta$ and $(c, c) \in \alpha, \beta$. Next, we can make use of the equivalence relation from the Mal'tsev polymorphism and arrive at the following conclusion: $(c, a) \in \alpha \circ \beta$ which is equivalent to $(a, c) \in \beta \circ \alpha$. This is illustrated below -

$$\begin{array}{cccc} a & a & c & \longrightarrow c \\ a & b & c & \longrightarrow * \\ a & c & c & \longrightarrow a \\ \in & \in & \in & \in \\ \alpha \circ \beta & \alpha \circ \beta & \alpha \circ \beta & \alpha \circ \beta \end{array}$$

Thus, we prove that the existence of a Mal'tsev polymorphism is sufficient for the congruences to commute.

References

[1] Andrei Bulatov and Victor Dalmau, *Towards a Dichotomy Theorem for the Counting Constraint Satisfaction Problem*, In Proceedings of the 44th IEEE Symposium on Foundations of Computer Science, FOCS'03, pages 562571, Cambridge, MA, USA, October 2003. IEEE Computer Society.

[2] Jin-Yi Cai, Sangxia Huang, and Pinyan Lu, *From Holant to #CSP and Back: Dichotomy for Holant^c Problems*, ISAAC'10. 1:253-265, 2010.

[3] Jin-Yi Cai, Michael Kowalczyk, and Tyson Williams, *Gadgets and Anti-gadgets Leading to a Complexity Dichotomy*, arXiv:1108.3383, To appear at ITCS 2012.

[4] N. Creignou and M. Hermann, *Complexity of generalized satisability counting problems*, Information and Computation, 125(1):1-12, 1996.