CS 880: Complexity of Counting Problems 2/2/2012

Lecture 4: Baby Dichotomy Theorem - Part 2

Instructor: Jin-Yi Cai Scribe: Tyson Williams

In this lecture, we complete are first dichotomy theorem by completing the hardness proof, which is broken into two parts based on the roots of the characteristic polynomial of a second order recurrence relations. After more discussion about the tractable cases, we introduce the framework for our next dichotomy.

1 Recap

Last time we set off to prove our first dichotomy theorem for a restricted case.

Theorem 1 (Theorem 8.3 in [2])**.** *Every counting problem* Holant$([x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3])$*, where* $[x_0, x_1, x_2]$ *and* $[y_0, y_1, y_2, y_3]$ *are Boolean signatures, is either*

- *in* P*,*
- #P*-complete but solvable in* P *for planar graphs, or*
- #P*-complete even for planar graphs.*

There is a reason why we choose Holant$([x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3])$ for the first Holant dichotomy. It is because signatures of arity 3 are the smallest arity that can be #P-hard. If all signatures are at most arity 2, then the connected components in the allowed graphs are just cycles or paths, both of which have simple polynomial time algorithms. Then, putting an arity 2 signature in between all of the arity 3 signatures naturally follows from the fact that want to do holographic transformations.

2 Proving Hardness

2.1 Case 1: Distinct Roots

There are two cases in the hardness proof, and they depend on the roots of the characteristic polynomial of second order recurrence relation defined by the entries of $[y_0, y_1, y_2, y_3]$. If the roots are distinct, then there exists α_1, α_2, β_1, and β_2 such that $y_i = \alpha_1^{3-i}\alpha_2^i + \beta_1^{3-i}\beta_2^i$. Under

a holographic transformation,

$$\begin{aligned}[y_0, y_1, y_2, y_3] &= \begin{bmatrix}\alpha_1 \\ \alpha_2\end{bmatrix}^{\otimes 3} + \begin{bmatrix}\beta_1 \\ \beta_2\end{bmatrix}^{\otimes 3} \\ &= \begin{bmatrix}\alpha_1 & \beta_1 \\ \alpha_2 & \beta_2\end{bmatrix}^{\otimes 3} \left(\begin{bmatrix}1 \\ 0\end{bmatrix}^{\otimes 3} + \begin{bmatrix}0 \\ 1\end{bmatrix}^{\otimes 3} \right) \\ &= \begin{bmatrix}\alpha_1 & \beta_1 \\ \alpha_2 & \beta_2\end{bmatrix}^{\otimes 3} [1, 0, 0, 1]^T,\end{aligned}$$

our arity 3 signature $[y_0, y_1, y_2, y_3]$ is just $[1, 0, 0, 1]$, the equality signature on three bits. With $[1, 0, 0, 1]$ on the right, if we had $[0, 1, 1]$ on the left, this problem would be #P-hard as it is #VertexCover. So, we prove #P-hardness by reducing #VertexCover to our problem. The first step is the holographic transformation from above, which is just a constant time reduction! The action on the left side is

$$[0, 1, 1] \left(\begin{bmatrix}\alpha_1 & \beta_1 \\ \alpha_2 & \beta_2\end{bmatrix}^{-1} \right)^{\otimes 2} = [a_0, a_1, a_2].$$

Now the y_i's are Boolean by assumption, but these a_i's could be complex numbers.

We want to interpolation any $[g_0, g_1, g_2]$ on the left side using an oracle for our problem Holant$([x_0, x_1, x_2] \mid [y_0, y_1, y_2, y_3])$, which by our constant time holographic reduction, is equivalent to an oracle for the problem Holant$([a_0, a_1, a_2] \mid [1, 0, 0, 1])$.

Consider the gadget construction in sections 7 and 8 of [2].[1] Given that we want to interpolate an arity two signature, this is about the simplest thing one can do. This is in stark contrast gadget constructions in the theory of NP-completeness, where the gadgets require some thought.[2]

2.1.1 Holant$([0, 1, 0] \mid [0, 1, 1, 0])$

Here is one example of a problem that we prove is #P-hard. This problem Holant$([0, 1, 0] \mid [0, 1, 1, 0])$ is also a problem in the Ising model from physics known as an "ice" problem. The reason for this is that it models the possible configurations that water molecules can be in when they freeze. The molecules/vertices (of degree 3) have the Not-All-Equal signature. The bonds/edges (of degree 2) also have the Not-All-Equal signature, but it is better thought of as orientation of the edge. Valiant showed [3] that this problem is solvable in polynomial time using holographic algorithms with matchgates. We show that this problem is #P-hard over general (i.e. (2,3)-bipartite but not necessarily planar) graphs.

We have already proved that Holant$([1, 0, 1] \mid [0, 1, 1, 0])$ is hard, so our goal is to interpolate all signatures (on the left) of the form $[a, b, a]$.

[1] A more complete version [1] titled "Holographic Reduction, Interpolation and Hardness" was handed out in class and is also available on the class website. In this version, see Figures 2 and 4.

[2] See section 10 of [1] for more on this point.

Theorem 2 (Theorem 6.1 of [1])**.** Holant($[1,0,1] \mid [0,1,1,0]$) *can be used to interpolate all signatures of the form* $[a,b,a]$.

Proof. The proof uses the gadget is Figure 2 of [1]. In the general case, the entries in the signature of $N_i = [a_i, b_i, c_i]$ can be expressed by the entries in the signature of N_{i-1}. For this problem, the symmetry forces $a_i = c_i$. Thus,

$$\begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \end{bmatrix},$$

and one can verify that this matrix satisfies the three conditions that are sufficient for interpolation to succeed that we previously discussed for 2-by-2 matrixes. □

2.1.2 Holant($[1,1,0] \mid [1,1,1,0]$)

The previous example was #P-hard over general graphs, but not planar graphs. This problem Holant($[1,1,0] \mid [1,1,1,0]$) is #P-hard even over planar graphs. This time, the proof uses Gadget 1 in Figure 3, which gives the recursive relation

$$\begin{bmatrix} a_i \\ b_i \\ c_i \end{bmatrix} = \begin{bmatrix} 7191 & 12618 & 5535 \\ 3816 & 6723 & 2961 \\ 2025 & 3582 & 1584 \end{bmatrix} \begin{bmatrix} a_{i-1} \\ b_{i-1} \\ c_{i-1} \end{bmatrix}.$$

Now we must check that this 3-by-3 matrix satisfies sufficient conditions for interpolation to succeed. Let the matrix that defines the recursive relation be A. Then three conditions are

1. $\det A \neq 0$,
2. $\begin{bmatrix} a_b \\ b_b \\ c_b \end{bmatrix}$ is not orthogonal to any row eigenvector of A, and
3. $\forall (i,j,k) \neq (i',j',k')$ with $i+j+k = 0$, $\alpha^i \beta^j \gamma^k \neq \alpha^{i'} \beta^{j'} \gamma^{k'}$, where α, β, and γ are the eigenvalues of A.

Since $\det A \neq 0$, $\alpha\beta\gamma \neq 0$, so we can divide one side by the other and rewrite condition 3 as $\forall (i,j,z) \in \mathbb{Z}^3 - \{(0,0,0)\}$ with $i+j+k = n$, $\alpha^i \beta^j \gamma^k \neq 1$. This is a lattice condition.

Recall that we defined the $\binom{n+2}{2}$-by-$\binom{n+2}{2}$ matrix $\widetilde{B^{\otimes n}}$. We think of the rows being indexed by an element of $\kappa = \{0^i 1^j 2^k \mid i+j+k = n\}$ and the columns by s where $1 \leq s \leq \binom{n+2}{2}$. The entry at $(0^i 1^j 2^k, s)$ is $(\alpha^i \beta^j \gamma^k)^s$, so it will have full rank is the lattice condition is satisfied.

We were able to find an algorithm that runs in polynomial time in the size of the matrix that defines the recursive gadget relation and determines if the matrix satisfies the lattice condition.

Lemma 1 (Lemma 5.1 in [1]). *Let $f(x) \in \mathbb{Q}[x]$ with roots α, β, and γ. It is decidable in polynomial time whether any non-trivial solutions to $\alpha^i\beta^j\gamma^k = 1$ exists, and if so, find all solutions using a short basis of the lattice.*

However, we decided against using it in our proof. Instead, we came up with a sufficient condition.

Lemma 2 (Lemma 5.1 in [1]). *Let $f(x) \in \mathbb{Q}[x]$ with roots α, β, and γ. If f is irreducible except the form $x^3 + c$ for some $c \in \mathbb{Q}$, there are no non-trivial solutions to $\alpha^i\beta^j\gamma^k = 1$.*

The characteristic polynomial of our gadget construction is $x^3 - 15498x^2 + 419904x - 19683$, and one can check that it is indeed irreducible.

At this point, it seems somewhat ridiculous that we are allowed to use such a large gadget in a #P-hardness reduction. If P $\neq$ #P, then computing the matrix of a recursive gadget construction with e edge truly requires $2^{(e)}$ steps. Since e does not depend on the problem, this is a constant![3]

2.2 Case 2: Double Root

The other case, the characteristic polynomial of second order recurrence relation defined by the entries of $[y_0, y_1, y_2, y_3]$ has a double root. Then there exists $A \neq 0$ and B such that $y_i = Ai\alpha^{i-1} + B\alpha^i$ (if $A = 0$, then the signature is degenerate, which makes the problem easy). In this case, we do a holographic transformation by

$$M = \begin{bmatrix} 1 & \frac{B-1}{3} \\ \alpha & A + \frac{B-1}{3}\alpha \end{bmatrix},$$

which sends $[y_0, y_1, y_2, y_3]$ to $[1, 1, 0, 0]$. Just as in our paper, we state this transformation with discussing the background, except to say that its selection if informed by an underlying signature theory of holographic algorithms.

What if the signature on the left side was $[1, 0, 1]$? What problem is Holant($[1, 0, 1] \mid [1, 1, 0, 0]$)? The arity 2 signature is equality, so we think of the vertices of degree 2 as edges and we are either picking or not picking these edges. On the right, the vertices (of degree 3) demand that at most one of their incident edges should be selected. This problem counts the number of (general) matchings. Since this problem is #P-hard even for planar 3-regular graphs, we can do similar gadget constructions to those above to prove #P-hardness for the problems in this double root case.

3 More on Tractability

In this section, we prepare for our next dichotomy theorem by extending the range of the cases that we already know to be tractable.

[3] See section 10 of [1] for more on this point.

Recall that a symmetric signature $f = [f_0, f_1, \cdots, f_n]$ is Fibonacci if $f_{k+2} = f_{k+1} + f_k$ for $0 \le k \le n-2$. The characteristic polynomial of this recurrence relation is $x^2 - x - 1$ with roots

$$\phi = \frac{1+\sqrt{5}}{2} \qquad \text{and} \qquad \overline{\phi} = \frac{1-\sqrt{5}}{2}.$$

Then we can express f_k as

$$f_k = a \begin{pmatrix} 1 \\ \phi \end{pmatrix}^{\otimes n} + b \begin{pmatrix} 1 \\ \overline{\phi} \end{pmatrix}^{\otimes n}.$$

What do you think we should do next? A holographic transformation of course.

$$\begin{aligned} f_k &= a \begin{pmatrix} 1 \\ \phi \end{pmatrix}^{\otimes n} + b \begin{pmatrix} 1 \\ \overline{\phi} \end{pmatrix}^{\otimes n} \\ &= \begin{bmatrix} 1 & 1 \\ \phi & \overline{\phi} \end{bmatrix}^{\otimes n} \left(a \begin{pmatrix} 1 \\ 0 \end{pmatrix}^{\otimes n} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}^{\otimes n} \right). \end{aligned}$$

We call signatures of the form $[a, 0, \ldots, 0, b]$ generalized equality because they still enforce that all bits should be equal but contribute a factor of a or b (instead of 1) when all bits agree.

Let $\mathscr{F}$ib be the set of signatures that satisfy the Fibonacci recurrence relation. If we do the inverse of M to $\mathscr{F}$, then they are all transformed to generalized equality signatures. On the left, we can assume there is a binary equality signature $[1, 0, 1]$. Transforming $[1, 0, 1]$ by M gives another generalized equality signature! When we first discovered this, we did not stop to understand why this happened. We now know that this is because M has one of the two properties of an orthogonal matrix. Namely, the inner product of the columns is zero. More generally, for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ that is an orthogonal matrix,

$$\begin{aligned} (1,0,0,1) &= \left((1,0)^{\otimes 2} + (0,1)^{\otimes 2} \right) \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ &= (a,b)^{\otimes 2} + (c,d)^{\otimes 2} \\ &= (a^2, ab, ab, b^2) + (c^2, cd, cd, d^2) \\ &= (a^2 + c^2, ab + cd, ab + cd, b^2 + d^2) \\ &= (1,0,0,1). \end{aligned}$$

Notice that this also provides an alternate proof of the tractability of $\mathscr{F}$, since the set of a set of generalized equality signatures is tractable. Of the exponentially many terms in the Holant sum, there are only two that could possibly be nonzero, the all 0's and the 1's. With this understanding, we can get a closed form (in terms of the first two entries of the signatures and four entries in the transformation matrix) for what signatures are realizable by a signature in $\mathscr{F}$ib under a holographic transformation.

Theorem 3. *A symmetric signature $[x_0, x_1, \ldots, x_n]$ is realizable under a holographic transformation from $\mathscr{F}ib$ iff $\exists a, b, c$ such that*

$$b^2 - 4ac \neq 0 \qquad \text{and} \qquad ax_k + bx_{k+1} + c_{k+1} = 0$$

for all $0 \leq k \leq n-2$.

However, the real question is when you have two sets of signatures and want to know if they are simultaneously realizable as signatures in $\mathscr{F}$ib under that same holographic transformation.

Theorem 4 (Theorem 2.4 of [1])**.** *Let $\mathcal{G}$ and $\mathcal{R}$ be sets of symmetric signatures. Then there exists a holographic transformation from* Holant$(\mathcal{G} \mid \mathcal{R})$ *to* Holant$(\mathscr{F}ib)$ *if $\exists a, b, c$ such that $b^2 - 4ac \neq 0$ and the following two conditions are satisfied:*

1. *for any $R_i = [x_0^{(i)}, \cdots, x_{n_i}^{(i)}]$ and $k = 0, 1, \ldots, n_i$, $ax_k^{(i)} + bx_{k+1}^{(i)} + cx_{k+2}^{(i)} = 0$*
2. *for any $G_j = [y_0^{(j)}, \cdots, y_{m_i}^{(j)}]$ and $k = 0, 1, \ldots, m_i$, $ay_\ell^{(j)} - by_{\ell+1}^{(j)} + cy_{\ell+2}^{(j)} = 0$*

If $a = -c = 0$, then the signatures are of the form $[*, 0, \ldots, 0, *]$, which is not in $\mathscr{F}ib$ or generalized $\mathscr{F}$ib (which we define shortly). Otherwise, if $a = -c \neq 0$, then both expressions become the same and we can normalize a to 1 and get $x_{k+2} = mx_{k+1} + x_k$ for any m. We call signatures with this form generalized Fibonacci. Under the assumption $a = -c = 1$, the exceptional case is $b^2 - 4ac = m^2 + 4 = 0$, so $m = \pm 2i$. However, we still have the following theorem.

Theorem 5. *All generalized Fibonacci signatures are tractable (i.e. tractable $\forall m \in \mathbb{C}$).*

Proof. The proof can go in one of two ways. First, you can say that generalized Fibonacci signatures capture everything except when $m = \pm 2i$. This for this exceptional case, there exists an algorithm (that we have not discussed) that can handle these two special points.

Alternatively, you can say that everything is either covered by generalized Fibonacci signatures or generalized equality signatures. □

4 Next Dichotomy

Our next dichotomy will be for Holant$^*(\mathcal{F})$ with any set of symmetric signatures $\mathcal{F}$. The star denotes the fact that in addition to the signatures in $\mathcal{F}$, inputs are also allowed to use any $[a, b]$ from the set of unary functions $\mathcal{U}$. Thus, Holant$^*(\mathcal{F})$ = Holant$(\mathcal{F} \cup \mathcal{U})$. Allowing inputs to use functions not explicitly allowed is actually quite natural, since this is precisely what happens in $\#\,\mathrm{CSP}(\mathcal{F})$.

In the CSP framework, there is a bipartite graph with constraints on vertices in one partite set and assignments to the vertices in the other partite set (with edges connecting a constraint vertex to a variable vertex if the constraint using the variable). From the perspective of the Holant framework, the assignments are the edges, so it is as if the variables vertices have

equality functions (with arity equal to their degree). Let $\mathrm{EQ} = \{=_k | \ k > 0\}$ be the set of equality functions. Then

$$\mathrm{Holant}(\mathrm{EQ} \cup \mathcal{F}) = \#\,\mathrm{CSP}(\mathcal{F}) = \mathrm{Holant}(\mathrm{EQ} \mid \mathcal{F}).$$

References

[1] Jin-Yi Cai, Pinyan Lu, and Mingji Xia. Holographic reduction, interpolation and hardness.

[2] Jin-Yi Cai, Pinyan Lu, and Mingji Xia. Holographic algorithms by fibonacci gates and holographic reductions for hardness. In *FOCS*, pages 644–653. IEEE Computer Society, 2008.

[3] Leslie G. Valiant. Holographic algorithms. *SIAM J. Comput.*, 37(5):1565–1594, 2008.