Lecture 3: VNP-completeness of $\{\mathsf{Per}_n\}_{n\in\mathbb{N}}$

Instructor: Rafael Oliveira *Scribe: Avantika Agarwal*

Remark These notes have not been subjected to the scrutiny of a journal publication, and it may contain errors. If you find one, please contact the instructor.

1 Introduction

In this lecture, we will prove that $\{\mathsf{Per}_n\}_{n\in\mathbb{N}}$ is VNP-complete. In order to do so, we will show that $\{\mathsf{Per}_n\}_{n\in\mathbb{N}} \in \mathsf{VNP}$ and every polynomial in VNP can be written as the projection of the permanent of some polynomial sized matrix. Before we do that, we state two facts (without proof) which will be used later in the lecture.

Proposition 1 (Homework 1)**.** *Any algebraic formula Ψ of size s can be computed by an algebraic branching program Φ of size $O(s)$.*

Theorem 2 ([Val80])**.** $\mathsf{VNP} = \mathsf{VNP}_e$

We start by showing that $\{\mathsf{Per}_n\}_{n\in\mathbb{N}} \in \mathsf{VNP}$.

Lemma 3. $\{\mathsf{Per}_n\}_{n\in\mathbb{N}} \in \mathsf{VNP}$

Let us begin with an example which illustrates what we will try to do in the proof. Suppose we want to compute the permanent of a 2x2 matrix X. If we index the columns using variables y_1 and y_2, then each term in the resulting permanent polynomial will have a factor of y_1y_2 in it (because every term in the permanent polynomial will have exactly one variable in it from each column).

$$XY = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \cdot \begin{bmatrix} y_1 & 0 \\ 0 & y_2 \end{bmatrix} = \begin{bmatrix} x_{11}y_1 & x_{12}y_2 \\ x_{21}y_1 & x_{22}y_2 \end{bmatrix}$$

$$\mathsf{Per}(XY) = x_{11}y_1x_{22}y_2 + x_{21}y_1x_{12}y_2 = (x_{11}x_{22} + x_{21}x_{12})y_1y_2$$

Now if we define $g(X, y_1, y_2) = (x_{11}y_1 + x_{12}y_2)(x_{21}y_1 + x_{22}y_2) = y_1^2x_{11}x_{21} + y_2^2x_{12}x_{22} + y_1y_2\mathsf{Per}(X)$, and we can use this to find $\mathsf{Per}(X)$ as follows:

$$\begin{aligned} g(X,1,0) &= x_{11}x_{21} \\ g(X,0,1) &= x_{12}x_{22} \\ g(X,1,1) &= x_{11}x_{21} + x_{12}x_{22} + \mathsf{Per}(X) \\ \mathsf{Per}(X) &= g(X,1,1) - g(X,0,1) - g(X,1,0) \end{aligned}$$

Let us now generalize this discussion to an arbitrary $n \times n$ matrix X.

Proof. This proof shows the more general statement that if a polynomial p appears as a coefficient in a bigger polynomial g that is easy to compute, then the said polynomial p is in VNP. We start by defining this bigger polynomial g when p is the Per_n polynomial.

$$\begin{aligned} g_n(X, y_1, \dots, y_n) &= \prod_{i=1}^{n} \Big(\sum_{j=1}^{n} x_{ij}y_j\Big) \\ &= y_1y_2\dots y_n\mathsf{Per}_n(X) + \sum_{\substack{e\in\mathbb{N}^n \\ \|e\|_1=n}} h_e(X)\prod_{i=1}^{n} y_i^{e_i} \end{aligned}$$

where $h_e(X)$ is some polynomial in X, dependent on the vector e. Note now that since we only want to set values $y_i \in \{0,1\}$, we can replace y_i^2 by y_i everywhere, and the evaluation of the polynomial will be the same. So for now we will work with the multilinear polynomial $\tilde{g}_n$ defined below:

$$\tilde{g}_n(X, b_1, \ldots, b_n) = b_1 b_2 \ldots b_n \mathsf{Per}_n(X) + \sum_{S \subset [n]} h_S(X) b_S$$

where $b_i \in \{0,1\}$, $b_S = \prod_{i \in S} b_i$ and $h_S(X)$ is the sum of $h_e(X)$ for all exponent vectors e such that the corresponding monomial of y in g_n was replaced by b_S in $\tilde{g}_n$. Now we want to compute the coefficient of $b_1 b_2 \ldots b_n$ in $\tilde{g}_n$. If we set some value of $b \in \{0,1\}^n$ and look at the set $T \subseteq [n]$ corresponding to the indicator vector b, then all terms in $\tilde{g}_n$ except subsets of T will evaluate to 0. So using the principle of inclusion-exclusion

$$\begin{aligned}
\mathsf{Per}(X) &= \sum_{S \subseteq [n]} (-1)^{n-|S|} \tilde{g}_n(X, 1_S) \\
&= \sum_{S \subseteq [n]} \tilde{g}_n(X, 1_S) \prod_{j \notin S} (b_j - 1) \\
&= \sum_{S \subseteq [n]} \tilde{g}_n(X, 1_S) \prod_{j=1}^{n} (2b_j - 1)
\end{aligned}$$

Now we can replace the polynomial $\tilde{g}_n$ above with our original polynomial g_n, to get the polynomial $\hat{g}_n \in \mathsf{VP}$.

$$\hat{g}_n(X, y_1, y_2, \ldots, y_n) = \left(\prod_{i=1}^{n} (2y_i - 1)\right) \cdot \left(\prod_{i=1}^{n} \left(\sum_{i=1}^{n} x_{ij} y_j\right)\right)$$

Clearly, $\hat{g}_n \in \mathsf{VP}$. From the discussion previously, it now follows that

$$\mathsf{Per}_n(X) = \sum_{b \in \{0,1\}^n} \hat{g}_n(X, b)$$

Therefore, $\mathsf{Per}_n \in \mathsf{VNP}$. $\square$

We now show that $\{\mathsf{Per}_n\}_{n \in \mathbb{N}}$ is complete for VNP_e, and then from Theorem 2 we can conclude that $\{\mathsf{Per}_n\}_{n \in \mathbb{N}}$ is complete for VNP.

Note: For the rest of this document, we follow the given convention for any algebraic branching program diagrams:

1. Arrows or nodes in black represent the original ABP computing a given polynomial.
2. Edges in any ABP without any label have weight 1.
3. Arrows or nodes in blue represent modifications to the ABP in order to get a permanent polynomial.
4. Labels in green are vertex labels to be used in the proof for notational convenience.

Lemma 4. *$\{\mathsf{Per}_n\}_{n \in \mathbb{N}}$ is complete for VNP_e.*

Proof. We show that any polynomial $\{f_n\}_n \in \mathsf{VNP}_e$ is a projection of the permanent of a polynomial-sized matrix. Since $\{f_n\}_n \in \mathsf{VNP}_e$, there exists $\{g_n\}_n \in \mathsf{VP}_e$ such that $f_n(x_1, \ldots, x_n) = \sum_{b \in \{0,1\}^{r(n)}} g_n(x, b)$ and g_n is computable by a polynomial-sized formula Ψ_n. Using Proposition 1, let Φ_n be the ABP of size $s(n)$ computing g_n, where $s(n)$ is a polynomial in n. Then we will construct a matrix Y of size $O(s(n)) \times O(s(n))$ such that $\mathsf{Per}(Y) = \sum_{b \in \{0,1\}^{r(n)}} g_n(x, b) = f_n$. The proof is illustrated through two examples. Consider the polynomial $g = x_1 y + x_2^2$. Then $g(x, 0) + g(x, 1) = x_1 + 2x_2^2$. Let us look at the ABP computing g,

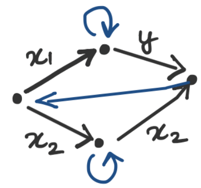

Figure 1: Permanent polynomial for g

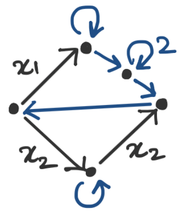

Figure 2: Permanent polynomial for $g(x, 0) + g(x, 1)$

augmented to get the corresponding permanent, in Figure 1. In order to compute $g(x, 0) + g(x, 1)$, we want that cycles containing the y edge have weight 1, while cycles not containing the y edge have weight 2. It is easy to modify the ABP in Figure 1 to achieve that, as shown in Figure 2. However, this technique does not work more generally, when the variable y appears more than once in the ABP.
Let us see an example of a polynomial where the above fix will not work. Let $g = x_1y^3 + x_2^2y^2 + x_3^3y + x_4^4$. Then $g(x, 0) + g(x, 1) = x_1 + x_2^2 + x_3^3 + 2x_4^4$. Once again we look at the ABP computing h, augmented to get the corresponding permanent.

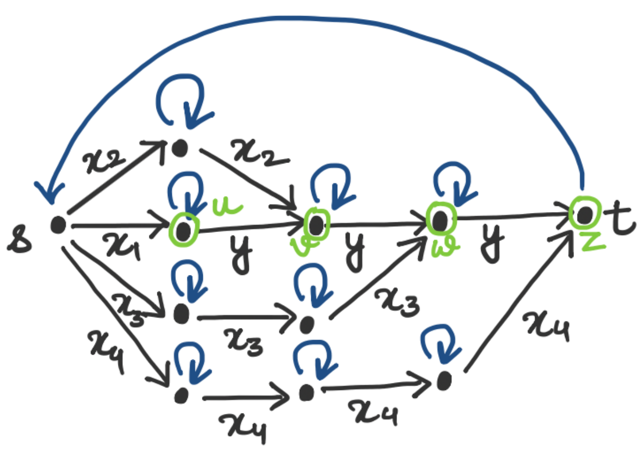

Figure 3: Permanent polynomial for g

If suppose now each y edge in Figure 3 is replaced by a modification similar to Figure 2. Then the $s-t$ path containing only the x_4 edges gets weight 8 (a factor of 2 for each y edge not included in the path). The $s-t$ path containing the x_3 edges followed by the (w, z) edge gets weight 4. The $s-t$ path containing the x_2 edges followed by $(v, w), (w, z)$ edges gets weight 2 and the $s-t$ path containing all y edges gets weight 1. Thus such a modification computes the polynomial $x_1 + 2x_2^2 + 4x_3^3 + 8x_4^4$, which is not what we wanted to compute. This happens because there are different weights associated to paths containing different number

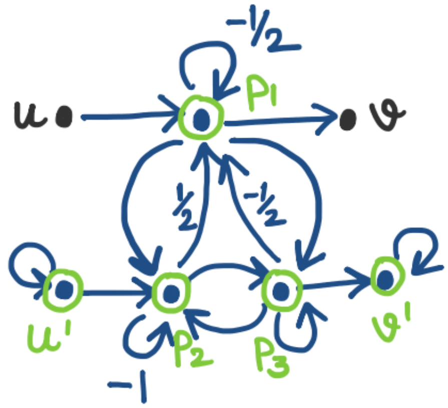

Figure 4: Glue gadget

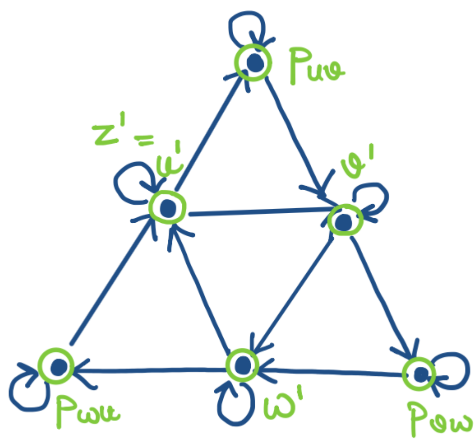

Figure 5: Rosette gadget

of y edges. We instead want the following two properties from a suitable modification of Figure 3:

1. Let E_y be the set of y edges in Φ_n (ABP computing g). For any non-empty subset $S \subseteq E_y$, there is exactly one cycle cover containing S (thus giving weight 1 to terms in g containing E_y).

2. There are exactly two cycle covers that do not include any edge in E_y, for each such $s - t$ path which does not include any edge in E_y (thus giving weight 2 to terms in g without a y factor).

This is achieved using two gadgets: Rosette gadget and glue gadget. The Rosette gadget has one edge for each y-edge in the ABP, along with some additional edges and nodes, and it satisfies the two properties mentioned above. The glue gadget acts to *glue* the y-edges in the ABP to the corresponding edges in the Rosette gadget, thus ensuring that the above two properties are satisfied for the augmented ABP. So if g contains variables $y_1, \ldots, y_k$ (that we sum over), in addition to the x variables, then in the augmented ABP, there will be one Rosette gadget for each y_i-variable, and there will be one glue gadget for each each y_i-edge. Below we show the glue gadget in Figure 4 and the Rosette gadget for 3 y-edges in Figure 5.
Note here that the Rosette gadget has been simplified to not show the nodes p_2, p_3 included in the glue gadget. We will first prove that the glue gadget ensures that only cycle covers which pick both the edges (u, v) and (u', v') (or neither of them) make a non-zero contribution to the permanent polynomial.

- Case 1: Pick both (u, v) and (u', v')
  Then the cycle covers will look something like $\ldots(\ldots, u, p_1, v, \ldots)(\ldots u', p_2, p_3, v', \ldots)\ldots$, which has weight 1.

- Case 2: Pick neither (u, v) nor (u', v')
  Then the nodes p_1, p_2, p_3 will be in a cycle by themselves and the cycle covers will look something like $\ldots(u)(v)(u')(v')(\text{cycle of } p_1, p_2, p_3)\ldots$. The total contribution for all cycles of p_1, p_2, p_3 is given by the permanent of the corresponding adjacency matrix:

$$A = \begin{bmatrix} -1/2 & 1 & 1 \\ 1/2 & -1 & 1 \\ -1/2 & 1 & 1 \end{bmatrix}$$
$$\mathsf{Per}(A) = 1$$

  Since the weights of all self-edges are 1, the total contribution of this case is also 1.

- Case 3: Pick (u, v) but not (u', v')
  Then the nodes p_2, p_3 will be in a cycle by themselves (otherwise we will have to pick $u' \to p_2 \to p_3 \to v'$). The cycle covers will look something like $\ldots(u')(v')(\ldots, u, p_1, v, \ldots)(\text{cycle of } p_2, p_3)\ldots$. But the cycles formed by p_2 and p_3 are $(p_2)(p_3)$ (which has weight -1) and (p_2, p_3) (which has weight 1). Hence the total contribution of such cycle covers is 0.

- Case 4: Pick (u', v') but not (u, v)
  Then the cycle covers will look something like $\ldots(\ldots, u', p_2, p_1, p_3, v', \ldots)\ldots$ (which has weight 1/2) or $\ldots(\ldots, u', p_2, p_3, v', \ldots)(p_1)\ldots$ (which has weight -1/2). Hence the total contribution of such cycle covers is 0.

From the above analysis we can conclude that the glue gadget ensures that for any y-edge (u, v) in the ABP, either both (u, v) and (u', v') are included in the relevant cycle covers of the augmented ABP, or neither is included. This edge (u', v') is also part of the Rosette gadget in Figure 5. So we will now prove that the Rosette gadget satisfies the two properties we need. We only argue the case for 3 edges here, but this proof can be generalized for a Rosette gadget containing an arbitrary number of y-edges.

- Case 1: None of the y-edges are included
  Then we want from property 2, that the Rosette gadget has exactly two cycle covers, each of weight 1. These two cycle covers are $(u', p_{uv}, v', p_{vw}, w', p_{wu})$ and $(u')(p_{uv})(v')(p_{vw})(w')(p_{wu})$. Any other cycle cover will need to include at least one of the edges from $(u', v'), (v', w'), (w', u')$, which is not allowed. Hence the gadget satisfies Property 2.

- Case 2: Only one of the y-edges is included
  We assume without loss of generality that the included edge is $(u'v')$. Then the only cycle cover possible is $(u', v', p_{vw}, w', p_{wu})(p_{uv})$, which has weight 1.

- Case 3: Only two of the y-edges are included
  We assume without loss of generality that the included edges are (u', v') and (v', w'). Then the only cycle cover possible is $(u', v', w', p_{wu})(p_{uv})(p_{vw})$, which has weight 1.

- Case 4: All three y-edges are included
  Then the only cycle cover possible is $(u', v', w')(p_{uv})(p_{vw})(p_{wu})$, which has weight 1.

Hence the Rosette gadget for 3 edges satisfies the properties we want. For the general construction of the Rosette gadget, the cycle covers are constructed similarly: for each edge (u', v') that is included, the node p_{uv} will be in a cycle of its own, and all the other nodes are included in the cycle containing the included edges (u', v').

We can now finish the proof by showing that the augmented ABP (which has the Rosette gadget and one glue gadget for each y-edge) satisfies Properties 1 and 2. Let S be a non-empty subset of y-edges in Φ_n. Then in any cycle cover containing the edges in S, the corresponding edges in the Rosette gadget must also be included (because of the glue gadget), and therefore there can only be one cycle cover containing these edges (because Rosette gadget satisfies Property 1). Thus the augmented ABP satisfies Property 1. Now let there be some $s - t$ path which does not include any y-edge, then none of the edges in the Rosette corresponding to y-edges will be included in the cycle cover (because of the glue gadget), and therefore there will be two cycle covers which do not include any y-edge (because Rosette gadget satisfies Property 2). As mentioned previously, in the more general case when g is a polynomial in $x, y_1, \ldots y_k$, there is one Rosette gadget for each variable y_i, and there is one glue gadget for each y_i edge in the ABP, for every i. Note that we only add a constant number of nodes and edges in the ABP, for each y-edge, hence the size of the augmented ABP is $cs(n)$ for a small constant c (say 10). Since the cycle covers of this augmented ABP give a permanent polynomial, we can conclude that Per is VNP-complete. $\square$

References

[Val80] L.G. Valiant. *Reducibility by Algebraic Projections.* Internal report. University of Edinburgh, Department of Computer Science, 1980.