Algebraic Complexity Theory

Lecture 4: VP, VBP and VF completeness; Class VNP, VNP-completeness

Department of Computer Science,
Indian Institute of Science

Recap

- In the last lecture, we defined the complexity classes VP, VBP and VF, and observed that VF $\subseteq$ VBP $\subseteq$ VP.

- We saw that the polynomial families Det, IMM and ESym are in VBP. Also, SP and PSym are in VF, and ESym too (over sufficiently large fields).

Recap

- In the last lecture, we defined the complexity classes VP, VBP and VF, and observed that VF $\subseteq$ VBP $\subseteq$ VP.

- We saw that the polynomial families Det, IMM and ESym are in VBP. Also, SP and PSym are in VF, and ESym too (over sufficiently large fields).

- In today's lecture, we'll introduce an algebraic notion of reduction and use it to define "complete" families of polynomials for the abovementioned classes. We'll also define the class VNP – the algebraic analog of NP.

Reductions and Completeness

Few words on reductions

- As to how we define a reduction from one polynomial family to another is guided by a *question on whether two algebraic complexity classes are different or identical.*

- The relevant questions in this context are whether or not VF equals VBP and VBP equals VP.

- Reductions help us define *complete families* (i.e., the 'hardest' families in a class) which in turn help us compare the complexity classes under consideration.

Projections and affine projections

- Definition. A polynomial $f(x_1,\ldots, x_n)$ is a *projection* of another polynomial $g(y_1,\ldots, y_m)$ if $f = g(z_1,\ldots, z_m)$, where every $z_i \in \{x_1,\ldots, x_n\} \cup \mathbb{F}$. f is an *affine projection* of g if $f = g(A\mathbf{x} + \mathbf{b})$, where $A \in \mathbb{F}^{m \times n}$, $\mathbf{b} \in \mathbb{F}^m$ & $\mathbf{x} = \{x_1,\ldots, x_n\}$.

- Projections are special kind of affine projections.

- E.g., $x_1^2 - x_2^2 - 1$ is a projection of $y_1^2 - y_2^2 + y_3^3$, whereas $4x_1x_2$ is an affine projection of $y_1^2 - y_2^2 + y_3^3$.

p-projections and complete families

- The reduction that is typically studied in algebraic complexity is given by *p-projections*.

- Definition. A polynomial family $\{f_n\}_{n\geq 1}$ is a *p-projection* of another family $\{g_m\}_{m\geq 1}$ if there's a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that f_n is a projection of $g_{p(n)}$.

- Obs. Let $\mathcal{C}$ be the class VP or VBP or VF. If a family $\mathcal{F}$ is a p-projection of another family $\mathcal{G} \in \mathcal{C}$, then $\mathcal{F} \in \mathcal{C}$.

p-projections and complete families

- The reduction that is typically studied in algebraic complexity is given by *p-projections*.

- Definition. A polynomial family $\{f_n\}_{n\geq 1}$ is a *p-projection* of another family $\{g_m\}_{m\geq 1}$ if there's a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that f_n is a projection of $g_{p(n)}$.

- Definition. Let $\mathcal{C}$ be the class VP or VBP or VF. A family $\mathcal{G}$ is *$\mathcal{C}$–complete* if $\mathcal{G} \in \mathcal{C}$ and every $\mathcal{F} \in \mathcal{C}$ is a p-projection of $\mathcal{G}$.

VBP-complete families

- Obs. IMM is VBP-complete.
- *Proof.* Easy exercise.

VBP-complete families

- Obs. IMM is VBP-complete.
- *Proof.* Easy exercise.
- Theorem. Det is VBP-complete.
- *Proof sketch.* We've already seen that Det is in VBP. It is sufficient to prove the following claim.
- Claim. *(Valiant '79)* IMM is a p-projection of Det.

VBP-complete families

- Obs. IMM is VBP-complete.
- *Proof.* Easy exercise.
- Theorem. Det is VBP-complete.
- *Proof sketch.* We've already seen that Det is in VBP. It is sufficient to prove the following claim.
- Claim. *(Valiant '79)* IMM is a p-projection of Det.
- *Proof sketch.* The underlying weighted DAG of $IMM_{w,d}$ has $w(d-1)+2$ nodes with source s and sink t. Modify this graph as follows: Put a self-loop on every node other than s and t and give it weight 1.

VBP-complete families

- Obs. IMM is VBP-complete.
- *Proof.* Easy exercise.
- Theorem. Det is VBP-complete.
- *Proof sketch.* We've already seen that Det is in VBP. It is sufficient to prove the following claim.
- Claim. *(Valiant '79)* IMM is a p-projection of Det.
- *Proof sketch.* The underlying weighted DAG of $IMM_{w,d}$ has $w(d-1)+2$ nodes with source s and sink t. Modify this graph as follows: Add an edge from t to s and give it weight 1 if d is even, else give weight -1.

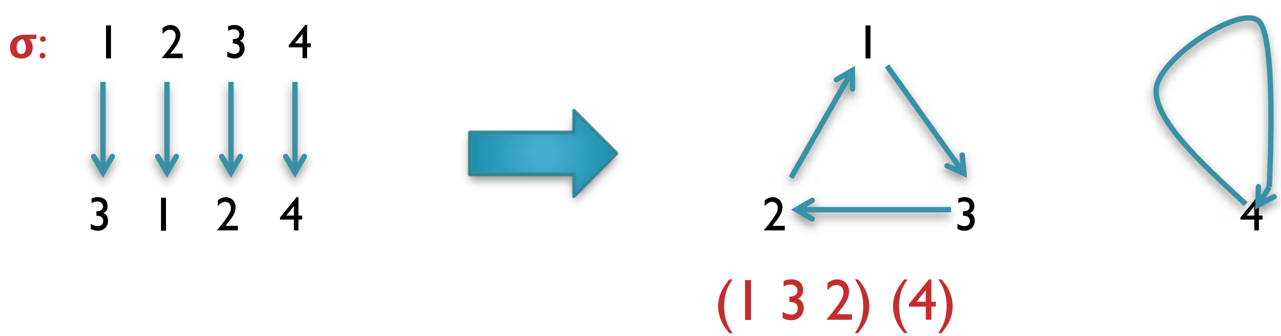
VBP-complete families

- Obs. IMM is VBP-complete.
- *Proof.* Easy exercise.
- Theorem. Det is VBP-complete.
- *Proof sketch.* We've already seen that Det is in VBP. It is sufficient to prove the following claim.
- Claim. *(Valiant '79)* IMM is a p-projection of Det.
- *Proof sketch.* Let A be the adjacency matrix of the resulting weighted graph G. Obs. IMM = det(A). *Why?*
- The answer lies in the graph theoretic interpretation of the determinant.

Graph theoretic interpretation of Det

- Let $A = (a_{ij})_{i,j\in[r]}$. Then, $\det(A) = \sum_{\sigma\in S_r} \mathrm{sign}(\boldsymbol{\sigma}) \prod_{i\in[r]} a_{i\,\sigma(i)}$.

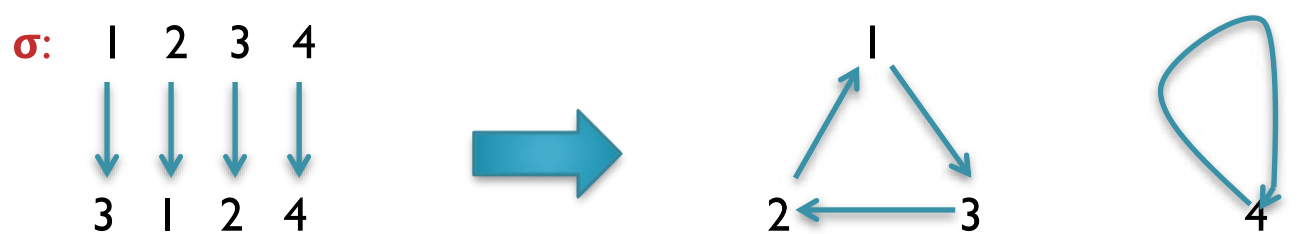
- Let G be the weighted digraph on r vertices with adjacency matrix A, i.e., the edge (i, j) in G has weight a_{ij}.
- Every permutation $\boldsymbol{\sigma}$: $[r] \rightarrow [r]$ can be expressed (uniquely) as a product of disjoint cycles.



Graph theoretic interpretation of Det

- Let $A = (a_{ij})_{i,j \in [r]}$. Then, $\det(A) = \sum_{\sigma \in S_r} \text{sign}(\boldsymbol{\sigma}) \prod_{i \in [r]} a_{i\,\sigma(i)}$.

- Let G be the weighted digraph on r vertices with adjacency matrix A, i.e., the edge (i, j) in G has weight a_{ij}.
- Let b be *number of transpositions* (swaps) that define $\boldsymbol{\sigma}$. Then $\text{sign}(\boldsymbol{\sigma}) := (-1)^b$. The $\boldsymbol{\sigma}$ below has sign 1 as it is defined by an even no. of transpositions.



(1 3 2) (4) = (2 3)(1 3)(4)

Graph theoretic interpretation of Det

- Definition. A *cycle cover* of a digraph G is a subgraph of G having in-degree and out-degree of every vertex exactly 1, i.e., the subgraph is a disjoint union of cycles covering all the vertices of G.

- *Weight* of a cycle cover C, denoted wt(C), is defined as the product of the weights of the edges in C.

Graph theoretic interpretation of Det

- Definition. A <u>*cycle cover*</u> of a digraph G is a subgraph of G having in-degree and out-degree of every vertex exactly 1, i.e., the subgraph is a disjoint union of cycles covering all the vertices of G.

- <u>*Weight*</u> of a cycle cover C, denoted wt(C), is defined as the <u>product</u> of the weights of the edges in C.

- Obs. $$\det(A) = \sum_{\substack{C:\ C \text{ is cycle} \\ \text{cover of } G}} \mathrm{sign}(\sigma_C) \cdot \mathrm{wt}(C)\ .$$

Every "contributing" permutation σ_C corresponds to a cycle cover C and vice versa.

VBP-complete families

- Obs. IMM is VBP-complete.
- *Proof.* Easy exercise.
- Theorem. Det is VBP-complete.
- *Proof sketch.* We've already seen that Det is in VBP. It is sufficient to prove the following claim.
- Claim. *(Valiant '79)* IMM is a p-projection of Det.
- *Proof sketch.* Let A be the adjacency matrix of the resulting weighted graph G. Obs. IMM = det(A). *Why?*
- As det(A) is the signed sum of the weights of the cycle covers of G. Every cycle cover consists of a cycle from s to t to s and a collection of self-loops. ∎

VBP-complete families

- Obs. IMM is VBP-complete.
- *Proof.* Easy exercise.
- Theorem. Det is VBP-complete.
- *Proof sketch.* We've already seen that Det is in VBP. It is sufficient to prove the following claim.
- Claim. *(Valiant '79)* IMM is a p-projection of Det.
- Claim. *(Valiant '79)* If f is computable by a layered ABP of size s then f is an affine projection of $\text{Det}_{O(s)}$.
- *Proof.* Same idea. (*homework*) ∎

VBP-complete families

- Obs. IMM is VBP-complete.
- Theorem. Det is VBP-complete.
- Corollary. If IMM or Det is in VF then VBP = VF.

A VF-complete family

- Let $\mathsf{IMM}_3 := \{\mathsf{IMM}_{3,d}\}_{d\geq 1}$.
- Theorem. *(Ben-Or & Cleve '88)* IMM_3 is VF-complete.
- *Proof.* We start with the following observation:

- Obs. If f is computable by a *constant width* ABP of size s, then it is also computable by a formula of size $s^{O(1)}$.
- *Proof.* Use divide & conquer on the length of the ABP. (*Homework*) ∎

- So, IMM_3 is in VF.

A VF-complete family

- Let $IMM_3 := \{IMM_{3,d}\}_{d \geq 1}$.
- Theorem. *(Ben-Or & Cleve '88)* IMM_3 is VF-complete.
- *Proof.* We also need a depth reduction result:

- Theorem. *(Brent '74)* If f is computable by a formula of size s, then it is also computable by a formula of size $s^{O(1)}$ and depth $O(\log s)$.
- *Proof.* We'll prove it when we discuss depth reduction.

A VF-complete family

- Let $IMM_3 := \{IMM_{3,d}\}_{d \geq 1}$.
- Theorem. *(Ben-Or & Cleve '88)* IMM_3 is VF-complete.
- *Proof.* Let f be computable by a formula of size s and depth $d = O(\log s)$. Then, f is also computable by a width-3 ABP of length at most $4^d = s^{O(1)}$. Use the following relations to prove this:

A VF-complete family

- Let $IMM_3 := \{IMM_{3,d}\}_{d \geq 1}$.
- Theorem. *(Ben-Or & Cleve '88)* IMM_3 is VF-complete.
- *Proof.* Let f be computable by a formula of size s and depth $d = O(\log s)$. Then, f is also computable by a width-3 ABP of length at most $4^d = s^{O(1)}$. Use the following relations to prove this:

$$\begin{bmatrix} 1 & & \\ & 1 & \\ f_1 & & 1 \end{bmatrix} \begin{bmatrix} 1 & & \\ & 1 & \\ f_2 & & 1 \end{bmatrix} = \begin{bmatrix} 1 & & \\ & 1 & \\ f_1+f_2 & & 1 \end{bmatrix}$$

A VF-complete family

- Let $IMM_3 := \{IMM_{3,d}\}_{d\geq 1}$.
- Theorem. *(Ben-Or & Cleve '88)* IMM_3 is VF-complete.
- *Proof.* Let f be computable by a formula of size s and depth $d = O(\log s)$. Then, f is also computable by a width-3 ABP of length at most $4^d = s^{O(1)}$. Use the following relations to prove this:

$$\begin{bmatrix} 1 & & \\ -f_2 & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & & \\ & 1 & \\ & f_1 & 1 \end{bmatrix} \begin{bmatrix} 1 & & \\ f_2 & 1 & \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & & \\ & 1 & \\ & -f_1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & & \\ & 1 & \\ f_1 f_2 & & 1 \end{bmatrix}$$

Power of IMM_2

- Theorem. *(Allender & Wang '11)* The polynomial $x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$ cannot be computed by affine projections of $IMM_{2,d}$ for *any* d over *any* $\mathbb{F}$.

- Theorem. *(S., Saptharishi, Saxena '09)* If f is computable by a depth-3 circuit of size s, then $L \cdot f$ is computable by affine projections of $IMM_{2,poly(s)}$, where L is a product of *non-zero affine forms*.

Power of IMM_2

- Theorem. *(Allender & Wang '11)* The polynomial $x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$ cannot be computed by affine projections of $IMM_{2,d}$ for *any* d over *any* $\mathbb{F}$.

- Theorem. *(S., Saptharishi, Saxena '09)* If f is computable by a depth-3 circuit of size s, then $L \cdot f$ is computable by affine projections of $IMM_{2,poly(s)}$, where L is a product of *non-zero affine forms*.
- Corollary. PIT (or the *hitting-set problem*) for affine projections of IMM_2 is at least as hard as PIT (or the hitting-set problem) for depth-3 circuits.

Power of IMM_2

- Theorem. *(Allender & Wang '11)* The polynomial $x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8$ cannot be computed by affine projections of $IMM_{2,d}$ for *any* d over *any* $\mathbb{F}$.

- Theorem. *(S., Saptharishi, Saxena '09)* If f is computable by a depth-3 circuit of size s, then $L \cdot f$ is computable by affine projections of $IMM_{2,poly(s)}$, where L is a product of *non-zero affine forms*.
- Theorem. *(Bringmann, Ikenmeyer, Zuiddam '18)* *Orbit closure* of IMM_2 capture orbit closure of formulas.

A VP-complete family

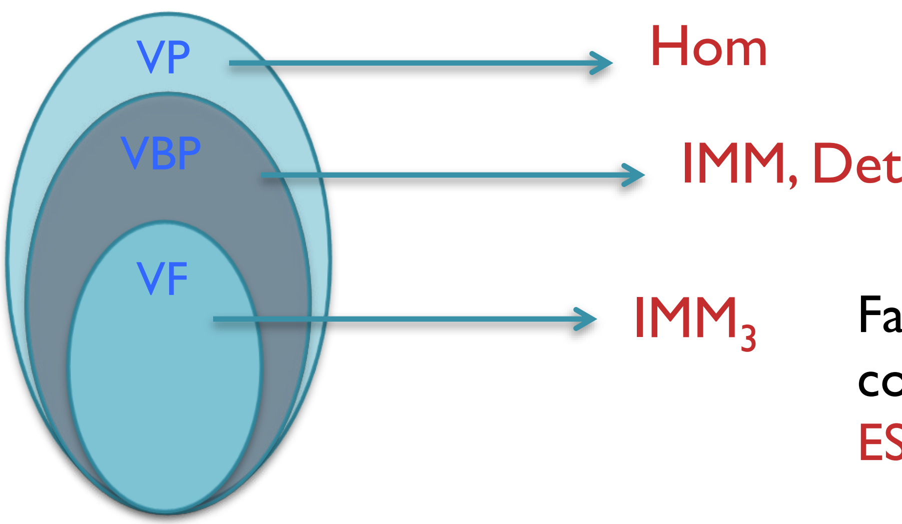
- For a long time no “natural” VP-complete family of polynomials were known.

- Theorem. *(Mahajan & Saurabh ’17; Durand, Mahajan, Malod, Rugy-Altherre, Saurabh’14)* A certain family of graph *homomorphism polynomials* Hom is VP-complete.

A VP-complete family

- For a long time no “natural” VP-complete family of polynomials were known.

- Theorem. *(Mahajan & Saurabh ’17; Durand, Mahajan, Malod, Rugy-Altherre, Saurabh’14)* A certain family of graph *homomorphism polynomials* Hom is VP-complete.



Families in VF that are not VF-complete are SP, PSym, and ESym (over char 0 fields)

Class VNP and VNP-completeness

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- It follows from the definition of class VP that the number of variables and the degree of f_n is polynomially bounded in n.

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function p: $\mathbb{N} \rightarrow \mathbb{N}$ such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- Valiant called such a family $\mathcal{F}$ *p-definable*.

- Clearly, VP $\subseteq$ VNP.

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- Recall that a language L is in NP/poly if there's a polynomial size circuit family $\{C_m\}_{m\geq 1}$ and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$\mathbf{x} \in L \iff \bigvee_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} C_{p(|\mathbf{x}|)}(\mathbf{x},\mathbf{y}) = 1.$$

- W.l.o.g we can assume that C_m is a 3CNF.

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|y|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- Recall that a language L is in NP/poly if there's a polynomial size circuit family $\{C_m\}_{m\geq 1}$ and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$\mathbf{x} \in L \iff \bigvee_{\mathbf{y}\in\{0,1\}^{|y|}} C_{p(|\mathbf{x}|)}(\mathbf{x}, \mathbf{y}) = 1.$$

- VNP may be regarded as the algebraic analog of NP/poly.

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function p: $\mathbb{N} \to \mathbb{N}$ such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- A function f: $\{0,1\}^* \to \mathbb{N}$ is in #P/poly if there's a polynomial size circuit family $\{C_m\}_{m\geq 1}$ and a polynomial function p: $\mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$f(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} C_{p(|\mathbf{x}|)}(\mathbf{x}, \mathbf{y}).$$

- W.l.o.g we can assume that C_m is a 3CNF.

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- A function $f: \{0,1\}^* \to \mathbb{N}$ is in #P/poly if there's a polynomial size circuit family $\{C_m\}_{m\geq 1}$ and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$f(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} C_{p(|\mathbf{x}|)}(\mathbf{x}, \mathbf{y}).$$

- So, VNP is closer to #P/poly than NP/poly.

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function p: N → N such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- Proposition. *(Valiant '79)* If $c: \{0,1\}^* \to \mathbb{N}$ is in #P/poly, the family $\{f_n\}_{n\geq 1}$ defined as $f_n(\mathbf{x})=\sum_{\mathbf{e}\in\{0,1\}^n} c(\mathbf{e})x_1^{e_1}\cdot x_2^{e_2}\cdot\ldots\cdot x_n^{e_n}$ is in VNP.

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function p: $\mathbb{N} \to \mathbb{N}$ such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- Proposition. *(Valiant '79)* If $c: \{0,1\}^* \to \mathbb{N}$ is in #P/poly, the family $\{f_n\}_{n\geq 1}$ defined as $f_n(\mathbf{x})=\sum_{\mathbf{e}\in\{0,1\}^n} c(\mathbf{e})x_1^{e_1}\cdot x_2^{e_2}\cdot\ldots\cdot x_n^{e_n}$ is in VNP.

- *Proof sketch.* Arithmetize the 3CNF associated with c and replace $x_1^{e_1}\cdot x_2^{e_2}\cdot\ldots\cdot x_n^{e_n}$ by $(e_1x_1+1-e_1)(e_2x_2+1-e_2)\ldots(e_nx_n+1-e_n)$. *Homework:* Fill in the details. ∎

Class VNP

- Definition. *(Valiant '79)* A polynomial family $\mathcal{F} = \{f_n\}_{n\geq 1}$ is in class VNP if there's another polynomial family $\mathcal{G} = \{g_m\}_{m\geq 1}$ in VP and a polynomial function $p: \mathbb{N} \rightarrow \mathbb{N}$ such that for every $n \geq 1$, $f_n(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|y|}} g_{p(n)}(\mathbf{x},\mathbf{y})$.

- Proposition. *(Valiant '79)* If $c: \{0,1\}^* \rightarrow \mathbb{N}$ is in #P/poly, the family $\{f_n\}_{n\geq 1}$ defined as $f_n(\mathbf{x})=\sum_{\mathbf{e}\in\{0,1\}^n} c(\mathbf{e})x_1^{e_1}\cdot x_2^{e_2}\cdot\ldots\cdot x_n^{e_n}$ is in VNP.

- The above <u>*sufficient condition*</u> for membership in VNP is known as **Valiant's criterion**.

Examples of families in VNP

- As VP $\subseteq$ VNP, any family in VP is also in VNP.
- Question. Are there families in VNP that are not in VP?

Examples of families in VNP

- As VP $\subseteq$ VNP, any family in VP is also in VNP.
- Question. Are there families in VNP that are not in VP?
- Let $X = (x_{ij})_{i,j \in [n]}$. Then,

$$\mathrm{Perm}_n := \mathrm{perm}(X) = \sum_{\sigma \in S_n} \prod_{i \in [n]} x_{i\,\sigma(i)} \,.$$

- Easy to see from Valiant's criterion that $\mathrm{Perm} := \{\mathrm{Perm}_n\}_{n \geq 1}$ is in VNP.

Examples of families in VNP

- As VP ⊆VNP, any family in VP is also in VNP.
- Question. Are there families in VNP that are not in VP?
- Let $X = (x_{ij})_{i,j\in[n]}$. Then,

$$\mathrm{Perm}_n := \mathrm{perm}(X) = \sum_{\sigma\in S_n} \prod_{i\in[n]} x_{i\,\sigma(i)} .$$

- Easy to see from Valiant's criterion that $\mathrm{Perm} := \{\mathrm{Perm}_n\}_{n\geq 1}$ is in VNP.
- The evaluation of Perm_n at the biadjacency matrix of a bipartite graph G gives the number of perfect matching in G. As this is a #P-complete problem, Perm ought to be outside VP. (more on this later.)

Examples of families in VNP

- As VP $\subseteq$ VNP, any family in VP is also in VNP.
- Question. Are there families in VNP that are not in VP?
- Let $X = (x_{ij})_{i,j\in[n]}$. Then,

$$\mathrm{Ham}_n := \sum_{\substack{\sigma\in S_n \\ \text{is a cycle of length } n}} \prod_{i\in[n]} x_{i\,\sigma(i)} \;.$$

- Easy to see from Valiant's criterion that $\mathrm{Ham} := \{\mathrm{Ham}_n\}_{n\geq 1}$ is in VNP.
- The evaluation of Ham_n at the adjacency matrix of a digraph G gives the number of Hamiltonian cycles in G. As this is a #P-complete problem, Ham ought to be outside VP. (more on this later.)

Examples of families in VNP

- As VP $\subseteq$ VNP, any family in VP is also in VNP.
- Question. Are there families in VNP that are not in VP?

- More such VNP polynomial families can be defined using various *graph properties*.

- Ref: *Completeness and Reductions in Algebraic Complexity Theory (habilitation)* by Bürgisser (1998)

Examples of families in VNP

- As VP $\subseteq$ VNP, any family in VP is also in VNP.
- Question. Are there families in VNP that are not in VP?
- Let $X = (x_{ij})_{i,j\in[n]}$, n a prime, $k < n$, and $\mathbb{F}_n[y]_k$ the set of univariate polynomials over $\mathbb{F}_n$ of deg $\leq k$. Then,

$$NW_{n,k} := \sum_{h\in\mathbb{F}_n[y]_k} \prod_{i\in[n]} x_{i\,h(i)} \,.$$

- Easy to see from Valiant's criterion that $NW := \{NW_{n,k}\}_{n>k\geq 1}$ is in VNP. NW is the family of *Nisan-Wigderson design polynomials* (simply, *design polynomials*).

Examples of families in VNP

- As VP ⊆ VNP, any family in VP is also in VNP.
- Question. Are there families in VNP that are not in VP?
- Let $X = (x_{ij})_{i,j\in[n]}$, n a prime, $k < n$, and $\mathbb{F}_n[y]_k$ the set of univariate polynomials over $\mathbb{F}_n$ of deg $\leq k$. Then,

$$NW_{n,k} := \sum_{h\in\mathbb{F}_n[y]_k} \prod_{i\in[n]} x_{i\,h(i)}\,.$$

- $NW_{n,k}$ is the polynomial corresponding to *Reed-Solomon codes* with message length $k+1$ and codeword length n. A monomial $\prod_{i\in[n]} x_{i\,h(i)}$ is the "codeword" for the coefficient vector of h.

Examples of families in VNP

- As VP $\subseteq$ VNP, any family in VP is also in VNP.
- Question. Are there families in VNP that are not in VP?

- Question. Are the families Perm, Ham and NW in VP?
- **We do not know!**

- If VP = VNP then they are obviously in VP.

Valiant's hypothesis

- Conjecture. *(Valiant '79)* VP $\neq$ VNP over *any* field.
- The conjecture is known as **Valiant's hypothesis**.

- We'll see later that if Valiant's hypothesis is true, then Perm and Ham are not in VP.

- Question. If VP $\neq$ VNP then is NW not in VP?
- **We do not know!**

Valiant's hypothesis

- Conjecture. *(Valiant '79)* $VP \neq VNP$ over *any* field.
- The conjecture is known as **Valiant's hypothesis**.

- Question. How does the $P \neq NP$ problem (Cook's hypothesis) relate to Valiant's hypothesis?

Valiant's hypothesis

- **Conjecture.** *(Valiant '79)* VP $\neq$ VNP over *any* field.
- The conjecture is known as **Valiant's hypothesis**.

- **Question.** How does the P $\neq$ NP problem (Cook's hypothesis) relate to Valiant's hypothesis?

- To prove P $\neq$ NP it is "*necessary*" to prove VP $\neq$ VNP. Let's see why…

Valiant's hypothesis

- **Proposition.** If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly.
- *Proof sketch.* Let $f: \{0,1\}^* \to \mathbb{N}$ be in #P/poly. Then, there's a polynomial size 3CNF family $\{C_m\}_{m\geq 1}$ and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$f(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|y|}} C_{p(|\mathbf{x}|)}(\mathbf{x}, \mathbf{y}).$$

Valiant's hypothesis

- Proposition. If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly.
- *Proof sketch.* Let $f: \{0,1\}^* \to \mathbb{N}$ be in #P/poly. Then, there's a polynomial size 3CNF family $\{C_m\}_{m\geq 1}$ and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$f(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|y|}} C_{p(|\mathbf{x}|)}(\mathbf{x}, \mathbf{y}).$$

- By arithmetizing the 3CNF $C_{p(|\mathbf{x}|)}$, we see that f defines a polynomial family in VNP over $\mathbb{Z}$. If VP=VNP over $\mathbb{Z}$ then $f(\mathbf{x})$ has a circuit D over $\mathbb{Z}$ of size $poly(|\mathbf{x}|)$.

Valiant's hypothesis

- Proposition. If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly.
- *Proof sketch.* Let $f: \{0,1\}^* \to \mathbb{N}$ be in #P/poly. Then, there's a polynomial size 3CNF family $\{C_m\}_{m\geq 1}$ and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$f(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} C_{p(|\mathbf{x}|)}(\mathbf{x}, \mathbf{y}).$$

- By arithmetizing the 3CNF $C_{p(|\mathbf{x}|)}$, we see that f defines a polynomial family in VNP over $\mathbb{Z}$. If VP=VNP over $\mathbb{Z}$ then $f(\mathbf{x})$ has a circuit D over $\mathbb{Z}$ of size $poly(|\mathbf{x}|)$. This "almost" implies $f \in$ FP/poly; the issue is D may have very <u>large integers</u> labeling its edges!

Valiant's hypothesis

- Proposition. If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly.
- *Proof sketch.* Let $f: \{0,1\}^* \to \mathbb{N}$ be in #P/poly. Then, there's a polynomial size 3CNF family $\{C_m\}_{m\geq 1}$ and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$f(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|y|}} C_{p(|\mathbf{x}|)}(\mathbf{x}, \mathbf{y}).$$

- By arithmetizing the 3CNF $C_{p(|\mathbf{x}|)}$, we see that f defines a polynomial family in VNP over $\mathbb{Z}$. If VP=VNP over $\mathbb{Z}$ then $f(\mathbf{x})$ has a circuit D over $\mathbb{Z}$ of size $poly(|\mathbf{x}|)$. As the value of $|f(\mathbf{x})|$ is $\leq 2^{poly(|\mathbf{x}|)}$, it is sufficient to do the computation in D modulo a prime $q > 2^{poly(|\mathbf{x}|)}$.

Valiant's hypothesis

- Proposition. If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly.
- *Proof sketch.* Let $f: \{0,1\}^* \to \mathbb{N}$ be in #P/poly. Then, there's a polynomial size 3CNF family $\{C_m\}_{m\geq 1}$ and a polynomial function $p: \mathbb{N} \to \mathbb{N}$ such that for every $\mathbf{x}$,

$$f(\mathbf{x}) = \sum_{\mathbf{y}\in\{0,1\}^{|\mathbf{y}|}} C_{p(|\mathbf{x}|)}(\mathbf{x}, \mathbf{y}).$$

- By arithmetizing the 3CNF $C_{p(|\mathbf{x}|)}$, we see that f defines a polynomial family in VNP over $\mathbb{Z}$. If VP=VNP over $\mathbb{Z}$ then $f(\mathbf{x})$ has a circuit D over $\mathbb{Z}$ of size $poly(|\mathbf{x}|)$. Finally, convert D modulo q to a multi-output Boolean circuit computing $f(\mathbf{x})$ implying $f \in$ FP/poly. ∎

Valiant's hypothesis

- Proposition. If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly, which implies P/poly = NP/poly.

- Theorem. *(Bürgisser '98)* Assuming GRH, if VP=VNP over $\mathbb{C}$, then NC^3/poly = P/poly = NP/poly = PH/poly and FP/poly = #P/poly.

- NC enters the picture because of depth reduction results for arithmetic circuits (we'll discuss this later).

Valiant's hypothesis

- Proposition. If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly, which implies P/poly = NP/poly.

- Theorem. *(Bürgisser '98)* Assuming GRH, if VP=VNP over $\mathbb{C}$, then NC^3/poly = P/poly = NP/poly = PH/poly and FP/poly = #P/poly.

- GRH (Generalized Riemann Hypothesis) is used to "replace" the complex numbers labelling the edges with integers of polynomial bit complexity.

Valiant's hypothesis

- Proposition. If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly, which implies P/poly = NP/poly.

- Theorem. *(Bürgisser '98)* Assuming GRH, if VP=VNP over $\mathbb{C}$, then NC^3/poly = P/poly = NP/poly = PH/poly and FP/poly = #P/poly.

- More precisely, GRH is used to show that if a system of integer polynomial equations is solvable over $\mathbb{C}$, then it is solvable modulo q for many primes q.

Valiant's hypothesis

- Proposition. If VP=VNP over $\mathbb{Z}$ then FP/poly = #P/poly, which implies P/poly = NP/poly.

- Theorem. *(Bürgisser '98)* If VP=VNP over a finite field then NC^2/poly = P/poly = NP/poly.

- In this sense, it is necessary to prove VP $\neq$ VNP before proving P/poly $\neq$ NP/poly.

VNP-completeness

- Definition. A family $\mathcal{G}$ is *VNP–complete* if $\mathcal{G} \in$ VNP and every $\mathcal{F} \in$ VNP is a p-projection of $\mathcal{G}$.

- Theorem. *(Valiant '79)* Perm is VNP-complete over any field of char $\neq 2$. Ham is VNP-complete over *any* field.

- Several other families have been shown to be VNP-complete by Bürgisser (1998).

VNP-completeness

- Definition. A family $\mathcal{G}$ is *VNP–complete* if $\mathcal{G} \in$ VNP and every $\mathcal{F} \in$ VNP is a p-projection of $\mathcal{G}$.

- Theorem. *(Valiant '79)* Perm is VNP-complete over any field of char $\neq 2$. Ham is VNP-complete over *any* field.

- The proof of the above theorem involves *clever gadget constructions*. Refer to Bürgisser (1998) or *Completeness classes on algebra* by Valiant (1979).

VNP-completeness

- Definition. A family $\mathcal{G}$ is *VNP–complete* if $\mathcal{G} \in$ VNP and every $\mathcal{F} \in$ VNP is a p-projection of $\mathcal{G}$.

- Theorem. *(Valiant '79)* Perm is VNP-complete over any field of char $\neq 2$. Ham is VNP-complete over *any* field.

- Question. Is NW VNP-complete?
- **We do not know!** Nor do we know if NW is in VP.

Circuits for Perm, Ham and NW

- Proposition. *(Ryser '63)* Let $X = (x_{ij})_{i,j \in [n]}$. Then,

$$\mathrm{Perm}_n := \mathrm{perm}(X) = \sum_{S \subseteq [n]} (-1)^{n-|S|} \prod_{i \in [n]} \Big(\sum_{j \in S} x_{ij} \Big).$$

- *Proof sketch.* Use inclusion-exclusion principle.

Circuits for Perm, Ham and NW

- Proposition. *(Ryser '63)* Let $X = (x_{ij})_{i,j \in [n]}$. Then,

  $$\mathrm{Perm}_n := \mathrm{perm}(X) = \sum_{S \subseteq [n]} (-1)^{n-|S|} \prod_{i \in [n]} \left(\sum_{j \in S} x_{ij} \right).$$

- The above formula gives a depth-3 formula of size $O(n^2 2^n)$ (which is the *smallest known formula*) for Perm_n.

- Question. Is there a circuit of size $2^{o(n)}$ for Perm_n?
- Question. Is there a circuit of size $2^{o(n \log n)}$ for Ham_n?
- Question. Is there a circuit of size $n^{o(k)}$ for $\mathrm{NW}_{n,k}$?
- **We do not know!**

Zero-testing

- Problem. *(Zero-testing on the Boolean cube)* Let $X = (x_{ij})_{i,j \in [n]}$ and f be $Perm_n$ or Ham_n or $NW_{n,k}$. Given an $A \in \{0,1\}^{n \times n}$, check if $f(A) = 0$.

Zero-testing

- Problem. *(Zero-testing on the Boolean cube)* Let $X = (x_{ij})_{i,j \in [n]}$ and f be $Perm_n$ or Ham_n or $NW_{n,k}$. Given an $A \in \{0,1\}^{n \times n}$, check if $f(A) = 0$.

- Obs. Zero-testing $Perm_n$ (which is the perfect matching problem) is in P. Zero-testing Ham_n (which is the Hamiltonian Cycle problem) is NP-complete.
- Question. What is the complexity of zero-testing $NW_{n,k}$ on the Boolean cube? Is it in P?
- **We do not know!** (a.k.a. the *Andreev's problem*)