Lecture 1: Algebraic Circuits & Algebraic Complexity

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

January 11, 2021

Overview

- Algebraic Primitives
- Algebraic Complexity: Complexity Classes
- Conclusion
- Acknowledgements

Groups

- *Group*: set G with law of composition $\circ : G \times G \to G$ such that
  1. *associative:* $(a \circ b) \circ c = a \circ (b \circ c)$
  2. *identity element:* $1 \in G$ such that $1 \circ a = a \circ 1 = a$, for all $a \in G$
  3. *inverse:* every element $a \in G$ has an inverse $a^{-1} \in G$ such that

$$a \circ a^{-1} = a^{-1} \circ a = 1$$

Groups

- *Group*: set G with law of composition $\circ : G \times G \to G$ such that
  1. *associative:* $(a \circ b) \circ c = a \circ (b \circ c)$
  2. *identity element:* $1 \in G$ such that $1 \circ a = a \circ 1 = a$, for all $a \in G$
  3. *inverse:* every element $a \in G$ has an inverse $a^{-1} \in G$ such that

$$a \circ a^{-1} = a^{-1} \circ a = 1$$

- Examples:
  - *Invertible matrices* (quintessential example) with *matrix multiplication*
  - *Permutations of a set* with *function composition*

Groups

- *Group*: set G with law of composition $\circ : G \times G \to G$ such that
  1. *associative:* $(a \circ b) \circ c = a \circ (b \circ c)$
  2. *identity element:* $1 \in G$ such that $1 \circ a = a \circ 1 = a$, for all $a \in G$
  3. *inverse:* every element $a \in G$ has an inverse $a^{-1} \in G$ such that

$$a \circ a^{-1} = a^{-1} \circ a = 1$$

- Examples:
  - *Invertible matrices* (quintessential example) with *matrix multiplication*
  - *Permutations of a set* with *function composition*
- G is *abelian group* if the law of composition is *commutative*

$$a \circ b = b \circ a, \quad \forall a, b \in G$$

Groups

- *Group*: set G with law of composition $\circ : G \times G \to G$ such that
  1. *associative:* $(a \circ b) \circ c = a \circ (b \circ c)$
  2. *identity element:* $1 \in G$ such that $1 \circ a = a \circ 1 = a$, for all $a \in G$
  3. *inverse:* every element $a \in G$ has an inverse $a^{-1} \in G$ such that

$$a \circ a^{-1} = a^{-1} \circ a = 1$$

- Examples:
  - *Invertible matrices* (quintessential example) with *matrix multiplication*
  - *Permutations of a set* with *function composition*
- G is *abelian group* if the law of composition is *commutative*

$$a \circ b = b \circ a, \quad \forall a, b \in G$$

- Examples of abelian groups
  - Integers, with addition operation
  - Real numbers, with addition operation
  - Integer matrices, with addition operation

Rings[1]

- *Ring* : set R with laws of composition
  - Addition $+ : R \times R \to R$
  - Multiplication $\cdot : R \times R \to R$

[1] Commutative rings with unit

Rings[1]

- *Ring* : set R with laws of composition
  - Addition $+ : R \times R \to R$
  - Multiplication $\cdot : R \times R \to R$
- R is *abelian group* with respect to addition
  - $0 \in R$ identity w.r.t. addition

[1] Commutative rings with unit

Rings[1]

- *Ring* : set R with laws of composition
  - Addition $+ : R \times R \to R$
  - Multiplication $\cdot : R \times R \to R$
- R is *abelian group* with respect to addition
  - $0 \in R$ identity w.r.t. addition
- Multiplication satisfies following properties
  - *associative*: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
  - *commutative*: $a \cdot b = b \cdot a$
  - *identity*: $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$
  - *distributive over addition*:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

[1] Commutative rings with unit

Rings[1]

- *Ring* : set R with laws of composition
  - Addition $+ : R \times R \to R$
  - Multiplication $\cdot : R \times R \to R$
- R is *abelian group* with respect to addition
  - $0 \in R$ identity w.r.t. addition
- Multiplication satisfies following properties
  - *associative*: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
  - *commutative*: $a \cdot b = b \cdot a$
  - *identity*: $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$
  - *distributive over addition*:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

- Examples
  - Integers with addition and multiplication (quintessential example)
  - Real numbers, complex numbers, with usual addition and multiplciation
  - Polynomial rings

[1] Commutative rings with unit

Rings - Definitions

- **Unit:** an element $u \in R$ is a unit if there is $v \in R$ such that $uv = 1$

Rings - Definitions

- **Unit:** an element $u \in R$ is a unit if there is $v \in R$ such that $uv = 1$
- **Associates:** two elements $a, b \in R$ are associates if there is a unit $u \in R$ such that $a = ub$

Rings - Definitions

- **Unit:** an element $u \in R$ is a unit if there is $v \in R$ such that $uv = 1$
- **Associates:** two elements $a, b \in R$ are associates if there is a unit $u \in R$ such that $a = ub$
- **Zero divisor:** a zero divisor in R is an element $a \in R \setminus \{0\}$ such that there is a non-zero $b \in R \setminus \{0\}$ such that $a \cdot b = 0$

Rings - Definitions

- **Unit:** an element $u \in R$ is a unit if there is $v \in R$ such that $uv = 1$
- **Associates:** two elements $a, b \in R$ are associates if there is a unit $u \in R$ such that $a = ub$
- **Zero divisor:** a zero divisor in R is an element $a \in R \setminus \{0\}$ such that there is a non-zero $b \in R \setminus \{0\}$ such that $a \cdot b = 0$
- **Integral domain:** a ring R is an integral domain if it has *no zero divisor*.

Rings - Definitions

- **Unit:** an element $u \in R$ is a unit if there is $v \in R$ such that $uv = 1$
- **Associates:** two elements $a, b \in R$ are associates if there is a unit $u \in R$ such that $a = ub$
- **Zero divisor:** a zero divisor in R is an element $a \in R \setminus \{0\}$ such that there is a non-zero $b \in R \setminus \{0\}$ such that $a \cdot b = 0$
- **Integral domain:** a ring R is an integral domain if it has *no zero divisor*.
- **Euclidean domain:** a ring R is an Euclidean domain if:
  - R is an integral domain and there is an Euclidean function $|\cdot| : R \to \mathbb{N} \cup \{-\infty\}$
  - for all $a, b \in R$, with $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r \quad \text{and} \quad |r| < |b|$$

Rings - Definitions

- **Unit:** an element $u \in R$ is a unit if there is $v \in R$ such that $uv = 1$
- **Associates:** two elements $a, b \in R$ are associates if there is a unit $u \in R$ such that $a = ub$
- **Zero divisor:** a zero divisor in R is an element $a \in R \setminus \{0\}$ such that there is a non-zero $b \in R \setminus \{0\}$ such that $a \cdot b = 0$
- **Integral domain:** a ring R is an integral domain if it has *no zero divisor*.
- **Euclidean domain:** a ring R is an Euclidean domain if:
  - R is an integral domain and there is an Euclidean function $|\cdot| : R \to \mathbb{N} \cup \{-\infty\}$
  - for all $a, b \in R$, with $b \neq 0$, there exists $q, r \in R$ such that

$$a = qb + r \quad \text{and} \quad |r| < |b|$$

- **Greatest common divisor:** the greatest common divisor of $a, b \in R$, denoted by $\gcd(a, b)$ is an element of R which divides both a and b, and if $c \in R$ divides a and b, then c divides $\gcd(a, b)$.

Fields

- *Field*: a ring $\mathbb{F}$ with addition and multiplication such that
  - every non-zero element has a multiplicative inverse

Fields

- *Field*: a ring $\mathbb{F}$ with addition and multiplication such that
  - every non-zero element has a multiplicative inverse
- Examples
  - Rational numbers
  - Real numbers
  - Complex numbers
  - Set of integers modulo a prime

Polynomial Rings

- Given a base ring R, we can construct a polynomial ring $R[x]$ by "adding a new variable" x to R in the *freest way possible*

Polynomial Rings

- Given a base ring R, we can construct a polynomial ring $R[x]$ by "adding a new variable" x to R in the *freest way possible*
- That is:

Leading coefficient

leading monomial

$b(x)$

$$a(x) = \underline{a_0 + a_1x + \cdots + a_dx^d} = \underline{b_0 + b_1x + \cdots + b_ex^e}, \qquad (a_d, b_e \neq 0)$$

Leading term

if, and only if, $d = e$ and $a_0 = b_0, a_1 = b_1, \ldots, a_d = b_d$

Polynomial Rings

- Given a base ring R, we can construct a polynomial ring $R[x]$ by "adding a new variable" x to R in the *freest way possible*
- That is:

$$a_0 + a_1 x + \cdots + a_d x^d = b_0 + b_1 x + \cdots + b_e x^e, \qquad (a_d, b_e \neq 0)$$

  if, and only if, $d = e$ and $a_0 = b_0, a_1 = b_1, \ldots, a_d = b_d$
- Can create the polynomial ring $R[x_1, \ldots, x_n]$ by adding the variables $x_1, \ldots, x_n$ freely as above.

Polynomial Rings

- Given a base ring R, we can construct a polynomial ring $R[x]$ by "adding a new variable" x to R in the *freest way possible*
- That is:

$$a_0 + a_1 x + \cdots + a_d x^d = b_0 + b_1 x + \cdots + b_e x^e, \qquad (a_d, b_e \neq 0)$$

  if, and only if, $d = e$ and $a_0 = b_0, a_1 = b_1, \ldots, a_d = b_d$
- Can create the polynomial ring $R[x_1, \ldots, x_n]$ by adding the variables $x_1, \ldots, x_n$ freely as above.
- What is our computational model to compute polynomials?

Polynomial Rings

- Given a base ring R, we can construct a polynomial ring $R[x]$ by "adding a new variable" x to R in the *freest way possible*
- That is:

$$a_0 + a_1 x + \cdots + a_d x^d = b_0 + b_1 x + \cdots + b_e x^e, \qquad (a_d, b_e \neq 0)$$

  if, and only if, $d = e$ and $a_0 = b_0, a_1 = b_1, \ldots, a_d = b_d$
- Can create the polynomial ring $R[x_1, \ldots, x_n]$ by adding the variables $x_1, \ldots, x_n$ freely as above.
- What is our computational model to compute polynomials?
- How can we measure computational complexity in such base rings?

Complexity measures in rings

- $\mathbb{Z} \to$ bit complexity of integer
  - $\lg a := \begin{cases} 1, & \text{if } a = 0 \\ 1 + \lfloor \log |a| \rfloor, & \text{otherwise} \end{cases}$

Complexity measures in rings

- $\mathbb{Z} \to$ bit complexity of integer
  - $\lg a := \begin{cases} 1, & \text{if } a = 0 \\ 1 + \lfloor \log |a| \rfloor, & \text{otherwise} \end{cases}$
- $\mathbb{Q} \to$ complexity of a/b is the total bit complexity of a and b

Complexity measures in rings

- $\mathbb{Z} \to$ bit complexity of integer
  - $\lg a := \begin{cases} 1, & \text{if } a = 0 \\ 1 + \lfloor \log |a| \rfloor, & \text{otherwise} \end{cases}$
- $\mathbb{Q} \to$ complexity of a/b is the total bit complexity of a and b
- $\mathbb{F}_q \to$ complexity of element is bit complexity $(\log q)$

$\mathbb{C} \to$ complexity of each element is 1

$\underline{\pi}$, 2 , $\underline{\sqrt{2}}$

Complexity measures in rings

- $\mathbb{Z} \to$ bit complexity of integer
  - $\lg a := \begin{cases} 1, & \text{if } a = 0 \\ 1 + \lfloor \log |a| \rfloor, & \text{otherwise} \end{cases}$
- $\mathbb{Q} \to$ complexity of a/b is the total bit complexity of a and b
- $\mathbb{F}_q \to$ complexity of element is bit complexity $(\log q)$
- Polynomial rings $R[x_1, \ldots, x_n]$
  1. dense representation

write down <u>every</u> coefficient of a monomial

$\mathbb{Z}[x, y]$

$$\begin{array}{ccccccc} & x^2 & xy & y^2 & x & y & 1 \\ xy \longmapsto d=2, & (0, & 1, & 0, & 0, & 0, & 0) \end{array}$$

<u>n d</u> $\binom{d+n}{d}$ coeffients $\sim n^d$

Complexity measures in rings

- $\mathbb{Z} \to$ bit complexity of integer
  - $\lg a := \begin{cases} 1, & \text{if } a = 0 \\ 1 + \lfloor \log |a| \rfloor, & \text{otherwise} \end{cases}$
- $\mathbb{Q} \to$ complexity of a/b is the total bit complexity of a and b
- $\mathbb{F}_q \to$ complexity of element is bit complexity $(\log q)$
- Polynomial rings $R[x_1, \ldots, x_n]$
  1. dense representation
  2. sparse representation

write down the <u>non-zero</u> coefficients

$P(x,y) = \underline{a}x^2 + \underline{b}xy + \underline{c}y^2$

$(a, (2,0))$ $(b, (1,1))$ $(c, (0,2))$

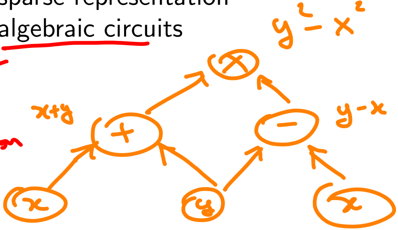
Complexity measures in rings

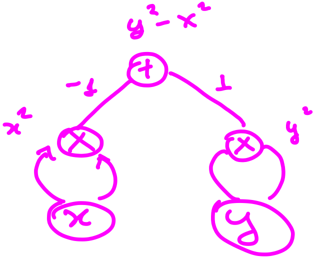
- $\mathbb{Z} \to$ bit complexity of integer
  - $\lg a := \begin{cases} 1, & \text{if } a = 0 \\ 1 + \lfloor \log |a| \rfloor, & \text{otherwise} \end{cases}$
- $\mathbb{Q} \to$ complexity of a/b is the total bit complexity of a and b
- $\mathbb{F}_q \to$ complexity of element is bit complexity $(\log q)$
- Polynomial rings $R[x_1, \ldots, x_n]$

unique rep.

1. dense representation
2. sparse representation
3. algebraic circuits

no unique representation

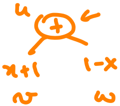




WORD PROBLEM: Φ, Ψ do they compute same polynomial?

Algebraic Circuits - Definitions

- **input gates:** gates of in-degree 0
- **output gates:** gates of out-degree 0
- **circuit size:** given by the number of edges in the circuit, denoted by $\mathcal{S}(\Phi)$
- **cost of field elements:** in classical algebraic complexity, there is unit cost for the use of any field element
- **circuit depth:** length of longest direct path from an input to an output
- **constant depth circuits:** for circuits of constant depth, we don't place restriction on the fan-in of an ~~edge~~. node
- **formal degree of a gate:** the degree of a gate is defined inductively
  - if input gate: degree is 0 if gate is element of the field, 1 if it is a variable
  - $u = w + v$ then $\deg(u) = \max(\deg(w), \deg(v))$
  - $u = w \times v$ then $\deg(u) = \deg(w) + \deg(v)$



VP [Valiant 1979, Valiant 1982]

Definition (p-bounded family of polynomials)

A family of polynomials $\{f_n\}_n$ over $\mathbb{F}$ is p-bounded if there is some polynomial $t : \mathbb{N} \to \mathbb{N}$ such that for every n,

- the *number of variables* in f_n and
- the *degree* of f_n

are $\leq t(n)$, and there is algebraic circuit of size $\leq t(n)$ computing f_n.

poly bounded

polynomial

VP [Valiant 1979, Valiant 1982]

Definition (p-bounded family of polynomials)

A family of polynomials $\{f_n\}_n$ over $\mathbb{F}$ is p-bounded if there is some polynomial $t : \mathbb{N} \to \mathbb{N}$ such that for every n,

- the *number of variables* in f_n and
- the *degree* of f_n

are $\leq t(n)$, and there is algebraic circuit of size $\leq t(n)$ computing f_n.

Definition (VP)

$\mathrm{VP}_{\mathbb{F}}$ is the class of all p-bounded families of polynomials over $\mathbb{F}$

VP [Valiant 1979, Valiant 1982]

Definition (p-bounded family of polynomials)

A family of polynomials $\{f_n\}_n$ over $\mathbb{F}$ is p-bounded if there is some polynomial $t : \mathbb{N} \to \mathbb{N}$ such that for every n,

- the *number of variables* in f_n and
- the *degree* of f_n

are $\leq t(n)$, and there is algebraic circuit of size $\leq t(n)$ computing f_n.

Definition (VP)

$\mathrm{VP}_{\mathbb{F}}$ is the class of all p-bounded families of polynomials over $\mathbb{F}$

- $\{x^{2^n}\}_n$ is not p-bounded, but can be computed by poly-sized circuits

repeated squaring

2^{2^n} mod p

VP [Valiant 1979, Valiant 1982]

Definition (p-bounded family of polynomials)

A family of polynomials $\{f_n\}_n$ over $\mathbb{F}$ is p-bounded if there is some polynomial $t : \mathbb{N} \to \mathbb{N}$ such that for every n,

- the *number of variables* in f_n and
- the *degree* of f_n

deg $\leq t(n)$ w.l.o.g.

are $\leq t(n)$, and there is algebraic circuit of size $\leq t(n)$ computing f_n.

Definition (VP)

$\mathrm{VP}_{\mathbb{F}}$ is the class of all p-bounded families of polynomials over $\mathbb{F}$

- $\{x^{2^n}\}_n$ is not p-bounded, but can be computed by poly-sized circuits
- Note that we don't require circuits in p-bounded family to have polynomial degree, but that comes "for free" as we will see.

VNP [Valiant 1979, Valiant 1982]

Definition (p-definable family of polynomials)

A family of polynomials $\{f_n\}_n$ over $\mathbb{F}$ is p-definable if there are

- $v : \mathbb{N} \to \mathbb{N}$ polynomial function (variable size)
- $w : \mathbb{N} \to \mathbb{N}$ polynomial function (witness size)
- and a family $\{g_n\}_n \in \mathrm{VP}_{\mathbb{F}}$ ("Turing machine")

such that for every n,

$$f_n(x_1, \ldots, x_{v(n)}) = \underbrace{\sum_{b \in \{0,1\}^{w(n)}}}_{\text{sum over all witnesses}} \overbrace{g_{w(n)}(x_1, \ldots, x_{v(n)}, b_1, \ldots, b_{w(n)})}$$

$$\mathrm{NP}: \; x \in L \iff \bigvee_{y \in \{0,1\}^{w(n)}} M(x,y) = 1 \quad \text{"existence of solution"}$$

$\updownarrow$ counting

$$\#P \qquad + \; g(x,y) \qquad \text{"counting \# of solutions / witnesses"}$$

VNP [Valiant 1979, Valiant 1982]

Definition (p-definable family of polynomials)

A family of polynomials $\{f_n\}_n$ over $\mathbb{F}$ is p-definable if there are

- $v : \mathbb{N} \to \mathbb{N}$ polynomial function (variable size)
- $w : \mathbb{N} \to \mathbb{N}$ polynomial function (witness size)
- and a family $\{g_n\}_n \in \mathrm{VP}_{\mathbb{F}}$ ("Turing machine")

such that for every n,

$$f_n(x_1, \ldots, x_{v(n)}) = \sum_{b \in \{0,1\}^{w(n)}} g_{w(n)}(x_1, \ldots, x_{vn}, b_1, \ldots, b_{wn})$$

Definition (VNP)

$\mathrm{VNP}_{\mathbb{F}}$ is the class of all p-definable families of polynomials over $\mathbb{F}$

VNP [Valiant 1979, Valiant 1982]

Definition (p-definable family of polynomials)

A family of polynomials $\{f_n\}_n$ over $\mathbb{F}$ is p-definable if there are

- $v : \mathbb{N} \to \mathbb{N}$ polynomial function (variable size)
- $w : \mathbb{N} \to \mathbb{N}$ polynomial function (witness size)
- and a family $\{g_n\}_n \in \mathrm{VP}_{\mathbb{F}}$ ("Turing machine")

such that for every n,

$$f_n(x_1, \ldots, x_{v(n)}) = \sum_{b \in \{0,1\}^{w(n)}} g_{w(n)}(x_1, \ldots, x_{vn}, b_1, \ldots, b_{wn})$$

Definition (VNP)

$\mathrm{VNP}_{\mathbb{F}}$ is the class of all p-definable families of polynomials over $\mathbb{F}$

- Roughly speaking, VNP class of polynomials f such that, given a monomial, one can efficiently compute the coefficient of this monomial in f

Analogies to P vs NP

Valiant's conjecture

- from the definitions above, it follows that

$$\mathrm{VP} \subseteq \mathrm{VNP}$$

- Valiant's conjecture is that these two classes are different.

Open Question

$$VP \neq^{?} VNP$$

Natural polynomials in VP?

$$\mathrm{Det}_n(X) = \sum_{\sigma \in S_n} (-1)^{\sigma} \cdot \prod_{i=1}^{n} X_{i\sigma(i)}$$

$\{\mathrm{Det}_n\} \in \mathrm{VP}$ (Gaussian elimination)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow \begin{pmatrix} a & b \\ 0 & d - \frac{cb}{a} \end{pmatrix}$$

$$a \cdot \left(d - \frac{cb}{a}\right) = ad - cb$$

we used divisions [if you can compute polynomial with divisions, then compute polynomial efficiently without] S'73

Natural polynomials in VP?

$$\mathrm{tr}\left[\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}\begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} \cdots \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}\right]$$

ABPs

Natural polynomials in VP?

Natural polynomials in VNP?

$$\mathrm{Per}_n(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i\sigma(i)}$$

$g(x,y)$
$\shortparallel$

$$\underbrace{\prod_{i=1}^{n}\left(\sum_{j=1}^{n} x_{ij}\, y_j\right)}_{\in \mathrm{VP}} = \underline{y_1 y_2 \cdots y_n} \cdot \mathrm{Per}_n(x) + \cdots$$

$$\mathrm{Per}_n(X) = \sum_{b \in \{0,1\}^n} \underbrace{g(x,b) \cdot \alpha_b}_{\in \mathrm{VP}}$$

Natural polynomials in VNP?

$\{ \mathrm{Perm}_n(x) \}_n$ complete for VNP

$\Updownarrow$

counting # perfect matchings in bipartite graphs is complete for #P

Reductions

Definition (linear projections)

A polynomial $f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ is a *projection* of a polynomial $g(y_1, \ldots, y_m) \in \mathbb{F}[y_1, \ldots, y_m]$ if there is an assignment $\rho \in (\{x_1, \ldots, x_n \cup \mathbb{F}\})^m$ such that $f(x_1, \ldots, x_n) = g(\rho_1, \ldots, \rho_m)$

$$y_i \mapsto \Phi_i(\bar{x}) \leftarrow$$

$$g(\Phi_1, \ldots, \Phi_m) = \underset{\in VP}{\underline{h}}(\quad)$$

Reductions

Definition (linear projections)

A polynomial $f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ is a *projection* of a polynomial $g(y_1, \ldots, y_m) \in \mathbb{F}[y_1, \ldots, y_m]$ if there is an assignment $\rho \in (\{x_1, \ldots, x_n \cup \mathbb{F}\})^m$ such that $f(x_1, \ldots, x_n) = g(\rho_1, \ldots, \rho_m)$

Definition (reduction via p-projections)

A polynomial family $\{f_n\}_n$ is a *p-projection* of a family $\{g_n\}_n$ if there is a polynomially bounded $t : \mathbb{N} \to \mathbb{N}$ such that for every n, f_n is a p-projection of $g_{t(n)}$.

Complete polynomials for VP and VNP?

Theorem (Completeness under quasi-poly projections [Valiant 1979])

The family $\{\mathrm{Det}_n\}$ *is* $\cancel{VP}_{\mathbb{F}}$*-complete with respect to quasi-polynomial projections.*

$VQP_{\mathbb{F}}$ quasi-poly ckt size

Theorem (Completeness for VNP [Valiant 1979])

The family $\{\mathrm{Per}_n\}$ *is* $VNP_{\mathbb{F}}$*-complete with respect to polynomial projections, as long as* $\mathrm{char}(\mathbb{F}) \neq 2$.

quasi-poly $\quad 2^{\log^c n} \quad n^{\log n}$

$n^{\log^2 n}$

Complete polynomials for VP and VNP?

Theorem (Completeness under quasi-poly projections [Valiant 1979])

The family $\{\mathrm{Det}_n\}$ is $VP_{\mathbb{F}}$-complete with respect to quasi-polynomial projections.

Theorem (Completeness for VNP [Valiant 1979])

The family $\{\mathrm{Per}_n\}$ is $VNP_{\mathbb{F}}$-complete with respect to polynomial projections, as long as $\mathrm{char}(\mathbb{F}) \neq 2$.

- Denoting VQP the class of quasi-p-bounded families (i.e., changing in the definition of VP all polynomially bounded by quasi-polynomially bounded), we have Valiant's second conjecture.

Open Question (Valiant)

$$VNP_{\mathbb{F}} \not\subset^{?} VQP_{\mathbb{F}}$$

Conclusion

- Today we learned some algebraic models of computation and their connections to some important problems in TCS
- We learned about the reductions between problems in the main classes
- We saw complete problems for the main algebraic classes

Det $\leftarrow$ bedrock of linear algebra

"linear algebra $\subset NC^2$"

Per $\leftarrow$ captures most interesting problems in combinatorics, statistical physics and many more

Director's cut: getting rid of divisions [Strassen 1973]

Director's cut: getting rid of divisions [Strassen 1973]

Director's cut: getting rid of divisions [Strassen 1973]

Acknowledgement

- Lecture based largely on:
  - Excellent survey by Shpilka and Yehudayoff [Shpilka & Yehudayoff 2010]
    https://www.nowpublishers.com/article/Details/TCS-039

References I

Valiant, Leslie 1979.
Completeness classes in algebra.
STOC

Valiant, Leslie 1982.
Reducibility by algebraic projections
L'Enseignement Mathematique

Shpilka, Amir and Yehudayoff, Amir 1982.
Arithmetic circuits: a survey of recent results and open questions
Foundations and Trends in Theoretical Computer Science

Strassen, Volker 1973.
Vermeidung von Divisionen
The Journal fur die Reine und Angewandte Mathematik