The border and its demystification

[-- Joint works with Pranjal Dutta, Prateek Dwivedi, CS Bhargav in CCC'21, FOCS'21, FOCS'22, STOC'24]

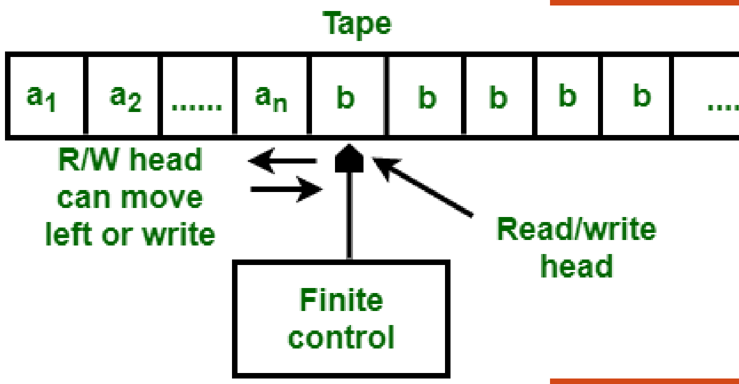
Nitin Saxena

CSE, IIT Kanpur

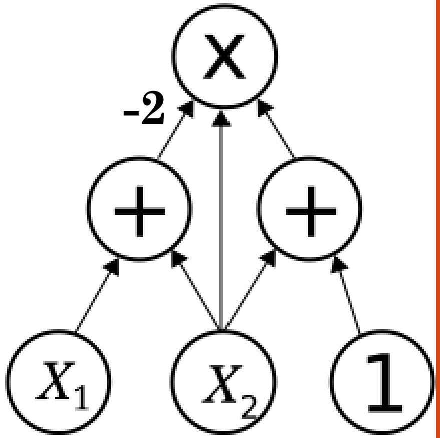
September 2024
Schloss Dagstuhl, Deutschland

SCHLOSS DAGSTUHL
Leibniz-Zentrum für Informatik

Computation, Circuit, VP



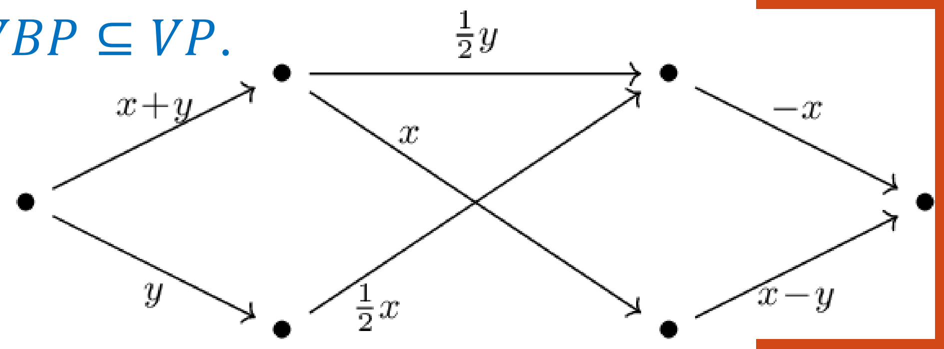
- Computation is what a Turing machine does.
  - Computes a language of strings.
  - Resources: *Time*, *Space*, …
- Circuit is a *relaxed* variant.
  - Boolean vs Algebraic.
  - Computes a polynomial $f(\boldsymbol{x}_n)$.
  - node = *operator* ; edge = *constant* ; leaf = *variable* ; root = *output* .
- size of a circuit = *#nodes* + *#edges* .
  - depth of a circuit = length of longest-path (leaf to root).
- $size(f)$ = min size of circuit computing $f(\boldsymbol{x}_n)$.
- Class VP is set of $f(\boldsymbol{x}_n)$ with $size(f) + deg(f) = poly(n)$.
  - $f = x_1^{2^n} x_2 \cdots x_n$ is **not** in VP.



Branching Program - VBP

- Determinant det_s: $det(X_{s\times s}) = \Sigma_\sigma\, sgn(\sigma)\cdot X_{1,\sigma(1)}\cdots X_{s,\sigma(s)}$.
- Iterated matrix multiplication (IMM): = *(1,1)*-th entry of $M_1\cdots M_d$, where, M_i are $s\times s$ matrices.
- **Theorem [Le Verrier 1840; Csanky'76]**: Both are in VP !
- IMM defines the algebraic branching program (ABP) model.
  - M_i with *linear* polynomials in $\boldsymbol{x}_n$.
  - ABPsize of this ABP is s^2dn .
  - Class VBP is set of $f(\boldsymbol{x}_n)$ with $ABPsize(f) = poly(n)$.
- **Theorem [Mahajan,Vinay'97]**: det ≡ IMM , and are in $VBP \subseteq VP$.
- OPEN: $VBP \neq VP$?
  - is Computing **harder** than Linear-Algebra ?

3x3 ABP ≡ Formula



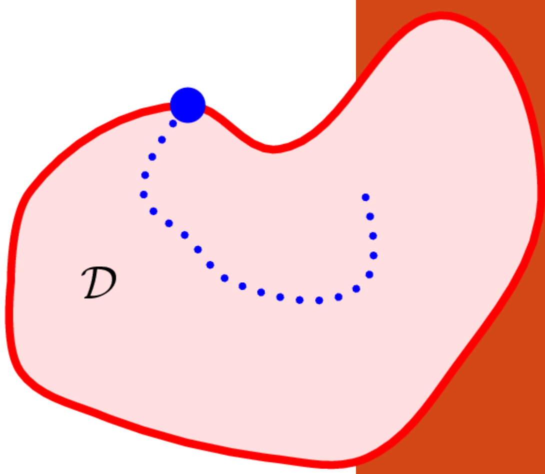
ExpSum circuits - VNP

- ExpSum circuit : $f(\boldsymbol{x}_n) = \Sigma_{\boldsymbol{a} \in \{0,1\}^m} g(\boldsymbol{x}, \boldsymbol{a})$, where verifier $g \in VP$.
  - Det, Permanent are of this type. [Count graph matchings]
- ExpSum defines the class *VNP*. [*Explicit* polynomials]
  - Like NP: $\boldsymbol{a}$ = witness string; g = verifier algorithm.
  - VNPsize of this ExpSum is $size(g) \cdot deg(g) \cdot nm$.
  - Class VNP is set of $f(\boldsymbol{x}_n)$ with VNP$size(f) = poly(n)$.
- **Theorem**: $VBP \subseteq VP \subseteq VNP$.
- OPEN: $VP \neq VNP$?
  - Is ExpSum *impractical* ?!
  - Algebraic version of $P \neq NP$!

Leslie Valiant (1949-)

- Valiant's conjecture ('79): There are *explicit*, **hard** polynomials ?
  - is Counting **harder** than Linear-Algebra ? $det \not\approx per$?

Approximative Circuits: $\overline{\mathrm{VP}}$



- How to *approximate* a polynomial?
  - Introduce variable ε, say $g(\boldsymbol{x},\varepsilon)$, and define $f(\boldsymbol{x}) := \lim_{\varepsilon\to 0} g(\boldsymbol{x},\varepsilon)$.
  - What's the *algebraic* way? *Any* field F.

- Approximative circuit : $g(\boldsymbol{x},\varepsilon) = \Sigma_{i=0}^{M} g_i(\boldsymbol{x}) \cdot \varepsilon^i$, of $VPsize\ s$, with constants in the function field $F(\varepsilon)$.

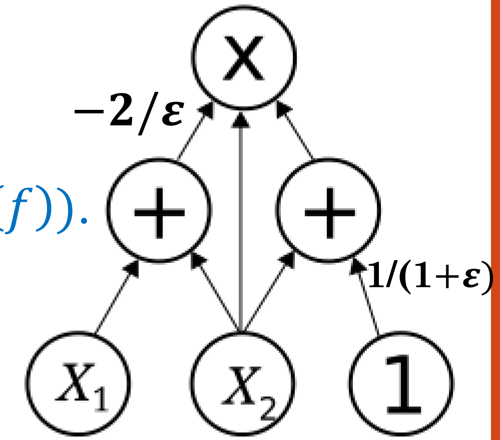
- Define $f(\boldsymbol{x}) := \lim_{\varepsilon\to 0} g(\boldsymbol{x},\varepsilon) := g_0(\boldsymbol{x})$.
  - $= g(\boldsymbol{x},0)$, but edge-constants may be undefined under $\varepsilon = 0$.

$((\boldsymbol{x}+\boldsymbol{\varepsilon y})^3 - \boldsymbol{x}^3)/3\boldsymbol{\varepsilon} \to \boldsymbol{x}^2\boldsymbol{y}$

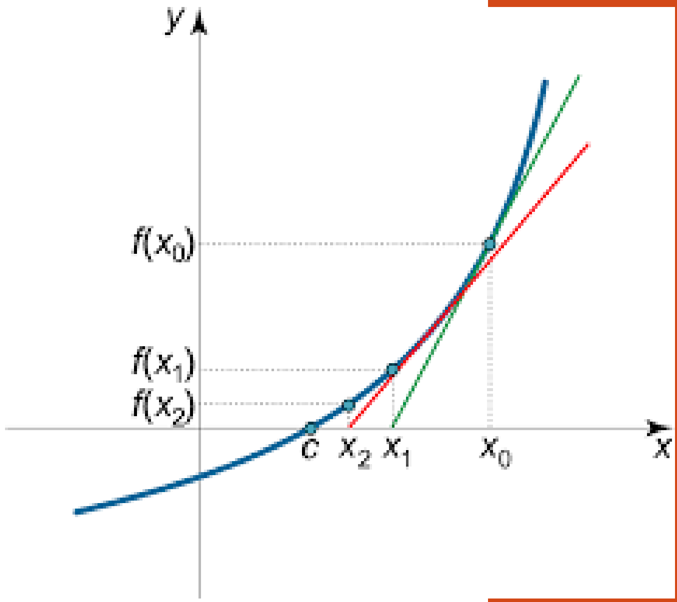
- Such $f(\boldsymbol{x})$ define the class $\overline{VP}$.
  - It's the Zariski closure of VP. *[Border]*
  - $\overline{size}(f)$ is $size(g)$. *[Approximative complexity]*

- **Theorem [Bürgisser'20]**: $M \le 2^{s^2}$; $\overline{size}(f) \le size(f) \le exp(\overline{size}(f))$.

- OPEN: $VP = \overline{VP}$?
  - is approximation **practical** ?



Motivating problem in $\overline{\text{VP}}$



$$f = x^{2^s} - 1$$

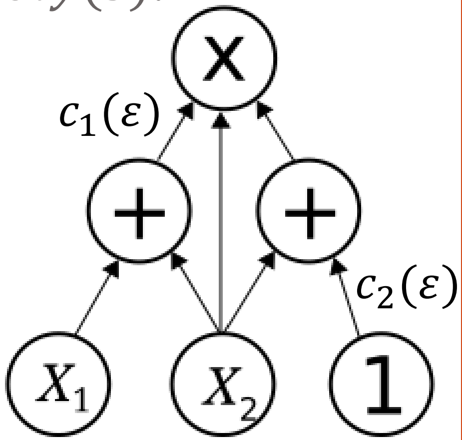
- Circuit factoring: Given $f(\boldsymbol{x})$ of size-s, find deg-d factor h ?
  - Degree of $f(\boldsymbol{x})$ could be 2^s. [so we need to *restrict* the factor degree]
  - What's the *algebraic* way? *Any* field F.
- OPEN: Is $size(h) = poly(sd)$? [Factor Conjecture]
- **Theorem [Bürgisser'04]**: $\overline{size}(h) = poly(sd)$.

- *Trick (perturbed Newton)*: Bad case is $f = h^{\boldsymbol{e}} q$, e is $superpoly(s)$.
  - Say, $h =: x_1 - \alpha \mod \langle x_2, \dots, x_n \rangle$.
  - Perturb, say x_1, by ε. Factor $f'(\boldsymbol{x}, \varepsilon) \coloneqq f(x_1 + \varepsilon, x_2, \dots) - f(\alpha + \varepsilon, x_2, \dots)$.
  - h is a simple factor of $f'(\boldsymbol{x}, \varepsilon) \mod \langle x_2, \dots, x_n \rangle$. [Kaltofen'89]
  - Lift to an actual factor in $F(\varepsilon)[\boldsymbol{x}]$ approximatively, i.e. $\varepsilon \to 0$. $\blacksquare$
- Gives $h \in \overline{VP}$, but **unknown** in VP.
  - Circuits closed under **Factoring** ?

Where does $\overline{\mathrm{VP}}$ live?

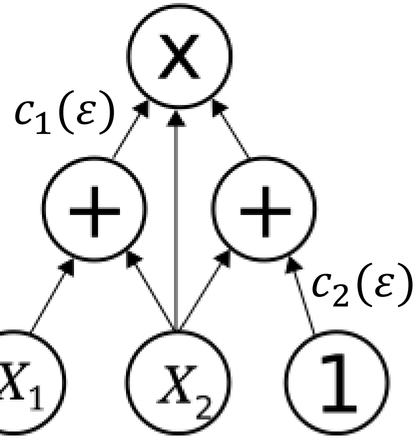
- OPEN: $\overline{VP} \subseteq VNP$? [deBorder]
  - How to present the approximative circuit $g(\boldsymbol{x}, \varepsilon)$, in practice.
- Presentable border: Assume $c_1(\varepsilon)$, $c_2(\varepsilon)$ to be circuits in ε !
  - ε is an *input* variable to size-s circuit $g(\boldsymbol{x}, \varepsilon)$.
  - Such $f(\boldsymbol{x})$ define the class $\overline{VP}_\varepsilon$. [Circuit in ε]
- **Theorem [Bhargav,Dwivedi,S., STOC'24]:** $\overline{VP}_\varepsilon \subseteq VNP$.
- *Trick (extract coeff)*: $g(\boldsymbol{x}, \varepsilon) = \varepsilon^M f(\boldsymbol{x}) + \varepsilon^{M+1} Q(\boldsymbol{x}, \varepsilon)$, M is *superpoly*(s).
  - Interpolate the circuit $g(\boldsymbol{x}, \varepsilon)$, with ε values in *finite field* F_{p^a} .
  - $p^a > M$, write $f(\boldsymbol{x})$ as ExpSum, with *verifier* g ?
  - $g(\boldsymbol{x}, \varepsilon)$, $\varepsilon \in F_{p^a}$: move to Boolean circuit and back. [Valiant's criterion]

$\blacksquare$



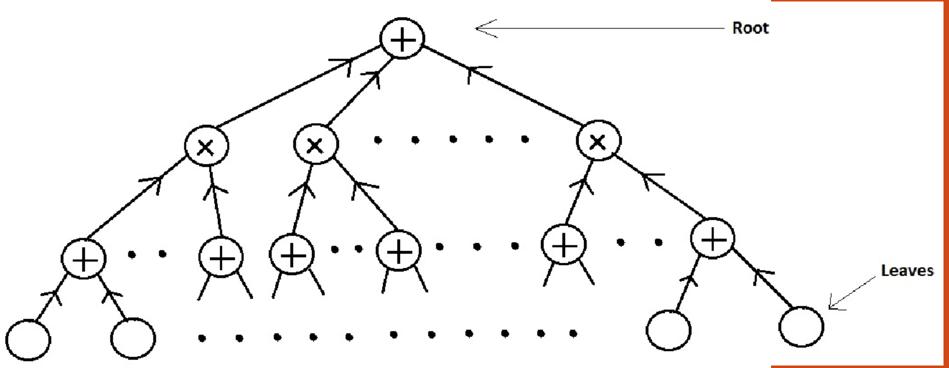
Where does $\overline{\mathrm{VP}}$ live? Factors?

- **Theorem [Bhargav,Dwivedi,S., STOC'24]**: $\overline{VP}_\varepsilon \subseteq VNP$.
  - Presentable is *explicit*!
- **Theorem [BDS'24]**: Size-s circuits have deg$\leq s$ factors* in VNP.
  - *separable [Bürgisser'04 gave *presentable* factor circuit!]
  - Also **[BDS'24]**: *VNP* is **closed** under factoring (over finite fields).
  - OPEN: Is VP closed under factoring (over finite fields)?
  - **[BDS'24]**: $\sqrt{f(\boldsymbol{x})}$ *mod* 2 is explicit, but is it *practical*?
- OPEN: $VP = \overline{VP}_\varepsilon = \overline{VP} \neq VNP$?
  - Is approximation *practical* & ExpSum *impractical* ?!



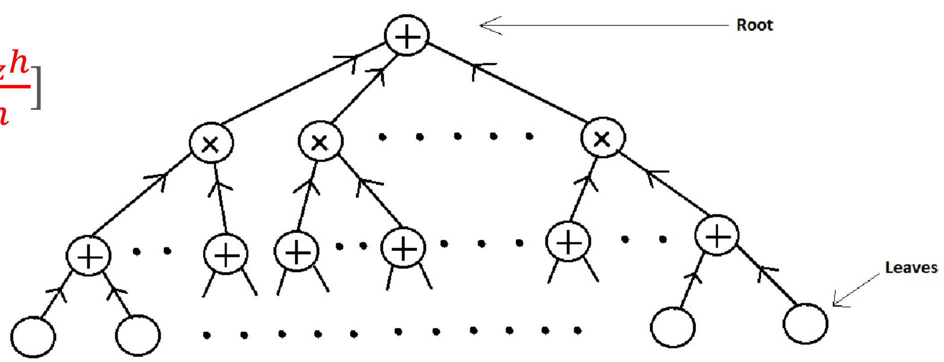
Shallow circuits - deeper techniques!

- Depth-3 circuit, fanin-k, $\Sigma^k \Pi \Sigma$: $g = \boldsymbol{\Sigma}_{i=1}^{k} \boldsymbol{\Pi}_{j=1}^{d} \ell_{i,j}(\boldsymbol{x})$, where $\ell_{i,j}$ are *linear* polynomials over field F.
- **Border**-depth-3 circuit, fanin-k, $\overline{\Sigma^k \Pi \Sigma}$: g as above, but over $F(\varepsilon)$, and then $f(\boldsymbol{x}) := \lim_{\varepsilon \to 0} g(\boldsymbol{x}, \varepsilon)$.
- What can $\Sigma^2 \Pi \Sigma$ and $\overline{\Sigma^2 \Pi \Sigma}$ compute?
- Former can't compute $f = x_1 x_2 + x_3 x_4 + x_5 x_6$.
- **Theorem [Kumar'20]**: $\overline{\Sigma^2 \Pi \Sigma}$ computes *every* $f(\boldsymbol{x})$.
- *Trick (Waring form & rank)*: Write $f(\boldsymbol{x}) = \boldsymbol{\Sigma}_{i=1}^{m} \ell_i^d$.
  - Stare at $\boldsymbol{\Sigma}_{i=1}^{m}(1 + \varepsilon^d \cdot \ell_i^d)$.
  - What's it mod ε^{2d} ?
  - $= 1 + \varepsilon^d \cdot f$. $\blacksquare$



Debordering border-depth-3

- $\overline{\Sigma^k \Pi \Sigma}$: Express $g = \boldsymbol{\Sigma}_{i=1}^{k} \boldsymbol{\Pi}_{j=1}^{d} \ell_{i,j}(\boldsymbol{x}, \varepsilon)$, and then $f(\boldsymbol{x}) := \lim_{\varepsilon \to 0} g(\boldsymbol{x}, \varepsilon)$.
- What's f exactly?
  - In VP? $\overline{VP}_{\varepsilon}$? VNP?
- **Theorem [Dutta,Dwivedi,S., FOCS'21]**: $\overline{\Sigma^2 \Pi \Sigma} \subseteq VBP$.
- *Trick (induction glorified)*: $T_1 + T_2 = f(\boldsymbol{x}) + \varepsilon \cdot S(\boldsymbol{x}, \varepsilon)$.
  - $T_1/T_2 + 1 = f/T_2 + \varepsilon \cdot S/T_2$.
  - Introduce variable z for derivation. Map $\varphi: x_i \mapsto z \cdot x_i + \alpha_i$.
  - $g_1 := \partial_z \varphi(T_1/T_2) = \partial_z \varphi(f/T_2) + \varepsilon \cdot \partial_z \varphi(S/T_2)$.
  - $g_1 = \varphi(T_1/T_2) \cdot (dlog\varphi(T_1) - dlog\varphi(T_2))$. $[dlog(h) := \frac{\partial_z h}{h}]$



Debordering border-depth-3

- $g_1 = \varphi(T_1/T_2) \cdot (dlog\varphi(T_1) \; - dlog\varphi(T_2))$. $[\, dlog(h) \coloneqq \frac{\partial_z h}{h} \,]$
  - $\in \overline{\left(\frac{\Pi\Sigma}{\Pi\Sigma}\right) \cdot \Sigma \wedge \Sigma}$ $\quad [\, dlog(A - z \cdot B) = \frac{-B}{A - z \cdot B} = \left(-\frac{B}{A}\right)\left(1 + \frac{zB}{A} + \left(\frac{zB}{A}\right)^2 + \cdots\right)]$
  - $\in \frac{ABP}{ABP}$ $\quad$ [*border of ROABP*]
  - $\partial_z \varphi\left(\frac{f}{T_2}\right) \to g_1 \to \frac{ABP}{ABP}$, gives $f \in ABP$ $\quad$ [*by interpolation*]
  - **DiDIL** = Divide, Derive, Induct, Limit .

$\blacksquare$

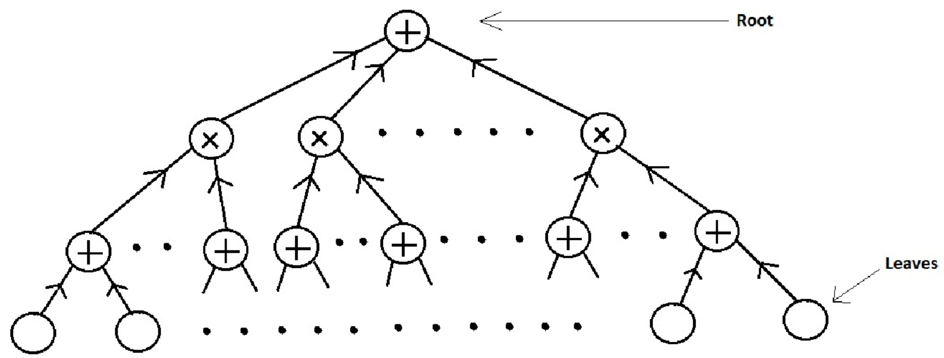
Theorem [Dutta,Dwivedi,S., FOCS'21]: $\overline{\Sigma^2 \Pi \Sigma} \subseteq VBP$.

$\overline{\Sigma^k \Pi \Sigma} \subseteq VBP$.

Finer lower bounds inside border-depth-3

- $\overline{\Sigma^k \Pi \Sigma}$: Express $g = \boldsymbol{\Sigma}_{i=1}^{k} \boldsymbol{\Pi}_{j=1}^{d} \ell_{i,j}(\boldsymbol{x}, \varepsilon)$, and then $f(\boldsymbol{x}) \coloneqq \lim_{\varepsilon \to 0} g(\boldsymbol{x}, \varepsilon)$.
- How do k and $k+1$ compare?
  - Remember $\overline{\Sigma^k \Pi \Sigma}$ computes every $f(\boldsymbol{x}_n)$!
- **Theorem [Dutta,S., FOCS'22]**: $\overline{\Sigma^k \Pi \Sigma}$, $\overline{\Sigma^{k+1} \Pi \Sigma}$ are *exp(n)* separated.
- *Trick (modify DiDIL)*: $P_d \coloneqq x_{1,1} \cdots x_{1,d} + x_{2,1} \cdots x_{2,d} + x_{3,1} \cdots x_{3,d}$.
  - Assume $T_1 + T_2 = P_d(\boldsymbol{x}) + \varepsilon \cdot S(\boldsymbol{x}, \varepsilon)$.
  - Introduce variable z for derivation. Homogenized map $\varphi: x_i \mapsto z \cdot x_i$.
  - $\partial_z \varphi \left(\frac{P_d}{T_2}\right) \to \overline{\left(\frac{\Pi\Sigma}{\Pi\Sigma}\right) \cdot \Sigma \wedge \Sigma}$
  - $x_{1,1} \cdots x_{1,d} \to \overline{\Sigma \wedge \Sigma}$ [coef of z^d & a trick]
  - implies *size* $\geq 2^d$ [Waring rank]

$\blacksquare$



Conclusion

- Special ABP (ROABP) makes *Debordering*, *Lower bounds*, and *Identity testing* possible.
  - What about the sum of two ROABPs?
- Strengthen results to $\overline{\Sigma^k \Pi\Sigma} \subseteq \Sigma\Pi\Sigma$?
- Is border presentable? Explicit?
- Circuit factoring?
- Details at https://www.cse.iitk.ac.in/users/nitin/

THANK YOU!

Questions?