Back to the seventies

In the 70's, Valiant defined two algebraic complexity classes : *VP* and *VNP*. What are they ?

Definition. A (family of) polynomial $(f_n) \in \mathbb{F}[X]$ over poly(n) variables and of (total) degree d, polynomial in n, is said to belong to *VP* if there is a polynomial size arithmetic circuit (C_n) computing it.
[Illustration of what's an arithmetic circuit]

Determinant, denoted det_n, lies in *VP*.

Permanent harder than Determinnat ?

Definition. A polynomial $(f_n) \in \mathbb{F}[X]$, is said to belong to VNP if there is a polynomial g_n in VP such that : $f_n(x, y_1, .., y_n) = \sum_{\varepsilon \in \{0,1\}^n} g_n(x, y_\varepsilon)$, where X is a (poly-size) set of variables, independent of y.

A key example is $per_n = \sum_\sigma \prod_{[n]} x_{i,\sigma(i)}$. It lies in VNP as the following formula shows :
$per_n = \sum_{T \subset [n]} (-1)^{n-|T|} \prod_{i=1}^n \sum_{j \in T} x_{i,j}$.

Indeed per_n is VNP-complete, meaning any other polynomial $g_n(X)$ in VNP is a projection of $per_N(A)$ (where $A = A(X, Y)$ has poly-size in n.)

and what do we expect ?

Fact. det_n is not VP-complete, it is VQP-complete, i.e. any $g_n \in VP$ is a projection of some $det_N(A)$ with $N = n^{O(\log n)}$.

per_n should not be a projection of det_N, that is we expect $VNP \neq VQP$. This is Valiant's second hypothesis.

Valiant's first hypothesis, the phare conjecture in this theory, is that $VP \neq VNP$. Very roughly, we loose non-negligible information by shutting down dimension of our algebraic varieties.

An intermediate class

The algebraic class of *branching programs*, is an intermediate model between arithmetic formulas and circuits. It "captures the computational power of matrix multiplication", meaning $IMM_{n,d}$, the $(1,1)$-entry of a product of d matrices of dimension $n \times n$, is complete for this class.
One of first successes in the theory was achieved by Ran Raz, for $IMM_{n,d}$, he introduced the partial derivatives method. It consists of studying dimension of a certain subspace of derivatives, and its robustness upon deletions during computation.

what we can prove so far

Restricted models have been studied thoroughly in the last 20 years : small depth circuits, monotone circuits, bounded degree circuits, multilinear or syntactically multilinear ones, and one can choose a setting with more constrained algebra, for instance not all variables commute.

Vinay, Agrawal, Koiran and Tavenas obtained a reduction of general model to the study of $\Sigma\Pi\Sigma\Pi$, i.e. subclass of depth four circuits : an exponential lower bound, with good enough constants, in the restricted case, implies $VP \neq VNP$.

Helplessness ?

But the best lower bound for small depth-circuits, is not even $n^{\omega(1)}$, it's a bare n^3, achieved by Limaye and Srinivasan (Bombay).
They used the shifted partial derivative method, a study of dimensions initiated by Kayal in 2014, together with "design gadgets", a method by Wigderson to exponentially reduce the number of variables in a particular case.

A common framework to prove a lower bound on size

Given a class of computation $\mathcal{F}$, find a finite measure ρ on polynomials such that : any polynomial computed by $F \in \mathcal{F}$ has a certain structure. For instance it can be written $\sum_{t \leq s} g_t h_t$; all building blocks $g_t h_t$ have a small measure : $\rho(gh) \leq A$; some polynomial $f \in VP$ enjoys $\rho(f) > M$.

It follows by considering some F computing f, that $s \geq M/A$.

example : multilinear setting and the rank method (Raz)

Structural result. Let f be a polynomial computed by a multilinear formula. Then

- f can be written as $\sum_{j \leq t} \prod_{i \leq k_j} g_i^{(j)}$
- with $k_j \geq c \log n$ for all j, $g_1, \dots, g_k$ variable-disjoint for all j
- inducing a partition $X_1 \cup \dots \cup X_k$ of $[n]$ such that all X_i have size at least $n^{7/8}$.
- Moreover $t \leq s^2$.

Rank method

Then building blocks are polynomials $g_1 \ldots g_k$, that is a product of a logarithmic (or more) number of multilinear factors defined on disjoint sets. What quantity is small for such product ? how about simultaneously small for a quadratic number of such products ?
Let $\mu(f) = \min_Y rk_Y(f)$ be the minimal rank of multilinear f seen as a $2^p \times 2^q$ matrix, where $p = |Y|$ and $q = n - p$.

Rank method : full-rank polynomials

A polynomial is full-rank if $\mu(f) = 2^{n/2}$ when Y runs over $\binom{[n]}{n/2}$, that is when the matrix $\Gamma_Y(f)$ has maximal rank for all balanced colorings of the set of variables.

Claim : one can unbalance a polynomial number of (distinct) $g_1 \ldots g_k$ simultaneously.

on board

- define a full-rank polynomial
- use probabilistic argument to prove existence of unbalancing coloring
- refine separtation by changing the target poynomial (Dvir et al.)
- how the bound is weakened upon less restrictive structural result (Alon-Kumar-Volk et al.)

future work ?

- The most general separations so far are the n^3 bound by Srinivasan for $\Sigma\Pi\Sigma$ model, and the $n^2/(\log n)^2$ bound for syntactically multilinear circuits by Alon et al.
- The only known result for the general setting is due to Strassen (back to the 80's), it gives a $\Omega(n \log n)$ lower bound to compute $(x_1 + \ldots + x_n)^k$, and the argument only uses a theorem by Bezout in algebraic geometry, bounding the cardinal of a finite intersection of varieties.