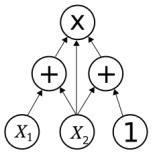
The P Versus NP Problem

Gorav Jindal, Anurag Pandey and Harry Zisopoulos

November 20, 2017

- A function $f : \mathbb{N} \longrightarrow \mathbb{N}$ is said to be "polynomially bounded" if there exists a polynomial $p \in \mathbb{R}[x]$ such that $f(n) \leq p(n)$ for all $n \in \mathbb{N}$.
- Arithmetization : Every Boolean circuit can be converted into an equivalent arithmetic circuit.
- $\mathbb{C}[x_1, x_2, ..., x_n]_d$ denotes the set of complex homogeneous polynomials of degree d in variables $x_1, x_2, ..., x_n$. We use $\overline{S}$ to denote the Zariski closure of a set S.

Definition 1 (Arithmetic or Algebraic Circuit)**.** An arithmetic circuit C over the field $\mathbb{F}$ and the set of variables $X = \{x_1, x_2, ..., x_n\}$ is a directed acyclic graph. Every node of C computes a polynomial in a natural way, polynomial computed by the output node of C is said to be the polynomial computed by C. Size of C is the number of nodes in C.



- Above circuit has size 6 and computes the polynomial $(x_1+x_2)\cdot x_2\cdot(x_2+1)\cdot$

Definition 2 (Complexity of a polynomial)**.** Complexity $L(f)$ of a polynomial $f \in \mathbb{F}[x_1, x_2, ..., x_n]$ is the size of smallest arithmetic circuit computing f.

- A p-family is a sequence $(f_1, f_2, \ldots, f_n, \ldots)$ of polynomials such that the number of variables and the degree of f_n are polynomially bounded functions of n.

Definition 3 (VP and VNP)**.** A p-family $(f_1, f_2, \ldots, f_n, \ldots)$ is in class VP if $L(f_n)$ is a polynomially bounded function of n. A p-family $(g_1, g_2, \ldots, g_n, \ldots)$ is in class VNP if there exists a p-family $(f_1, f_2, \ldots, f_n, \ldots)$ in VP such that $g_n = \sum_{e\in\{0,1\}^{q(n)}} f_n(x_1, x_2, ..., x_{p(n)}, e_1, e_2, \ldots, e_{q(n)})$ for some polynomially bounded functions $p(n)$ and $q(n)$.

- A similar notion of reductions to that of Karp reductions, called p-projections.
- Determinant family (Det_n) is almost "VP-complete" and permanent family (Per_n) is VNP-complete, here

$$\mathrm{Det}_n \stackrel{\text{def}}{=\!=} \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \prod_{i=1}^{n} x_{i\sigma(i)}$$

$$\mathrm{Per}_n \stackrel{\text{def}}{=\!=} \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i\sigma(i)}$$

- If GRH (Generalized Riemann hypothesis) is true then VP = VNP implies "P = NP", strictly speaking, the implication "P = NP" in this implication is not exactly P = NP but something closely related.
- So we can study (Det_n) vs (Per_n) instead of P vs NP.

Definition 4 (Orbit Closure of the determinant and border determinental complexity)**.** Define

$$D_n \stackrel{\text{def}}{=\!=} \overline{\mathrm{GL}_{n^2} \cdot [\mathrm{Det}_n]}$$

If $f \in \mathbb{C}[x_{11}, x_{12}, ...]_m$ then

$$\overline{\mathrm{dc}}(f) \stackrel{\text{def}}{=\!=} \min\{n \mid x_{nn}^{n-m} f \in D_n\}.$$

Conjecture 5 (Mulmuley-Sohoni)**.** $\overline{\mathrm{dc}}(\mathrm{Per}_m)$ *is not a polynomially bounded function of* m*.*

- GCT (Geometric complexity theory) approach to prove Mulmuley-Sohoni conjecture : define

$$P_n^m \stackrel{\text{def}}{=\!=} \overline{\mathrm{GL}_{n^2} \cdot [x_{nn}^{n-m} \, \mathrm{Per}_m]}$$

  We want to prove that if n is polynomially bounded in m then $P_n^m \not\subset D_n$. If this is true then there exists a non-zero $g \in \mathbb{C}[P_n^m]$ such that $g \notin \mathbb{C}[D_n]$, i.e, g is equal to zero in $\mathbb{C}[D_n]$. To find such g, GCT looks at $\mathbb{C}[P_n^m]$ and $\mathbb{C}[D_n]$ as GL_{n^2} representations and tries to find an irreducible representation of GL_{n^2} which appears with higher multiplicity in the irreducible GL_{n^2} decomposition of $\mathbb{C}[P_n^m]$ than in $\mathbb{C}[D_n]$.
- Waring rank : If $f \in \mathbb{C}[x_1, x_2, ..., x_n]_d$ then $W(f) \leq r$ if there exist $\ell_1, \ell_2, \ldots, \ell_r \in \mathbb{C}[x_1, x_2, ..., x_n]_1$ such that $f = \sum_{i=1}^{r} (\ell_i)^d$. Define

$$S_r^d = \{f \in \mathbb{C}[x_1, x_2, ..., x_n]_d \mid W(f) \leq r\}$$

  We say that $\overline{W}(f) \leq r$ if $f \in \overline{S_r^d}$.
- Characterization of $\overline{S_1^2}$ in case of $\mathbb{C}[x, y]_2$. If $f = ax^2 + bxy + cy^2$ then $\overline{W}(f) \leq 1$ iff $g(a, b, c) = b^2 - 4ac = 0$. For this very simple example, this is the desired g which we wanted to find above.