circuits $\mathcal{C} = \{C_i(x_1, \ldots, x_i) \mid i \in \mathbb{N}\}$ solves $\mathcal{F}$ if $\forall i$, $f_i = C_i$.

In this case, we can say that $\mathcal{F}$ can be solved in size bounded by size(C_n) & depth bounded by depth(C_n).

- This gives us a new way to measure the complexity of polynomials (or problems) — arithmetic circuit complexity.

- Arithmetic complexity classes were first defined by Valiant (1979).

In particular, the arithmetic analogs of P & NP.

- Defn: $VP_{\mathbb{F}}$ consists of families of polynomials, say $\{f_n\}_n$, over $\mathbb{F}$, that can be solved by circuits of poly(n) size & poly(n) degree.

- Eg. The family $\{x^{2^n}\}_n$ is not in $VP_{\mathbb{F}}$, for any $\mathbb{F}$.

  Though it is computable by poly(n)-size circuits, its degree is too high!

- An interesting polynomial (family) in VP is the determinant:

$$\det_n(\bar{x}) := \sum_{\pi \in Sym(n)} sgn(\pi) \cdot \prod_{i=1}^{n} x_{i,\pi(i)} .$$

Clearly $\det_n \in VP$

- We will see later that $\det_n \in VP$.

  (We'll abuse the notation a bit: by the polynomial $\det_n$ we actually mean the family $\{\det_n\}_n$.)

- VP is the algebraic analog of P.

  (The degree restriction is put to avoid computing very large numbers like 2^{2^n}, when $\mathbb{F}=\mathbb{Q}$.)

– What is the analog of NP ?

– **Defn**: A polynomial family $\{f_n\}_n$ is in $\underline{VNP_{\mathbb{F}}}$ if : $f_n(\bar{x}) = \sum_{\bar{\omega} \in \{0,1\}^{t(n)}} g_{n+t(n)}(\bar{x}, \bar{\omega})$,

where $\{g_n\}_n \in VP_{\mathbb{F}}$ & $t(n) = poly(n)$.

– One can think of $\bar{\omega}$ as a "witness" & so summing over all of them gives the arithmetic analog of an NP problem.

– A standard problem in VNP is:

Permanent $\underline{per_n(\bar{x})} := \sum_{\pi \in Sym(n)} \prod_{i \in [n]} x_{i,\pi(i)}$.

▷ $per_n(\bar{x}) \in VNP$.

Pf: • Let g be the function that takes an $n \times n$ matrix (x_{ij}), a vector $\bar{b} \in \{0,1\}^n$ & computes $g_{n^2+n}(\bar{x}, \bar{b}) := \prod_{i \in [n]} \left((-1+2b_i) \cdot \sum_{j \in [n]} b_j x_{ij} \right)$.

- Ryser's formula states:

$$\mathrm{per}_n(\bar{x}) = \sum_{\bar{t}\in\{0,1\}^n} g_{n^2+n}(\bar{x},\bar{t}).$$

[Pf sketch: Rewrite RHS as

$$\sum_{T\subseteq[n]} (-1)^{n-|T|} \left(\prod_{i\in[n]} \sum_{j\in T} x_{i,j}\right).$$

Note that the monomials involved are formed by picking a variable from each of the rows, eg. $x_{1,i_1} \cdot x_{2,i_2} \cdots x_{n,i_n}$.

Here, say i_1 repeats $r>1$ times. Then, the monomial can be associated to 2^{r-1} many subsets T: the sign contribution being

$$\sum_{S\subseteq[r-1]} (-1)^{|S|} = \sum_{0\le \ell\le r-1} (-1)^{\ell}\cdot\binom{r-1}{\ell} = (1-1)^{r-1} = 0.$$

$\Rightarrow$ The surviving monomials have distinct $i_1,\ldots,i_n$. □] □

- It is clear that:

▷ $VP \subseteq VNP$.