Depth-3 over finite fields

- Reduction to depth-4 works for *any* $\mathbb{F}$.

- The one to depth-3, however, requires $\mathrm{char}\,\mathbb{F} = \Omega(\sqrt{d})$ (in Ryser-Fischer's formula).

- Can we do reduction to depth-3 for small $\mathrm{char}\,\mathbb{F} =: p$? NO :

<u>Theorem</u> (Grigoriev, Karpinski '98): Over the field $\mathbb{F}_q$, $\det_d$ (or per_d) requires depth-3 circuits of size $2^{\Omega_q(d)}$.

<u>Rmk</u>: If there was a reduction for $\det_d$ to depth-3, over $\mathbb{F}_q$, then the size would have been $d^{O(\sqrt{d})}$.

<u>Proof</u>:
- Idea – $\mathbb{F}_q$ has q elements. We will think of q as fixed (i.e. constant wrt d).
- Let $C = \sum_{i \in [s]} T_i$ be a $\Sigma\Pi\Sigma$ circuit.

- Define $rk(T_i)$ to be the rank of the set of linear factors of T_i.
- Let $n := d^2$ & $\tau := \Theta_q(d)$ to be fixed later.
- A "low" rank T_i (say $rk(T_i) \leq \frac{\tau}{10q}$) has low rank partial derivatives.

  A "high" rank T_i $(rk(T_i) > \tau)$ we would like to zero out by picking a random evaluation in $\mathbb{F}_q^n$.
- These two together give us a matrix corresponding to the polynomial C.

$$M_k(C,\mathcal{A}) := \begin{array}{cc} & \bar{a} \\ \partial_\alpha & \underbrace{\begin{pmatrix} & & \\ \cdots & \partial_\alpha C(\bar{a}) & \\ & & \end{pmatrix}}_{\mathcal{A} \subseteq \mathbb{F}_q^n} \end{array} \Big\}\ \partial^{=k}$$

where, $k := \tau/10q$

& $\mathcal{A}$ shall be the set of evaluations on which each derivative $\partial^{=k} T_i$, for high $rk(T_i)$, vanishes.

- Once k, A are fixed we say that $\Gamma_{k,A}(f) := rk\, M_k(f, A)$ is a complexity measure (of polynomials).
- Obviously, we want to show $\Gamma_{k,A}(C)$ small & $\Gamma_{k,A}(\det_d)$ large.

Lemma 1 (Upper bound): $\forall \tau > 0$, $k \le \tau/10q$, there is a subset $\Sigma \subseteq \mathbb{F}_q^n$ of size $s \cdot e^{-\tau/8q} \cdot q^n$ s.t. for $A := \mathbb{F}_q^n \setminus \Sigma$, $\Gamma_{k,A}(C) < s \cdot q^\tau$.

Proof:

- To upper bound $\Gamma_{k,A}$ for C, it suffices to do it for T_1; because of subadditivity:

$$\Gamma(f+g) \le \Gamma(f) + \Gamma(g). \quad \text{(Exercise)}$$

- Let us now work with $T = \ell_1 \cdots \ell_D$.
- Case [$rk(T) \le \tau$]: Let $\{\ell_1, \ldots, \ell_r\}$ form a basis for $\{\ell_1, \ldots, \ell_D\}$.

Then T is a $\mathbb{F}_q$-lr. combination of $M :=$ $\{\ell_1^{e_1} \cdots \ell_r^{e_r} \mid e_i < q,\ i \in [r]\}$, as long as we evaluate it over $\mathbb{F}_q^n$.

$\Rightarrow \forall A \subseteq \mathbb{F}_q^n,\ \Gamma_{k,A}(T) \le |M| \le q^r \le q^\tau$.

• Case [$rk(T) > \tau$]: Now $r > \tau$ & $\ell_1, \dots, \ell_r$ span $\{\ell_1, \dots, \ell_D\}$.

For each nonconstant ℓ_i, $i \in [r]$, we have $\Pr_{\bar{a} \in \mathbb{F}_q^n} [\ell_i(\bar{a}) = 0] = 1/q$.

$$\Rightarrow \mathop{E}_{\bar{a}} [\# i \in [r],\ \ell_i(\bar{a}) = 0] = r/q > \tau/q$$

$$\Rightarrow \Pr_{\bar{a}} \left[\#\{i \mid \ell_i(\bar{a}) = 0\} < k = \frac{\tau}{10q} \right] < e^{-\tau/8q}$$

{ Exercise: Chernoff bounds
$$\Pr[X \gtrless (1 \pm \delta)\mu] < \left(\frac{e^{\pm\delta}}{(1\pm\delta)^{1\pm\delta}} \right)^{\mu}.$$ }

• Let $\mathcal{E}_T$ be the $\bar{a}$'s in the above "low" probability event. Then, $\bar{a} \notin \mathcal{E}_T$ makes $> k$ ℓ_i's zero in T.

$$\Rightarrow \forall \bar{a} \in \bigcup_{rk(T) > \tau} \mathcal{E}_T, \text{ every } \partial^{=k} T(\bar{a}) = 0.$$

$rk(T) > \tau$

$\Rightarrow \mathcal{E} := \bigcup_{rk(T)>\tau} \mathcal{E}_T$ has size $< s \cdot \varepsilon^{-\tau/8q} \cdot q^n$

& $A := \mathbb{F}_q^n \setminus \mathcal{E}$ zeroes out every function in $\partial^{=k} T$, for $T \in \{T_i \mid i \in [s], rk(T_i) > \tau\}$.

$\Rightarrow \Gamma_{k,A}(c)$ is contributed by only T_i's with $rk(T_i) < \tau$

$\Rightarrow \Gamma_{k,A}(c) < s \cdot q^{\tau}$. $\square$

- Next, we understand the measure for det_d & per_d, $n := d^2$.

<u>Lemma 2</u> (Lower bound): For any $A \subseteq \mathbb{F}_q^n$ of size $(1-o(1))q^n$, we have $\Gamma_{k,A}(det_d) = \binom{d}{k}^2$.

<u>Proof:</u> (from Saptharishi's survey)

•