Chapter 1

VF Factorization

In Rafael Oliviera's Paper [Oli16] he showed that if $P(\overline{x})$ is a polynomial with individual degrees bounded by r that can be computed by a formula size s and depth d, then any factor $f(\overline{x})$ of $P(\overline{x})$ can be computed bt a formula of size $poly((nr)^s, s)$ and depth $d+5$.

1.1 Factorizaion of Low Individual Degree

Lemma 1.1.1 (Approximation Lemma). *Let $P(\overline{x}, y) \in \mathbb{F}[\overline{x}, y]$. $P'(\overline{x}, y) \equiv \frac{\partial P}{\partial y}(\overline{x}, y)$ and $\mu \in \mathbb{F}$ be such that $P(\overline{0}, y) = 0$ but $P'(\overline{0}, y) = \xi \neq 0$. Then for each $t \geq 0$ there exists a unique polynomial $q_t(\overline{x})$ s.t. $\deg(q_t) \leq t$, $q_t(\overline{0}) = \mu$ and*

$$H^{\overline{x}}_{\leq t}[P(\overline{x}, q_t(\overline{x}))] \equiv 0$$

Moreover if P can be computed by a formula (circuit) Γ such that its output gate is an addition gate, there is a formula (circuit) Φ_t for the polynomial $q_t(\overline{x})$ such that the output gate of Φ_t is an addition gate, $depth(\Phi_t) \leq depth(\Gamma) + 2$ and

$$|\Phi_t| \leq 200(tr)^2 \binom{t+r+1}{r+1} |\Gamma|$$

If we require the in-degree of the formula (circuit) to be 2, then the size of Φ_t does not change and $depth(\phi_t) \leq depth(\Gamma) + 54\log(t)$.

Proof: We will prove the uniqueness of $q_t(\overline{x})$ and construct the formula of $q_t(\overline{x})$ by induction. First we will list our notations:
Notations:

- $P(\overline{x}, y) = \sum\limits_{i=0}^{r} C_i(\overline{x}) y^i$
- $\tilde{C}_i(\overline{x}) = C_i(\overline{x}) - C_i(\overline{0})$
- $H^{\overline{x}}_{\leq t}[P(\overline{x}, q_t(\overline{x}))]$ is same as saying $P(\overline{x}, q_t(\overline{x})) \bmod \langle \overline{x} \rangle^{t+1}$

We have $H^{\overline{x}}_{\leq t}[P(\overline{x}, q_t(\overline{x}))] \equiv 0$. Hence it must satisfy $H^{\overline{x}}_{\leq t-1}[P(\overline{x}, q_t(\overline{x}))] \equiv 0$ and therefore we have

$q_t(\overline{x}g(\overline{x}) + q_{t-1}(\overline{x})$ where $g(\overline{x})$ is a homogeneous polynomial of degree t. We can write. Therefore we have

$$\begin{aligned}
0 \equiv P(\overline{x}, q_t(\overline{x})) \bmod \langle\overline{x}\rangle^{t+1} &\equiv P(\overline{x}, q_{t-1} + g(\overline{x})) \bmod \langle\overline{x}\rangle^{t+1} \\
&\equiv \sum_{i=0}^{r} C_i(\overline{x}) \left(q_{t-1}(\overline{x}) + g(\overline{x})\right)^i \bmod \langle\overline{x}\rangle^{t+1} \\
&\equiv \sum_{i=0}^{r} C_i(\overline{x}) q_{t-1}^i(\overline{x}) + \sum_{i=0}^{r} i \cdot C_i(\overline{x}) g(\overline{x}) q_{t-1}^{i-1}(\overline{x}) \bmod \langle\overline{x}\rangle^{t+1} \\
&\qquad \text{[Since for all powers of } g(\overline{s}) \text{ more than 1 it has more than } t+1 \text{ degree} \\
&\qquad\qquad \overline{x} \text{ term which will be turned to 0 because of mod} \langle\overline{x}\rangle^{t+1}] \\
&\equiv \sum_{i=0}^{r} C_i(\overline{x}) q_{t-1}^i(\overline{x}) + \sum_{i=0}^{r} i \cdot C_i(\overline{0}) g(\overline{x}) q_{t-1}^{i-1}(\overline{0}) \bmod \langle\overline{x}\rangle^{t+1} \\
&\equiv \sum_{i=0}^{r} C_i(\overline{x}) q_{t-1}^i(\overline{x}) + \gamma \cdot g(\overline{x}) \bmod \langle\overline{x}\rangle^{t+1} \\
&\iff g(\overline{x}) \equiv -\frac{1}{\gamma} \sum_{i=0}^{r} C_i(\overline{x}) q_{t-1}^i(\overline{x}) \bmod \langle\overline{x}\rangle^{t+1}
\end{aligned}$$

Since we have $q_{t-1}(\overline{x})$ is unique we have $g(\overline{x})$ is also unique which implies that $q_t(\overline{x})$ is also unique. ■

Corollary 1.1.2. *Let $P(\overline{x}, y)$ and $\mu \in \mathbb{F}$ be defined as in Lemma 1.1.1 for each $t \in \mathbb{N}_0$ let $q_t(\overline{x})$ be the unique polynomial obtained from Lemma 1.1.1. If $h(\overline{x}, y) \in \mathbb{F}[\overline{x}, y]$ is such that $h(\overline{0}, y) = 0$, $\frac{\partial h}{\partial y}(\overline{0}, \mu) \neq 0$ and there exists $t \in \mathbb{N}$ and $Q(\overline{x}, y) \in \mathbb{F}$ such that*

$$H_{\leq t}^{\overline{x}}[P(\overline{x}, y)] \equiv H_{\leq t}^{\overline{x}}[h(\overline{x}, y) \cdot Q(\overline{x}, y)] \tag{1.1}$$

then the polynomial $q_t(\overline{x})$ also satisfies

$$H_{\leq t}^{\overline{x}}[h(\overline{x}, q_t(\overline{x}))] \equiv 0, \qquad \forall\, t \geq 0 \tag{1.2}$$

Proof: Since μ is a root of $h(\overline{0}, y)$ and $\frac{\partial h}{\partial y}(\overline{0}, \mu) \neq 0$ by Lemma 1.1.1 we have that there exists a unique $g_t(\overline{x})$ such that $H_{\leq t}^{\overline{x}}[h(\overline{x}, g_t(\overline{x}))] \equiv 0$. From (1.1) we have

$$\begin{aligned}
H_{\leq t}^{\overline{x}}[P(\overline{x}, g_t(\overline{x}))] &\equiv H_{\leq t}^{\overline{x}}\left[h\left(\overline{x}, g_t\left(\overline{x}\right)\right) \cdot Q\left(\overline{x}, g_t\left(\overline{x}\right)\right)\right] \\
&\equiv H_{\leq t}^{\overline{x}}\left[H_{\leq t}^{\overline{x}}\left[h\left(\overline{x}, g_t\left(\overline{x}\right)\right)\right] \cdot Q\left(\overline{x}, g_t\left(\overline{x}\right)\right)\right] \\
&\equiv H_{\leq t}^{\overline{x}}\left[0 \cdot Q\left(\overline{x}, g_t\left(\overline{x}\right)\right)\right] \equiv 0
\end{aligned}$$

Since $q_t(\overline{x})$ is unique by Lemma 1.1.1 we have $q_t(\overline{x}) \equiv g_t(\overline{x})$. ■

1.2 Reducing the Degree Bound to One Variable

Theorem 1.2.1. *Let $P(\overline{x}, y) \in \mathbb{F}[\overline{x}, y] \backslash \{0\}$ where $\overline{x} = (x_1, x_2, \ldots, x_n)$ such that $\deg_y(P) \leq r$ and $f(\overline{x}, y)$ be a monic factor of P or $g(\overline{x})$ be a root of P with respect to P i.e. $P(g(\overline{x}), y) = 0$, where $\mathbb{F}$ is a field of characteristic zero. If there exists a formula (circuit) of size s and depth d computing P then there exists a formula (circuit) of depth $d + 5$ and size $poly((nr)^r, s)$ computing f or g.*

Proof: content... ■

Bibliography

[Oli16] Rafael Oliveira. “Factors of Low Individual Degree Polynomials”. In: *computational complexity* 25.2 (June 2016), pp. 507–561. ISSN: 1420-8954. DOI: 10.1007/s00037-016-0130-2. (Visited on 07/28/2023).