# 1 Lecture 14, Scribe: Xuangui Huang

This lecture is given by Chin Ho Lee based on the paper [1]. In this lecture he proved the upper bound of the approximate degree of the surjectivity function. This upper bound matches the lower bound we have seen in this class, so we get a tight result of the approximate degree of SURJ.

## 1.1 Upper Bound of $d_{1/3}(\mathbf{SURJ})$

**Theorem 1.** $d_{1/3}(\mathrm{SURJ}_{R,N}) = \tilde{O}(N^{3/4})$.

Recall that $\mathrm{SURJ}_{R,N}\colon [R]^N \to \{0,1\}$ is the function that gets value 1 iff for all range item $r \in [R]$, $r$ appears in input. Without loss of generality we can assume $R = O(N)$ because:

- if $R > N$, then this function is always 0;
- if $R \ll N$, then $\mathrm{SURJ}_{R,N}(x_1, \ldots, x_N) = \mathrm{SURJ}_{R+N,2N}(x_1, \ldots, x_N, R+1, \ldots, R+N)$.

We will prove this theorem in a more general setting: let $\mathcal{R} \subseteq [R]$, define $\mathrm{SURJ}_{\mathcal{R}}(x) = 1$ iff $\forall r \in \mathcal{R}$, $r$ appears in $x$. Then what we will actually prove is:

**Theorem 2.** $d_{1/3}(\mathrm{SURJ}_{\mathcal{R}}) = \tilde{O}(N^{3/4})$.

We need the following lemma:

**Lemma 3.** Let $T$ be a number. There exists a polynomial $p_{\mathcal{R}}\colon \{0,1\}^{N \log R} \to \mathbb{R}$ of degree $\tilde{O}(\sqrt{NT})$ such that

- $p_{\mathcal{R}}(x) \in [\frac{9}{10}, 1]$ if $\mathrm{SURJ}_{\mathcal{R}}(x) = 1$ and $x \in G_{\mathcal{R}}$,
- $p_{\mathcal{R}}(x) \in [0, \frac{1}{10}]$ if $\mathrm{SURJ}_{\mathcal{R}}(x) = 0$ and $x \in G_{\mathcal{R}}$,
- $|p_{\mathcal{R}}(x)| \leq \exp\left(\tilde{O}(\sqrt{T} \cdot b_{\mathcal{R}}(x))\right)$ if $x \notin G_{\mathcal{R}}$,

where

- $\#_r(x) = \#\{i : x_i = r\}$,

- $G_{\mathcal{R}} = \{x : \#_r(x) \leq T, \forall r \in \mathcal{R}\}$,
- $b_{\mathcal{R}}(x) = \#\{r \in \mathcal{R} : \#_r(x) > T\}$.

*Proof of Theorem 2 assuming Lemma 3.* The algorithm corresponding to the polynomial we get to approximate $\mathrm{SURJ}_{\mathcal{R}}$ is:

1. Sample $S \subseteq [N]$ of size $s$;
2. Define $\mathcal{R}(x_S) = \{r \in \mathcal{R} : r \text{ appears in } x_S\}$, where $x_S$ is the restriction of input $x$ on $S$;
3. Output $p_{\overline{\mathcal{R}(x_S)}}(x)$.

Therefore we get

$$\begin{aligned} r(x) &= \mathbb{E}_{|S|=s}[p_{\overline{\mathcal{R}(x_S)}}(x)] \\ &= \frac{1}{\binom{N}{s}} \sum_{|S|=s} p_{\overline{\mathcal{R}(x_S)}}(x) \\ &= \frac{1}{\binom{N}{s}} \sum_{|S|=s} \sum_{y \in [R]^S} \mathbf{1}(x_S = y) \cdot p_{\overline{\mathcal{R}(x_S)}}(x), \end{aligned}$$

which can be written as a polynomial of degree

$$s \cdot logR + \deg(p_{\overline{\mathcal{R}(x_S)}}(x)) = \tilde{O}(s + \sqrt{NT}).$$

To see that this polynomial approximates $\mathrm{SURJ}_{\mathcal{R}}$, note that

$$\begin{aligned} \mathbb{E}_{|S|=s}[p_{\overline{\mathcal{R}(x_S)}}(x)] &= \frac{1}{\binom{N}{s}} \sum_{|S|=s} \sum_{b=0}^{N/T} \mathbf{1}(b_{\overline{\mathcal{R}(x_S)}} = b) \cdot p_{\overline{\mathcal{R}(x_S)}}(x) \\ &= \sum_{b=1}^{N/T} \frac{1}{\binom{N}{s}} \sum_{|S|=s} \mathbf{1}(b_{\overline{\mathcal{R}(x_S)}} = b) \cdot p_{\overline{\mathcal{R}(x_S)}}(x) \\ &\quad + \frac{1}{\binom{N}{s}} \sum_{|S|=s} \mathbf{1}(b_{\overline{\mathcal{R}(x_S)}} = 0) \cdot p_{\overline{\mathcal{R}(x_S)}}(x). \end{aligned}$$

We have

$$\begin{aligned}\Pr_{|S|=s}[b_{\overline{\mathcal{R}(x_S)}} = b] &\le \Pr_{|S|=s}[b_{\overline{\mathcal{R}(x_S)}} \ge b] \\ &\le \binom{|B_{\overline{\mathcal{R}(x_S)}}|}{b} \Pr[r_{i_1}, \ldots, r_{i_b} \text{ appears in } \overline{\mathcal{R}(x_S)}] \\ &\le \binom{|\mathcal{R}|}{b} \left(1 - \frac{T}{N}\right)^{s \cdot b},\end{aligned}$$

therefore

$$\begin{aligned}\sum_{b=1}^{N/T} \frac{1}{\binom{N}{s}} \sum_{|S|=s} \mathbf{1}(b_{\overline{\mathcal{R}(x_S)}} = b) \cdot p_{\overline{\mathcal{R}(x_S)}}(x) &\le \sum_{b=1}^{N/T} \left(\exp\left(-b\frac{sT}{N} + b \log R\right) |p_{\overline{\mathcal{R}(x_S)}}(x)|\right) \\ &\le \sum_{b=1}^{N/T} \exp\left(-b\left(\frac{sT}{N} + \tilde{O}(\sqrt{T})\right) + b \log R\right).\end{aligned}$$

To balance all the terms we need to set $\frac{sT}{N} = \sqrt{T}$ and $s = \sqrt{NT}$, thus we get $T = \sqrt{N}$ and $s = N^{3/4}$. Hence we get a degree-$\tilde{O}(N^{3/4})$ polynomial

$$r(x) = o(1) + (1 - o(1))\mathrm{SURJ}_{\mathcal{R}}(x).$$

□

*Proof of Lemma 3.* Recall the lemma in Justin Thaler's lecture:

**Claim 4.** Let $T$ be a number. There exists a polynomial $O\colon \{0,1\}^N \to \mathbb{R}$ of degree $O(\sqrt{T})$ such that

- $O(x) \in [1-\epsilon, 1]$ if $\bigvee_i x_i = 1$ and $|x| \le T$,
- $O(x) \in [0, \epsilon]$ if $\bigvee_i x_i = 0$ and $|x| \le T$,
- $|O(x)| \le exp(\tilde{O}(\sqrt{T}))$ if $|x| > T$.

Notice that $\mathrm{SURJ}_{\mathcal{R}}(x) = \bigwedge_{r \in \mathcal{R}} \bigvee_{i \in [N]} \mathbf{1}(x_i = r)$. We can composite the degree-$\sqrt{N}$ approximation polynomial $A$ of AND, the $O$ given above, and the degree-$logR$ polynomial of $\mathbf{1}(x_i = r)$. The degree of this polynomial is $\tilde{O}(\sqrt{NT})$, and we are done by the following claims.

**Claim 5.** $|A \circ O \circ \mathbf{1}(x_i = r)(x)| \leq \exp\left(\tilde{O}(\sqrt{T} b_{\mathcal{R}}(x))\right)$ for $|x| \geq T$.

**Claim 6.** If $\tilde{f}\colon \{0,1\}^N \to [0,1]$ $\epsilon$-approximates $f : \{0,1\}^N \to \{0,1\}$, $\tilde{g}\colon X \to [0,1]$ $\delta$-approximates $g : X \to \{0,1\}$, then $\tilde{f} \circ \tilde{g}\colon X^N \to \mathbb{R}$ $(\epsilon + \delta N)$-approximates $f \circ g$. □

*Proof of Claim 5.* $A\colon \{0,1\}^{|\mathcal{R}|} \to [0,1]$, thus we have

$$A(z) = \sum_{S \subseteq \mathcal{R}} A_S \prod_{i \in S} z_i \prod_{i \notin S} (1 - z_i),$$

where $|A_S| \leq 1$. Therefore

$$\begin{aligned} |A(z)| &\leq \sum_{S \subseteq \mathcal{R}} \prod_{i \in S} |z_i| \prod_{i \notin S} |1 - z_i| \\ &= \prod_{i \in \mathcal{R}} (|z_i| + |1 - z_i|) \\ &= \left(\exp(\tilde{O}(\sqrt{T}))\right)^{b_{\mathcal{R}}(x)}. \end{aligned}$$

□

*Proof of Claim 6.* Fix any input $x \in X^N$, let $y_i = g(x_i) \in \{0,1\}$, $z_i = \tilde{g}(x_i) \in [0,1]$. By triangle inequality, it suffices to show that $|\tilde{f}(y) - \tilde{f}(z)| \leq \delta N$.

Define independent random variables $Z_i \in \{0,1\}$ such that $\mathbb{E}[Z_i] = z_i$. Then

$$\tilde{f}(z) = \mathbb{E}[\tilde{f}(Z)] = \Pr[Z = y] \cdot \tilde{f}(y) + \Pr[Z \neq y] \cdot \mathbb{E}[\tilde{f}(Z) | Z \neq y].$$

Since $\tilde{g}$ $\delta$-approximates $g$, we have $|z_i - y_i| \leq \delta$. Hence

$$\Pr[Z = y] \geq (1 - \delta)^N \geq 1 - \delta N.$$

By the boundedness of $\tilde{f}$ we have

$$\begin{aligned} \tilde{f}(z) &\geq (1 - \delta N) \cdot \tilde{f}(y) + 0 \geq \tilde{f}(y) - \delta N \\ \tilde{f}(z) &\leq 1 \cdot \tilde{f}(y) + \delta N \cdot 1 = \tilde{f}(y) + \delta N. \end{aligned}$$

□

# References

[1] Mark Bun, Robin Kothari, and Justin Thaler. The polynomial method strikes back: Tight quantum query bounds via dual polynomials. *arXiv preprint arXiv:1710.09079*, 2017.