DD2445 Complexity Theory	3 Nov, 2017 (@ KTH)
13. Communication complexity of composed functions	
Lecturer: Sagnik Mukhopadhyay	*Scribe: Sagnik Mukhopadhyay*

Last time

- **Funcion composition:** We want to show $\mathsf{D}^{\mathrm{cc}}(f \circ g) = \Omega(\mathsf{D}^{\mathrm{q}}(f) \times \mathsf{D}^{\mathrm{cc}}(g))$. This is not true for all g.
- (δ, h)-**hitting monochromatic rectangle distribution:** We say that IP_m has $(o(1), m(\frac{1}{2} - \varepsilon))$-hitting monochromatic rectangle-distributions.

This lecture

We show the following theorem:

Theorem 13.1 (Generalized simulation)**.** *Let $\varepsilon \in (0,1)$ and $\delta \in (0, \frac{1}{100})$ be real numbers, and let $h \geq 6/\varepsilon$ and $1 \leq n \leq 2^{h(1-\varepsilon)}$ be integers. Let $f : \{0,1\}^n \to \mathcal{Z}$ be a function and $g : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ be a function. If g has (δ, h)-hitting monochromatic rectangle-distributions then*

$$\mathsf{D}^{\mathrm{q}}(f) \leq \frac{4}{\varepsilon \cdot h} \cdot \mathsf{D}^{\mathrm{cc}}(f \circ g^n).$$

For a more complete proof than what we are going to do today, refer to [CKLM17].

☞ **Attention: Text like this implies caution! Please be careful.**

A few notations (refer to Figure 1)

- Consider a product set $\mathcal{A} = \mathcal{A}_1 \times \ldots \times \mathcal{A}_n$, for some natural number $n \geq 1$, where each $\mathcal{A}_i$ is a subset of $\{0,1\}^m$.
- Let $A \subseteq \mathcal{A}$ and $I = \{i_1 < i_2 < \cdots < i_k\} \subseteq [n]$, and $J = [n] \setminus I$.
- **Projection:** For any $a \in (\{0,1\}^m)^n$, we let $a_I = \langle a_{i_1}, a_{i_2}, \ldots, a_{i_k} \rangle$ be the projection of a onto the coordinates in I. Correspondingly, $A_I = \{a_I \mid a \in A\}$ is the projection of the entire set A onto I.
- For any $a' \in (\{0,1\}^m)^k$ and $a'' \in (\{0,1\}^m)^{n-k}$, we denote by $a' \times_I a''$ the n-tuple a such that $a_I = a'$ and $a_J = a''$.
- For $i \in [n]$ and a n-tuple a, $a_{\neq i}$ denotes $a_{[n]\setminus\{i\}}$, and similarly, $A_{\neq i}$ denotes $A_{[n]\setminus\{i\}}$.
- For $a' \in (\{0,1\}^m)^k$, we define the set of extensions $\mathsf{Ext}_A^J(a') = \{a'' \in (\{0,1\}^m)^{n-k} \mid a' \times_I a'' \in A\}$; we call those a'' *extensions* of a'.

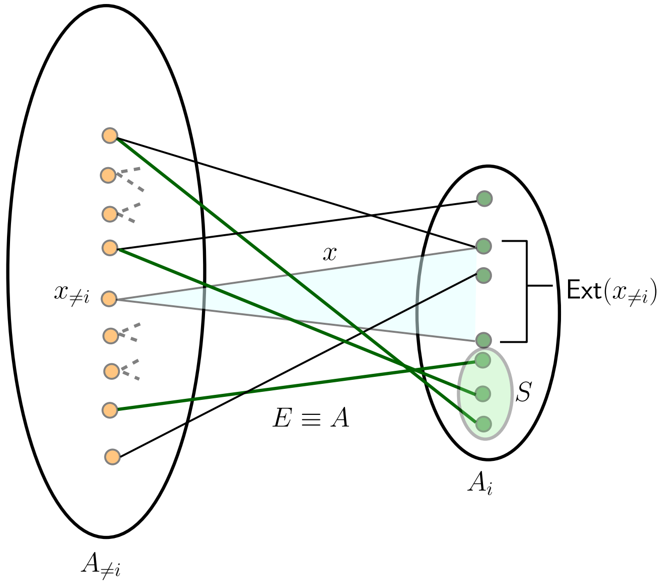

Figure 1: Projecions of set A

- For an integer n, a set $A \subseteq \mathcal{A}^n$ and a subset $S \subseteq \mathcal{A}$, the restriction of A to S at coordinate i is the set $A^{i,S} = \{a \in A \mid a_i \in S\}$.
- We write $A_I^{i,S}$ for the set $(A^{i,S})_I$ (i.e. we first restrict the i-th coordinate then project onto the coordinates in I).

13.1 The main idea

- We are given a protocol π for $f \circ g$ and input z for f. We will **simulate** a decision tree for f using π.
- Ideally we want to land on a leaf which has a pair (a, b) such that $g^n(a, b) = z$. This means that the label of the leaf is $f \circ g(a, b) = f(z)$.
- To trace such a root-to-leaf path, we will query bits of z from time to time.
- **Goal:** Devise a strategy to trace such a path.

13.2 Notion of the day: Thickness

Definition 13.2 (Aux graph, average and min-degrees)**.** *Let $n \geq 2$. For $i \in [n]$ and $A \subseteq \mathcal{A}^n$, the aux graph $G(A, i)$ is the bipartite graph with left side vertices A_i, right side vertices $A_{\neq i}$ and edges corresponding to the set A, i.e., (a', a'') is an edge iff $a' \times_{\{i\}} a'' \in A$. (See Figure 1.)*

We define the average degree of $G(A,i)$ *to be the average right-degree:*

$$d_{avg}(A,i) = \frac{|A|}{|A_{\neq i}|},$$

and the min-degree of $G(A,i)$*, to be the minimum right-degree:*

$$d_{min}(A,i) = \min_{a' \in A_{\neq i}} |\mathsf{Ext}(a')|.$$

Definition 13.3 (Thickness and average-thickness)**.** *For* $n \geq 2$ *and* $\tau, \varphi \in (0,1)$*, a set* $A \subseteq \mathcal{A}^n$ *is called* τ-thick *if*

$$d_{min}(A,i) \geq \tau \cdot |\mathcal{A}|$$

for all $i \in [n]$. ***Note, an empty set*** A ***is*** τ***-thick.***

Similarly, A *is called* φ-average-thick *if*

$$d_{avg}(A,i) \geq \varphi \cdot |\mathcal{A}|$$

for all $i \in [n]$.

☞ *For a rectangle* $A \times B \subseteq \mathcal{A}^n \times \mathcal{B}^n$*, we say that the rectangle* $A \times B$ *is* τ*-thick if both* A *and* B *are* τ*-thick. For* $n = 1$*, set* $A \subseteq \mathcal{A}$ *is* τ*-thick if* $|A| \geq \tau \cdot |\mathcal{A}|$.

13.3 High average degree

Lemma 13.4 (Average-thickness implies thickness)**.** *For any* $n \geq 2$*, if* $A \subseteq \mathcal{A}^n$ *is* φ*-average-thick, then for every* $\delta \in (0,1)$ *there is a* $\frac{\varphi}{2n}$*-thick subset* $A' \subseteq A$ *with* $|A'| \geq \frac{|A|}{2}$.

Proof idea. Go over every coordinate and discard vertices (and edges incident on them) which has extensions less than $\frac{\varphi}{2n} 2^m$. □

Consider the following algorithm. Set $\varphi = 4 \cdot 2^{-\varepsilon h}$ and $\tau = 2^{-h}$.

Algorithm 1 Decision-tree procedure assuming high average degree

Set v to be the root of the protocol tree for Π, $I = [n]$, $A = \mathcal{A}^n$ and $B = \mathcal{B}^n$.
while v is not a leaf **do**
  if A_I and B_I are both φ-average-thick **then**
    Let v_0, v_1 be the children of v.
    Choose $c \in \{0,1\}$ for which there is $A' \times B' \subseteq (A \times B) \cap R_{v_c}$ such that
      (1) $|A'_I \times B'_I| \geq \frac{1}{4}|A_I \times B_I|$
      (2) $A'_I \times B'_I$ is τ-thick. ▷ Using Lemma 13.4
    Update $A = A'$, $B = B'$ and $v = v_c$.
Output $f \circ g(A \times B)$.

Alice communicates at node v.

- Let A_0 be inputs from A on which Alice sends 0 at node v and $A_1 = A \setminus A_0$. We can pick $c \in \{0, 1\}$ such that $|A_c| \geq |A|/2$. Set $A'' = A_i$. **Since A is φ-average-thick, A'' is $\varphi/2$-average-thick.**
- Using Lemma 13.4 on A'', we can find a subset A' of A'' such that A' is $\frac{\varphi}{4 \cdot n}$-thick and $|A'| \geq |A''|/2$. Since $\varphi = 4 \cdot 2^{-\varepsilon h}$ and $n \leq 2^{h(1-\varepsilon)}$, the set A'_I will be 2^{-h}-thick, i.e. τ-thick. Setting $B' = B$, the rectangle $A' \times B'$ satisfies properties from lines 6–7.

Bob communicated at node v. A similar argument holds when Bob communicates at node v.

In the end, they are in a rectangle $A \times B$ which is τ-thick. Now we use the following lemma.

Lemma 13.5. *Let $n, h \geq 1$ be integers and $\delta, \tau \in (0, 1)$ be reals, where $\tau \geq 2^{-h}$.*

1. *Consider a function $g : \mathcal{A} \times \mathcal{B} \to \{0, 1\}$ which has (δ, h)-hitting monochromatic rectangle-distributions.*
2. *Let $A \times B \subseteq \mathcal{A}^n \times \mathcal{B}^n$ be a τ-thick non-empty rectangle.*

Then for every $z \in \{0, 1\}^n$ there is some $(a, b) \in A \times B$ with $g^n(a, b) = z$.

In particular, there is a pair $(a, b) \in A \times B$ such that $g^m(a, b)$ is the input z. So the protocol is correct. But it has not queried anything so far. **What is wrong then?**

13.4 Low average degree

The point is, the high average degree may not be mainatained though out the execution of Algorithm 1 (The **if** condition at line 3 may fail from time to time). When it drops, we have to query z. Consider the following algorithm.

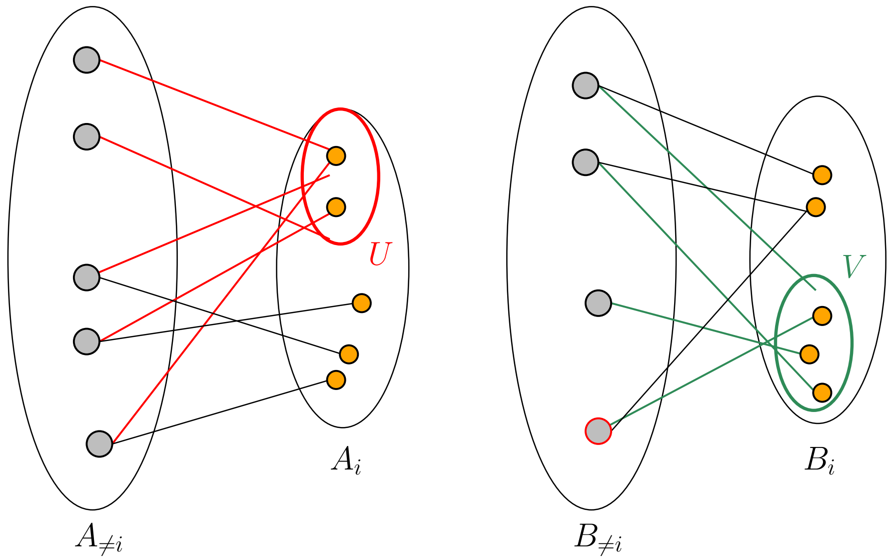

Figure 2: Projecions lemma

Algorithm 2 Query strategy

if $d_{\text{avg}}(A_I, j) < \varphi|\mathcal{A}|$ for some $j \in [|I|]$ **then**
  Query z_i, where i is the j-th (smallest) element of I.
  Let $U \times V$ be a z_i-monochromatic rectangle of g such that
    (1) $A^{i,U}_{I\setminus\{i\}} \times B^{i,V}_{I\setminus\{i\}}$ is τ-thick,
    (2) $\alpha^{i,U}_{I\setminus\{i\}} \geq \frac{1}{\varphi}(1-3\delta)\alpha$,
    (3) $\beta^{i,V}_{I\setminus\{i\}} \geq (1-3\delta)\beta$, ▷ Using Lemma 13.6
  Update $A = A^{i,U}, B = B^{i,V}$ and $I = I \setminus \{i\}$.
else if $d_{\text{avg}}(B_I, j) < \varphi|\mathcal{B}|$ for some $j \in [|I|]$ **then**
  Query z_i, where i is the j-th (smallest) element of I.
  Let $U \times V$ be a z_i-monochromatic rectangle of g such that
    (1) $A^{i,U}_{I\setminus\{i\}} \times B^{i,V}_{I\setminus\{i\}}$ is τ-thick,
    (2) $\alpha^{i,U}_{I\setminus\{i\}} \geq (1-3\delta)\alpha$,
    (3) $\beta^{i,V}_{I\setminus\{i\}} \geq \frac{1}{\varphi}(1-3\delta)\beta$, ▷ Using Lemma 13.6
  Update $A = A^{i,U}, B = B^{i,V}$ and $I = I \setminus \{i\}$.

Lemma 13.6. *Let $h \geq 1$, $n \geq 2$ and $i \in [n]$ be integers and $\delta, \tau, \varphi \in (0,1)$ be reals, where $\tau \geq 2^{-h}$.*

(a1) Consider a function $g : \mathcal{A} \times \mathcal{B} \to \{0,1\}$ which has (δ, h)-hitting monochromatic rectangle-distributions.

(a2) Suppose $A \times B \subseteq \mathcal{A}^n \times \mathcal{B}^n$ is a non-empty rectangle which is τ-thick.

(a3) Suppose also that $d_{avg}(A, i) \leq \varphi \cdot |\mathcal{A}|$.

Then for any $c \in \{0,1\}$, there is a c-monochromatic rectangle $U \times V \subseteq \mathcal{A} \times \mathcal{B}$ such that

(b1) $A^{i,U}_{\neq i}$ *and* $B^{i,V}_{\neq i}$ *is τ-thick,*

(b2) $\alpha^{i,U}_{\neq i} \geq \frac{1}{\varphi}(1 - 3\delta)\alpha$,

(b3) $\beta^{i,V}_{\neq i} \geq (1 - 3\delta)\beta$,

where $\alpha = |A|/|\mathcal{A}|^n$, $\beta = |B|/|\mathcal{B}|^n$, $\alpha^{i,U}_{\neq i} = |A^{i,U}_{\neq i}|/|\mathcal{A}|^{n-1}$ *and* $\beta = |B^{i,U}_{\neq i}|/|\mathcal{B}|^{n-1}$.

The constant 3 in the statement may be replaced by any value greater than 2, so the lemma is still meaningful for δ arbitrarily close to 1/2.

13.5 Putting everything together

Algorithm 3 Decision-tree procedure

Require: $z \in \{0,1\}^n$
Ensure: $f(z)$
1: Set v to be the root of the protocol tree for Π, $I = [n]$, $A = \mathcal{A}^n$ and $B = \mathcal{B}^n$.
2: **while** v is not a leaf **do**
3:     **if** A_I and B_I are both φ-average-thick **then**
4:         Run Algorithm 1.
5:     **else**
6:         Run Algorithm 2
7: Output $f \circ g^n(A \times B)$.

Correctness.

- The algorithm maintains an invariant that $A_I \times B_I$ is τ-thick. This invariant is trivially true at the beginning.

- If both A_I and B_I are φ-average-thick, the algorithm finds sets A' and B' on line 4 using Lemma 13.4.

- If A_I is not φ-average-thick, the existence of $U \times V$ at line 6 is guaranteed by Lemma 13.6. Similarly in the case when B_I is not φ-average-thick.

We argue that $f(A \times B)$ at the termination of Algorithm 3 is the correct output. Given an input $z \in \{0,1\}^n$, whenever the algorithm queries any z_i, the algorithm makes sure that all the input pairs (x, y) in the rectangle $A \times B$ are such that $g(x_i, y_i) = z_i$ — because $U \times V$ is always a z_i-monochromatic rectangle of g. At the termination of the algorithm, I is the set of i such that z_i was not queried by the algorithm. As $n > 4C/\varepsilon h$, I is non-empty. Since $A_I \times B_I$ is τ-thick, it follows from Lemma 13.5 that $A \times B$ contains some input pair (x, y) such that $g^{|I|}(x_I, y_I) = z_I$, and so $g^n(x, y) = z$. Since Π is correct, it must follow that $f(z) = f \circ g^n(A \times B)$. This concludes the proof of correctness.

Number of queries Next we argue that the number of queries made by Algorithm 3 is at most $5C/\varepsilon h$.

- In the first part of the **while** loop (line 4), the density of the current $A_I \times B_I$ drops by a factor 4 in each iteration. There are at most C such iterations, hence this density can drop by a factor of at most $4^{-C} = 2^{-2C}$.

- For each query that the algorithm makes, the density of the current $A_I \times B_I$ increases by a factor of at least $(1-3\delta)^2/\varphi \geq \frac{1}{2\varphi} \geq 2^{\varepsilon h - 3}$ **(here we use the fact that** $\delta \leq 1/100$**)**.

Since the density can be at most one, the number of queries is upper bounded by

$$\frac{2C}{\varepsilon h - 3} \leq \frac{4C}{\varepsilon h}, \qquad \text{when } h \geq 6/\varepsilon.$$

References

[CKLM17] Arkadev Chattopadhyay, Michal Koucký, Bruno Loff, and Sagnik Mukhopadhyay. Simulation theorems via pseudorandom properties. *CoRR*, abs/1704.06807, 2017.

Appendix: Missed proofs

13.5.1 Proof of Lemma 13.5

Lemma 13.7. *Let $n \geq 2$ be an integer, $i \in [n]$, $A \subseteq \mathcal{A}^n$ be a τ-thick set, and $S \subseteq \mathcal{A}$. The set $A_{\neq i}^{i,S}$ is τ-thick. $A_{\neq i}^{i,S}$ is empty iff $S \cap A_i$ is empty.*

Lemma 13.5 follows from repeated use of Lemma 13.7. Fix arbitrary $z \in \{0,1\}^n$. Set $A^{(1)} = A$ and $B^{(1)} = B$. We proceed in rounds $i = 1, \ldots, n-1$ maintaining a τ-thick rectangle $A^{(i)} \times B^{(i)} \subseteq \mathcal{A}^{n-i+1} \times \mathcal{B}^{n-i+1}$. If we pick $U_i \times V_i$ from σ_{z_i}, then the rectangle $(A^{(i)})_{\{i\}} \cap U_i \times (B^{(i)})_{\{i\}} \cap V_i$ will be non-empty with probability $\geq 1-\delta > 0$ (because σ_{z_i} is a (δ, h)-hitting rectangle-distribution and $\tau \geq 2^{-h}$). Fix such U_i and V_i. Set a_i to an arbitrary string in $(A^{(i)})_{\{i\}} \cap U_i$, and b_i to an arbitrary string in $(B^{(i)})_{\{i\}} \cap B_i$. Set $A^{(i+1)} = (A^{(i)})_{\neq i}^{i,\{a_i\}}$, $B^{(i+1)} = (B^{(i)})_{\neq i}^{i,\{b_i\}}$, and proceed for the next round. By Lemma 13.7, $A^{(i+1)} \times B^{(i+1)}$ is τ-thick.

Eventually, we are left with a rectangle $A^{(n)} \times B^{(n)} \subseteq \mathcal{A} \times \mathcal{B}$ where both $A^{(n)}$ and $B^{(n)}$ are τ-thick (and non-empty). Again with probability $1-\delta > 0$, the z_n-monochromatic rectangle $U_n \times V_n$ chosen from σ_{z_n} will intersect $A^{(n)} \times B^{(n)}$. We again set a_n and b_n to come from the intersection, and set $a = \langle a_1, a_2, \ldots, a_n \rangle$ and $b = \langle b_1, b_2, \ldots, b_n \rangle$.

13.5.2 Proof of Lemma 13.6

Fix $c \in \{0,1\}$. Consider a matrix M where rows correspond to strings $a \in A_{\neq i}$, and columns correspond to rectangles $R = U \times V$ in the support of σ_c. Set each entry $M(a,R)$ to 1 if $U \cap \mathsf{Ext}_A^{\{i\}}(a) \neq \emptyset$, and set it to 0 otherwise.

For each $a \in A_{\neq i}$, $|\mathsf{Ext}_A^{\{i\}}(a)| \geq \tau|\mathcal{A}|$, and because σ_c is a (δ, h)-hitting rectangle-distribution and $\tau \geq 2^{-h}$, we know that if we pick a column R according to σ_c, then $M(a,R) = 1$ with probability $\geq 1-\delta$. So the probability that $M(a,R) = 1$ over uniform a and σ_c-chosen R is $\geq 1-\delta$.

Call a column of M *A-good* if $M(a,R) = 1$ for at least $1-3\delta$ fraction of the rows a. Now it must be the case that the A-good columns have strictly more than $1/2$ of the σ_c-mass. Otherwise the probability that $M(a,R) = 1$ would be $< 1-\delta$.

A similar argument also holds for Bob's set $B_{\neq i}$. Hence, there is a c-monochromatic rectangle $R = U \times V$ whose column is both A-good and B-good in their respective matrices. This is our desired rectangle R.

We know: $|A_{\neq i}^{i,V}| \geq (1-3\delta)|A_{\neq i}|$ and $|B_{\neq i}^{i,V}| \geq (1-3\delta)|B_{\neq i}|$. Since $|B_{\neq i}| \geq |B|/|\mathcal{B}|$, we obtain $|B_{\neq i}^{i,V}|/|\mathcal{B}|^{n-1} \geq (1-3\delta)|B_{\neq i}|/|\mathcal{B}|^{n-1} \geq (1-3\delta)\beta$. Because $|A|/|A_{\neq i}| \leq \varphi|\mathcal{A}|$, we get

$$\frac{|A_{\neq i}|}{|\mathcal{A}|^{(n-1)}} \geq \frac{1}{\varphi} \cdot \frac{|A|}{|\mathcal{A}|^n} = \frac{\alpha}{\varphi}.$$

Combined with the lower bound on $|A_{\neq i}^{i,V}|$ we obtain $|A_{\neq i}^{i,U}|/|\mathcal{A}|^{n-1} \geq (1-3\delta)\alpha/\varphi$. The thickness of $A_{\neq i}^{i,U}$ and $B_{\neq i}^{i,V}$ follows from Lemma 13.7.