Hardness of Approximation

Before: LCS cannot be computed in time $O(n^{2-\delta})$

Open Question: Can we compute a $(1+\varepsilon)$-approx in time $O(n^{2-\delta})$? Can we show fine-grained lower bounds?

Generally proving good lower bounds for approximation problems is often hard

Today: Some SETH lower bounds for an approximation prob.:

Maximum Inner Product (MaxIP)

Input: Sets of n vectors $X, Y \subseteq \{0,1\}^d$

Output: $\max_{x \in X, y \in Y} \langle x, y \rangle$

$\langle x,y \rangle = \sum_{i=1}^{d} x[i] \cdot y[i]$

Can be solved in time $O(n^2)$

Lemma: SETH $\Rightarrow$ MaxIP is not in time $O(n^{2-\varepsilon} \operatorname{poly}(d))$ $(\forall \varepsilon > 0)$.

Proof: Reduce from OV (with dimension $d = c \log n$):

x: $\boxed{0 \mid 1 \mid \cdots \mid}$ $\qquad$ y: $\boxed{0 \mid 1 \mid \cdots \mid}$

x': $\boxed{11 \mid 10 \mid \cdots \mid}$ $\qquad$ y': $\boxed{10 \mid 01 \mid \cdots \mid}$

$\Rightarrow \langle x', y' \rangle = d - \langle x, y \rangle$

$\Rightarrow$ Distinguish whether max. inner prod. is $= d$ or $\leq d-1$ $\square$

α - Approximate MaxIP

Output: Value $\tilde{v}$ s.t. $\frac{1}{\alpha} \cdot \max_{\substack{x \in X \\ y \in Y}} \langle x, y \rangle \leq \tilde{v} \leq \max_{\substack{x \in X \\ y \in Y}} \langle x, y \rangle$

Does this reduction also imply that it is hard to approximate MaxIP? No!

Want: Gap-Introducing Reduction

Transform $x \rightsquigarrow x'$ and $y \rightsquigarrow y'$ such that:

- $\langle x, y \rangle = 0 \Rightarrow \langle x', y' \rangle = d$
- $\langle x, y \rangle \neq 0 \Rightarrow \langle x', y' \rangle < \frac{d}{\alpha}$.

Similar to PCP Theorems

But: "Distributed", i.e. x and y see only half of the variable assignments

Solution: Communication Complexity

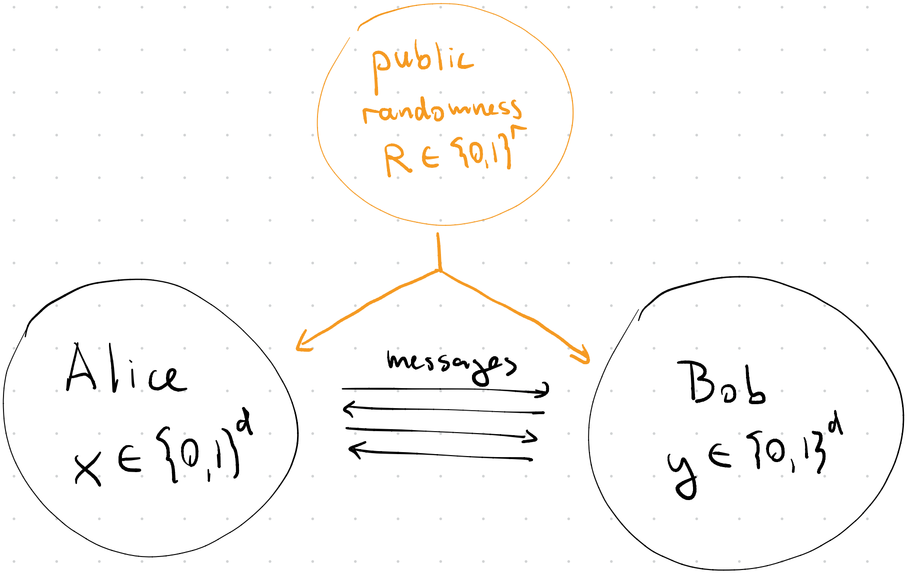
Theorem: [Abboud, Rubinstein, Williams '17]

SETH $\Rightarrow$ 100-Approximate MaxIP is not in time $O(n^{2-\varepsilon} \operatorname{poly}(d))$ for all $\varepsilon > 0$.

Remark: The constant $\alpha = 100$ is arbitrary

Improvements: [Rubinstein '18] [Chen, Williams '18] [Chen '18]

Communication Complexity



Goal: Function $f: \{0,1\}^d \times \{0,1\}^d \to \{0,1\}$

Alice and Bob communicate to learn $f(x,y)$

Comments:

- They agree on some protocol in advance
- Each message contains one bit
- They trust each other
- For randomized protocols we assume that Alice and Bob have access to a shared (public) source of randomness
- (Private randomness is also studied)

Example 1: Equality

$$Eq(x,y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{ow.} \end{cases}$$

Deterministic: $\Omega(d)$ messages

Randomized: $O(1)$ messages

Protocol:

- Choose random vector $R \in \{0,1\}^r$
- Bob sends $\langle y, R\rangle \pmod 2$ to Alice
- Alice accepts if $\langle x, R\rangle \equiv \langle y, R\rangle \pmod 2$
- Repeat to boost probability

Example 2: Disjointness (aka Orthogonality)

$$Disj(x,y) = \begin{cases} 1 & \text{if } \langle x, y\rangle = 0 \\ 0 & \text{ow} \end{cases}$$

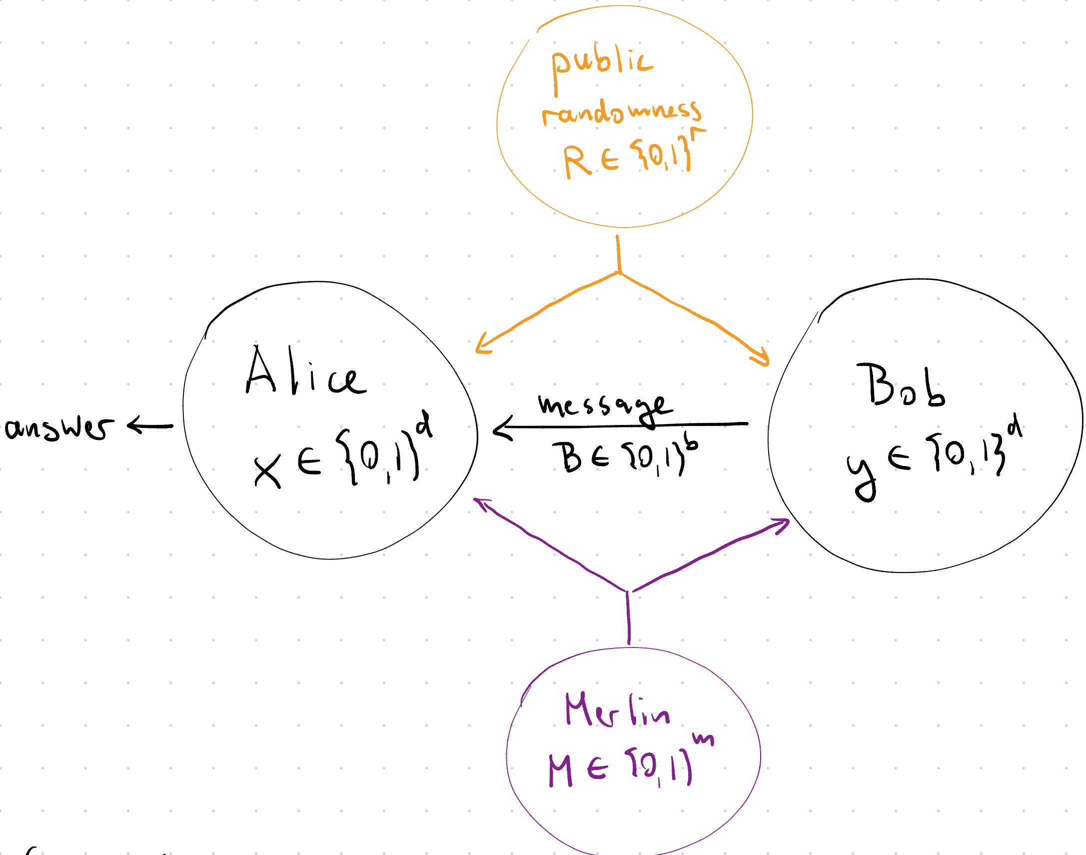
Clearly related to OV!

Deterministic: $\Omega(d)$ messages

Randomized: $\Omega(d)$ messages

With randomization and nondeterminism: $O(\sqrt{d})$ messages

Communication Setup



Comments:

- Alice and Bob receive shared randomness $R \in \{0,1\}^r$
- Alice and Bob receive shared nondeterministic untrusted advice $M \in \{0,1\}^m$ from Merlin
- Merlin knows x and y but not the randomness
- Bob sends one message $B \in \{0,1\}^b$ to Alice
- Alice reports the answer

Theorem: [Aaronson, Wigderson '09]

There is a protocol for Disj with $r, m, b \leq \tilde{O}(\sqrt{d})$ such that:

- Completeness:

  $\langle x, y\rangle = 0 \Rightarrow \exists M \in \{0,1\}^m : \underset{R \in \{0,1\}^r}{\mathbb{P}}(\text{protocol accepts } x, y, M, R) = 1$

- Soundness:

  $\langle x, y\rangle \neq 0 \Rightarrow \forall M \in \{0,1\}^m : \underset{R \in \{0,1\}^r}{\mathbb{P}}(\text{protocol accepts } x, y, M, R) < \frac{1}{100}$

Moreover, we can compute Alice and Bob's behavior in time poly(d)

Proof of the Reduction

Reduce from OV instance $X, Y \subseteq \{0,1\}^d$ (with $d = c \log n$)

For all $x \in X, y \in Y$ construct $x_{M,R}, y_{M,R} \in \{0,1\}^{2^b}$:

$$y_{M,R}[B] := \begin{cases} 1 & \text{if Bob sends message } B \text{ on input } y, M, R \\ 0 & \text{ow.} \end{cases}$$

$$x_{M,R}[B] := \begin{cases} 1 & \text{if Alice accepts } x, M, R, B \\ 0 & \text{ow.} \end{cases}$$

Observation:

$$\langle x_{M,R}, y_{M,R} \rangle = \begin{cases} 1 & \text{if protocol accepts } x, y, M, R \\ 0 & \text{ow.} \end{cases}$$

For all $x \in X, y \in Y$ construct $x_M, y_M \in \{0,1\}^{2^{b+r}}$:

$x_M :=$ concatenate $x_{M,R}$ for all $R \in \{0,1\}^r$

$y_M :=$ concatenate $y_{M,R}$ for all $R \in \{0,1\}^r$

Observation:

$$\langle x_M, y_M \rangle = 2^r \cdot \mathbb{P}_{R \in \{0,1\}^r} \left(\text{protocol accepts } x, y, M, R \right)$$

Construct

$$X_M = \{x_M : x \in X\}$$
$$Y_M = \{y_M : y \in Y\}$$

Observation: Completeness

YES instance

$\Rightarrow \exists x \in X, y \in Y: \langle x, y \rangle = 0$

$\Rightarrow \exists M \in \{0,1\}^m: \mathbb{P}_{R \in \{0,1\}^r}(\text{protocol accepts } x, y, M, R) = 1$

$\Rightarrow \langle x_M, y_M \rangle = 2^r$

$\Rightarrow \max_{M} \max_{\substack{x' \in X_M \\ y' \in Y_M}} \langle x', y' \rangle \geq 2^r$

Observation: Soundness

NO instance

$\Rightarrow \forall x \in X, y \in Y: \langle x, y \rangle \neq 0$

$\Rightarrow \forall M \in \{0,1\}^m: \mathbb{P}_{R \in \{0,1\}^r}(\text{protocol accepts } x, y, M, R) < \frac{1}{100}$

$\Rightarrow \langle x_M, y_M \rangle < 2^r \cdot \frac{1}{100}$

$\Rightarrow \max_{M} \max_{\substack{x' \in X_M \\ y' \in Y_M}} \langle x', y' \rangle < 2^r \cdot \frac{1}{100}$

Conclusion: Can solve the OV instance by 2^m calls to 100-approximate Max IP.

Running Time

If MaxIP is in time $O(n^{2-\varepsilon}\, poly(d'))$

$\Rightarrow$ OV is in time

$$
\begin{aligned}
& O(2^{m} \cdot n^{2-\varepsilon} \cdot poly(2^{b+r})) \\
&= O(n^{2-\varepsilon} \cdot 2^{O(m+r+b)}) \\
&= O(n^{2-\varepsilon} \cdot 2^{\tilde{O}(\sqrt{d'})}) \\
&= O(n^{2-\varepsilon} \cdot 2^{\tilde{O}(\sqrt{\log n'})}) \\
&= O(n^{2-\varepsilon+o(1)}) \\
&= O(n^{2-\varepsilon/2})
\end{aligned}
$$

$m, r, b \leq \tilde{O}(\sqrt{d'})$

$\square$

Intermezzo on Algebra

Let $\mathbb{F}$ be an arbitrary field.

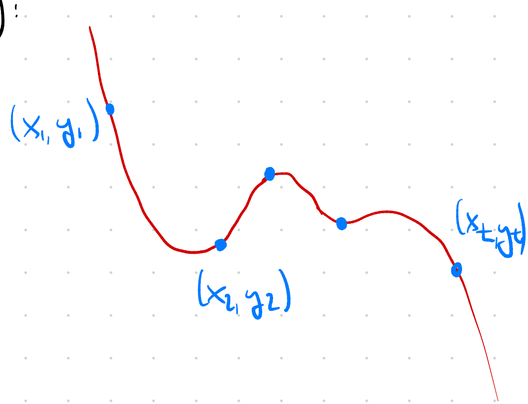
Later we choose an appropriate finite field $\mathbb{F}$

Fact 1 (Roots): Every degree-t polynomial p has at most t roots. (I.e. points x such that $p(x)=0$)

Fact 2 (Polynomial Interpolation):

Given distinct $x_1, \dots, x_t \in \mathbb{F}$ and arbitrary $y_1, \dots, y_t \in \mathbb{F}$, there is a degree-$t$ polynomial p such that:

$$p(x_i) = y_i \quad \forall i \in [t]$$



Proof:

$$p(x) = \sum_{i \in [t]} y_i \cdot \underbrace{\prod_{\substack{j \in [t] \\ j \neq i}} \frac{x - x_j}{x_i - x_j}}_{\substack{=1 \text{ if } x = x_i \\ =0 \text{ if } x = x_j \text{ for } j \neq i}}$$

$\square$

Proof of the Protocol

Let $\mathbb{F} = \mathbb{F}_p$ for some prime $p \in [200d, 400d]$

Let $t = \sqrt{d}$ (assume for simplicity that d is square)

Interpolate degree-t polynomials $p_1, \dots, p_t, q_1, \dots, q_t$ with

- $p_i(k) = x[it+k]$
- $q_i(k) = y[it+k]$

$$\underbrace{x[1] \cdots x[t]}_{p_1} \;\cdots\; \underbrace{x[d-t+1] \cdots x[d]}_{p_t}$$

Let $\phi(x) = \sum_{i \in [t]} p_i(x) \cdot q_i(x)$

<u>Observation</u>: $\langle x, y \rangle = \sum_{k \in [t]} \phi(k)$

<u>Observation</u>: ϕ is a degree-$2t$ polynomial

<u>Protocol</u>:

- <u>Randomness</u>: Random field element $R \in \mathbb{F}_p$
- <u>Merlin</u>: Is intended to send the polynomial $M = \phi$
- <u>Bob</u>: Sends $q_1(R), \dots, q_t(R)$ to Alice
- <u>Alice</u>:
  - Evaluates $\phi(R) = \sum_{i \in [t]} p_i(R) \cdot q_i(R)$
  - Accepts if $\underbrace{M(R) = \phi(R)}_{\text{(i) tests if Merlin is truthful}}$ and $\underbrace{\sum_{k \in [t]} M(k) = 0}_{\text{(ii) tests if } \langle x, y \rangle = 0}$

Completeness: Assume $\langle x, y \rangle = 0$

Merlin truthfully sends $M = \phi$ $\Longrightarrow$ (i) succeeds

$$\Longrightarrow \sum_{k \in [t]} M(k) = \sum_{k \in [t]} \phi(k) = \langle x, y \rangle = 0 \quad \Longrightarrow \text{(ii) succeeds}$$

Soundness: Assume $\langle x, y \rangle \neq 0$

- If Merlin truthfully sends $M = \phi$

$$\Longrightarrow \sum_{k \in [t]} M(k) = \sum_{k \in [t]} \phi(k) = \langle x, y \rangle \neq 0 \quad \Longrightarrow \text{(ii) fails}$$

- If Merlin cheats and sends some other degree-$2t$ polynomial $M \neq \phi$:

$$\begin{aligned}
&\mathbb{P}(\text{(i) succeeds}) \\
&= \mathbb{P}_{R \in \mathbb{F}_p}\left(M(R) = \phi(R) \right) \\
&= \mathbb{P}_{R \in \mathbb{F}_p}\left(\underbrace{(M - \phi)}_{\text{degree } 2t}(R) = 0 \right) \\
&\overset{\text{Fact 1}}{\leq} \frac{2t}{p} < \frac{2d}{200d} = \frac{1}{100}
\end{aligned}$$

Parameters:

- $r = \lceil \log p \rceil = O(\log d)$
- $m = \lceil \log p \rceil \cdot 2t = O(\sqrt{d} \log d)$
- $b = \lceil \log p \rceil \cdot t = O(\sqrt{d} \log d)$ $\square$