Equality Alone Does not Simulate Randomness

Marc Vinyals

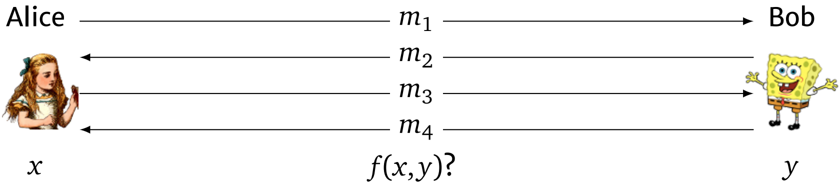
Tata Institute of Fundamental Research
Mumbai, India

Joint work with Arkadev Chattopadhyay and Shachar Lovett

34th Computational Complexity Conference

Deterministic Communication

P



Deterministic Communication P

Alice

x

$6 \mid x + y?$

Bob

y

Deterministic Communication P

Alice $\xrightarrow{x \pmod 2}$ Bob

x $6 \mid x + y?$ y

Deterministic Communication

P

Alice $\xrightarrow{\quad x \pmod 2 \quad}$ Bob

$\xleftarrow{\quad \text{No / Maybe}, y \pmod 3 \quad}$

x $\qquad 6 \mid x+y?$ $\qquad y$

Deterministic Communication

P

Alice $\xrightarrow{\quad x \pmod 2 \quad}$ Bob

$\xleftarrow{\quad \text{No / Maybe, } y \pmod 3 \quad}$

$\xrightarrow{\quad \text{Yes / No} \quad}$

x

$6 \mid x+y$?

y

Deterministic Communication P

Alice

x

$x = y?$

Bob

y

Deterministic Communication P

Alice $\xrightarrow{\quad x \quad}$ Bob

$\xleftarrow{\quad \text{Yes / No} \quad}$

x $\qquad$ $x = y?$ $\qquad$ y

- Equality needs $n + 1$ bits.

Randomized Communication BPP

Alice

x, r

Bob

y, r

$$\Pr_r[\text{error}] < 1/3$$

Randomized Communication BPP

Alice

x, r

Sample p among first $\Theta(n)$ primes

$x \pmod{p}$ →

← Yes / No

$x = y$?

Bob

y, r

Randomized Communication BPP

Alice

x, r

Bob

y, r

- Can solve equality with $O(\log n)$ bits.

Randomized Communication BPP

Alice

x, r

Bob

y, r

- Can solve equality with $O(1)$ bits.

Randomized Communication BPP

Alice

x, r

Bob

y, r

- Can solve equality with $\mathrm{O}(1)$ bits.
- Greater-than
  - $x \geq y$?
  - $\mathrm{O}(\log n)$ bits.

Randomized Communication BPP

Alice

x, r

Bob

y, r

- Can solve equality with $O(1)$ bits.
- Greater-than
  - $x \geq y$?
  - $O(\log n)$ bits.
- Small-set disjointness
  - $x \cap y = \emptyset$?, promise $|x|, |y| \leq k$
  - $O(k)$ bits.

Randomized Communication BPP

Alice

x, r

Bob

y, r

- Can solve equality with $O(1)$ bits.
- Greater-than
  - $x \geq y$?
  - $O(\log n)$ bits.
- Small-set disjointness
  - $x \cap y = \emptyset$?, promise $|x|, |y| \leq k$
  - $O(k)$ bits.
- Hashing / Equality is enough to efficiently solve all of these.

Communication with EQ Oracle

P^{EQ}

[Babai, Frankl, Simon ’86]

Alice	Oracle	Bob
	$=$	
$x, \cancel{r}$		$y, \cancel{r}$

- Send $f(x),\ g(y)$ to oracle
- Both parties see answer
- Cost number of calls

Communication with EQ Oracle

P^{EQ}

[Babai, Frankl, Simon '86]

Alice —— $\sum 1/n^2$ ——→ Oracle ←—— $\pi^2/6$ —— Bob

$\boxed{=}$

$x, \cancel{r}$ $y, \cancel{r}$

- Send $f(x),\ g(y)$ to oracle
- Both parties see answer
- Cost number of calls

Communication with EQ Oracle

P^{EQ}

[Babai, Frankl, Simon ’86]

Alice $\xrightarrow{\sum 1/n^2}$ Oracle $\xleftarrow{\pi^2/6}$ Bob

Alice $\xleftarrow{1}$ Oracle $\xrightarrow{1}$ Bob

$=$

$x, \cancel{r}$

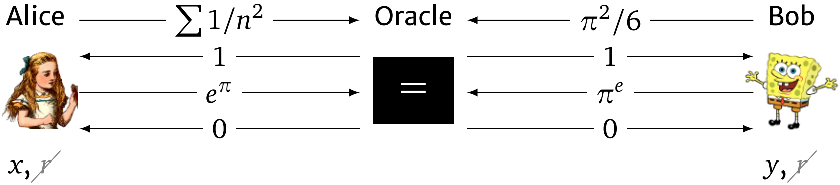
$y, \cancel{r}$

- Send $f(x),\ g(y)$ to oracle
- Both parties see answer
- Cost number of calls

Communication with EQ Oracle

P^{EQ}

[Babai, Frankl, Simon ’86]



- Send $f(x),\ g(y)$ to oracle
- Both parties see answer
- Cost number of calls

BPP vs P^{EQ}

Question

For every function, is P^{EQ} *cost* $\simeq$ BPP *cost?*

BPP vs P^{EQ}

Question

For every function, is P^{EQ} cost $\simeq$ BPP cost?

- Known false for partial functions
- e.g. $\mathrm{Maj}(x \oplus y)$, promise $x \oplus y$ has either $2n/3$ 0s or $2n/3$ 1s.

- 2-bit BPP protocol
  - Sample $i \in [n]$
  - Send x_i
  - Answer $x_i \oplus y_i$
- P^{EQ} cost $\Omega(n)$ [Papakonstantinou, Scheder, Song '14].

BPP vs P^{EQ}

Question

For every total function, is P^{EQ} *cost* $\simeq$ BPP *cost?*

- Known false for partial functions
- e.g. $\mathrm{Maj}(x \oplus y)$, promise $x \oplus y$ has either $2n/3$ 0s or $2n/3$ 1s.

BPP vs P^{EQ}

Question

For every total function, is P^{EQ} cost $\simeq$ BPP cost?

- Known false for partial functions
- e.g. $\mathrm{Maj}(x \oplus y)$, promise $x \oplus y$ has either $2n/3$ 0s or $2n/3$ 1s.

Our result: No.

Theorem

There is a total function with BPP cost $\mathrm{O}(\log n)$ and P^{EQ} cost $\Omega(n)$.

Integer Inner Product

Parameters t small constant, n growing, $N = 2^{n/t-1}$

Input t integers in $[-N, N]$

Alice $x = x_1, \ldots, x_t$

Bob $y = y_1, \ldots, y_t$

Output $\mathrm{IIP}(x,y) = [\![\langle x,y\rangle = 0]\!] = \begin{cases} 1 & \text{if } x_1 y_1 + \cdots + x_t y_t = 0 \\ 0 & \text{otherwise} \end{cases}$

Upper Bound

t small constant, n growing, $N = 2^{n/t-1}$
$\mathrm{IIP}(x,y) = [\![x_1y_1 + \cdots + x_ty_t = 0]\!]$

Protocol

- Sample p among first $\Theta(n)$ primes
- Send $x_1 \pmod p, \ldots, x_t \pmod p$
- Answer $\langle x,y\rangle \equiv 0 \pmod p$

Cost $t \log p = \mathrm{O}(\log n)$

Correct with probability $3/4$

Lower Bound

P^{GT}

Alice

x

Oracle

$\geq$

Bob

y

- Prove for P^{GT}.
- Can simulate EQ with 2 calls to GT.

Lower Bound

P^{GT}

Alice

x

Oracle

$\geq$

Bob

y

- Prove for P^{GT}.
- Can simulate EQ with 2 calls to GT.
- Cannot use BPP techniques.

Rectangle Partitions

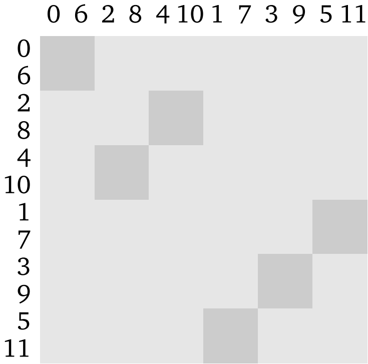
Alice

x

$6 \mid x+y$?

Bob

y

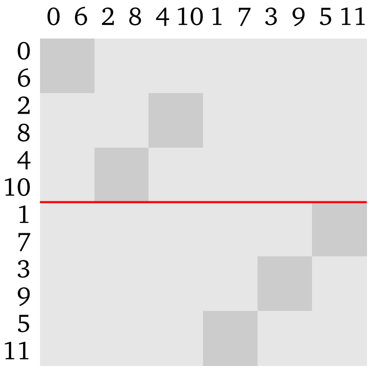


- Each bit splits inputs into 2 rectangles.
- After c bits have 2^c rectangles.

Rectangle Partitions

Alice —— $x \pmod 2$ ——→ Bob

x $\qquad 6 \mid x+y?$ $\qquad y$



- Each bit splits inputs into 2 rectangles.
- After c bits have 2^c rectangles.

Rectangle Partitions

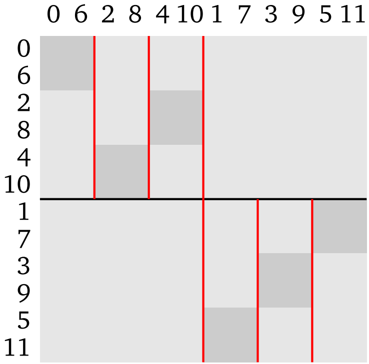
Alice $\xrightarrow{\quad x \pmod 2 \quad}$ Bob

Alice $\xleftarrow{\quad \text{No / Maybe, } y \pmod 3 \quad}$ Bob

x

$6 \mid x+y?$

y



- Each bit splits inputs into 2 rectangles.
- After c bits have 2^c rectangles.

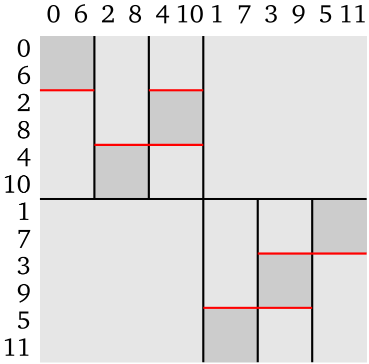
Rectangle Partitions

Alice ——— $x \pmod 2$ ———→ Bob

←——— No / Maybe, $y \pmod 3$ ———

——— Yes / No ———→

x $\quad 6 \mid x+y$? $\quad y$



- Each bit splits inputs into 2 rectangles.
- After c bits have 2^c rectangles.

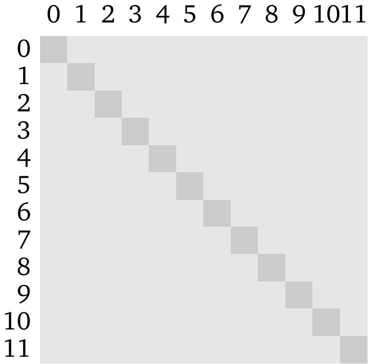
Rectangle Partitions

Alice

x

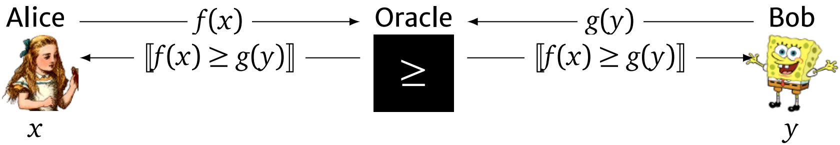
Bob

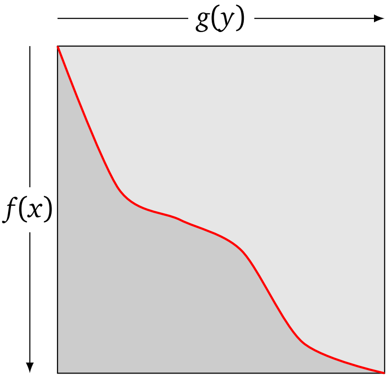
y



- Each bit splits inputs into 2 rectangles.
- After c bits have 2^c rectangles.
- Can show EQ requires 2^n rectangles.

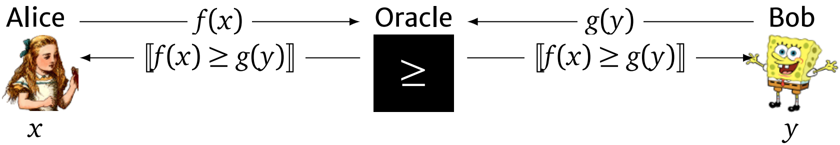
Triangle Partitions

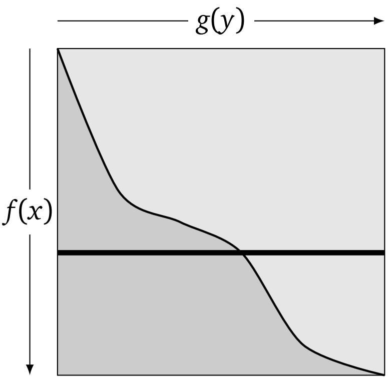




- Each call splits inputs into 2 triangles.

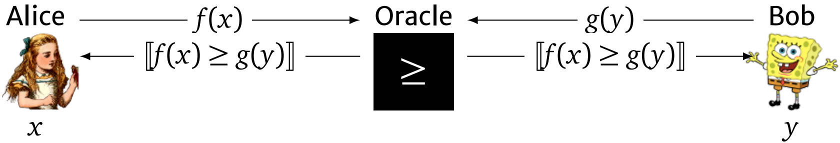
Triangle Partitions

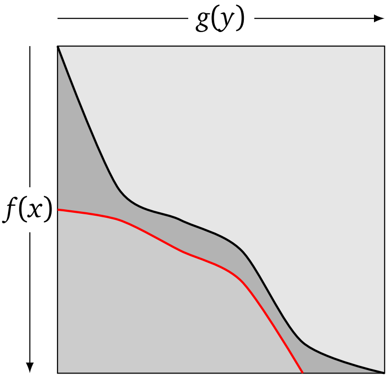




- Each call splits inputs into 2 triangles.

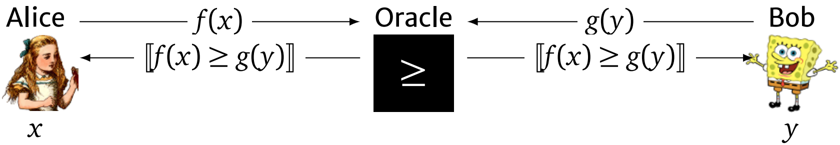
Triangle Partitions

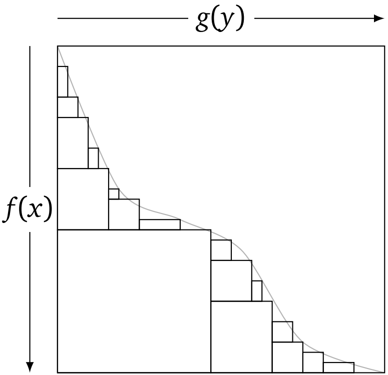




- Each call splits inputs into 2 triangles.
- After c calls have 2^c ??
- Intersections of triangles not triangles.
- Each call may use different order.

Rectangle Partitions of Triangle Partitions





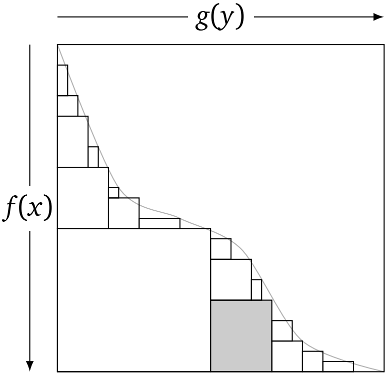
- Refine partition for free.

Rectangle Partitions of Triangle Partitions

Alice —— $f(x)$ ——→ Oracle ←—— $g(y)$ —— Bob

←—— $(x,y) \in R_{42}$ —— $\geq$ —— $(x,y) \in R_{42}$ ——→

x y



- Refine partition for free.

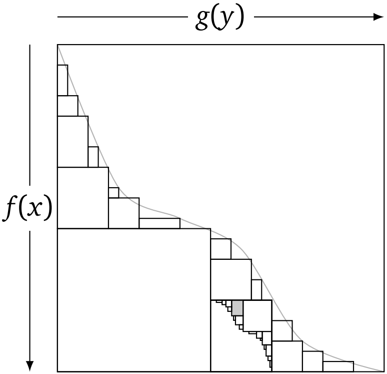
Rectangle Partitions of Triangle Partitions

Alice $\xrightarrow{f(x)}$ Oracle $\xleftarrow{g(y)}$ Bob

x

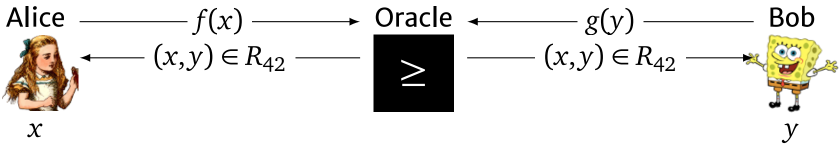
$\xleftarrow{(x,y) \in R_{42}}$ $\boxed{\geq}$ $\xrightarrow{(x,y) \in R_{42}}$

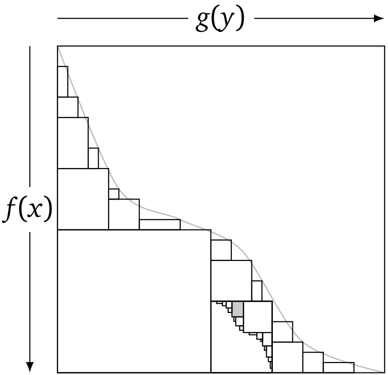
y



- Refine partition for free.
- Each call splits inputs into 2^n rectangles.
- After c calls have 2^{cn} rectangles.
- Useless?!

Rectangle Partitions of Triangle Partitions





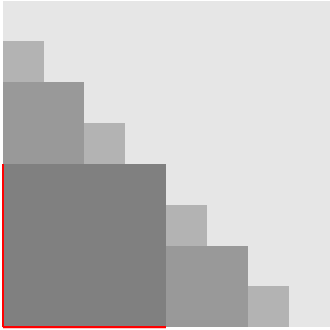
- Refine partition for free.
- Each call splits inputs into 2^n rectangles.
- After c calls have 2^{cn} rectangles.
- Useless?!
- Many of these rectangles are large. Can we exploit this?

Perimeter

Total perimeter $$\sum_{A\times B\in\mathcal{R}} |A| + |B|$$

Perimeter

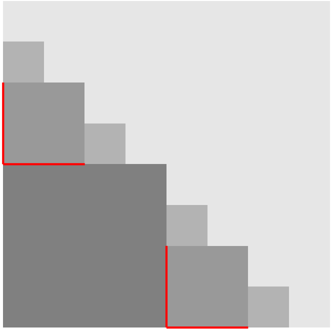
Total perimeter $\sum_{A \times B \in \mathcal{R}} |A| + |B|$



$2^n \cdot 2 \cdot 1/2$

Perimeter

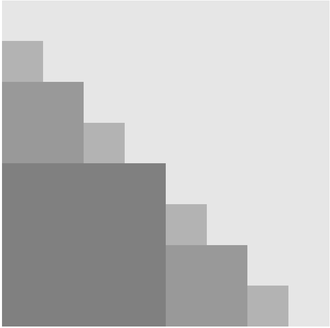
Total perimeter $$\sum_{A\times B\in\mathcal{R}} |A| + |B|$$



$$2^n \cdot (2\cdot 1/2 + 4\cdot 1/4)$$

Perimeter

Total perimeter $\sum_{A\times B\in\mathcal{R}} |A|+|B|$

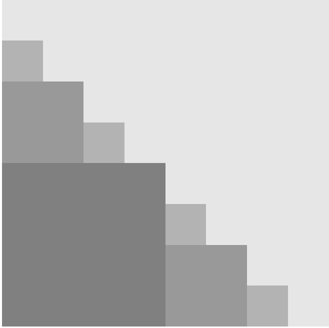


$$2^n(2\cdot 1/2+4\cdot 1/4+\cdots+2^n\cdot 2^{-n})=2^n\cdot n$$

Perimeter

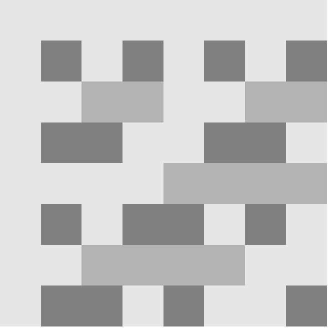
Total perimeter $\sum_{A \times B \in \mathcal{R}} |A| + |B|$

Greater-than



$2^n \cdot n$

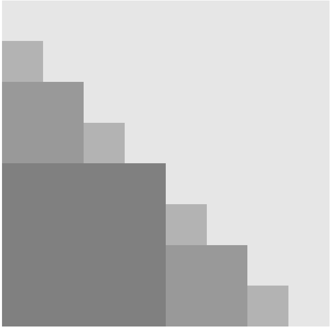
Inner product over $\mathbb{F}_2$



$(2^n - 1) \cdot (2^{n-1} + 1) \simeq 2^{2n-1}$

η-Area

Total η-area $$\sum_{A\times B\in\mathcal{R}} (|A||B|)^\eta$$ $1/2 < \eta < 1$



$$2^{2\eta n}(1\cdot(1/4)^\eta + 2\cdot(1/16)^\eta + \cdots + 2^{n-1}\cdot 2^{-2\eta n}) = 2^{2\eta n}\cdot q$$

Proof Sketch

Theorem

The P^{GT} *cost of* IIP_6 *is* $\Omega(n)$.

Proof Sketch

Theorem

The P^{GT} *cost of* IIP_6 *is* $\Omega(n/\log n)$.

Proof Sketch

Theorem

The P^{GT} *cost of* IIP_6 *is* $\Omega(n/\log n)$.

Claim Each call increases perimeter by factor n.
After c calls total perimeter $2^n \cdot n^c$.

Proof Sketch

Theorem

The P^{GT} *cost of* IIP_6 *is* $\Omega(n/\log n)$.

Claim Each call increases perimeter by factor n.
After c calls total perimeter $2^n \cdot n^c$.

Lemma

IIP_6 *has perimeter* $2^n \cdot \exp(\Omega(n))$.

Proof Sketch

Theorem

The P^{GT} *cost of* IIP_6 *is* $\Omega(n/\log n)$.

Claim Each call increases perimeter by factor n.
After c calls total perimeter $2^n \cdot n^c$.

Lemma

IIP_6 *has perimeter* $2^n \cdot \exp(\Omega(n))$.

Claim A function with 1-mass α and 1-rectangles of size at most β has perimeter $\alpha/\sqrt{\beta}$.

Proof Sketch

Theorem

The P^{GT} *cost of* IIP_6 *is* $\Omega(n/\log n)$.

Claim Each call increases perimeter by factor n.
After c calls total perimeter $2^n \cdot n^c$.

Lemma

IIP_6 *has perimeter* $2^n \cdot \exp(\Omega(n))$.

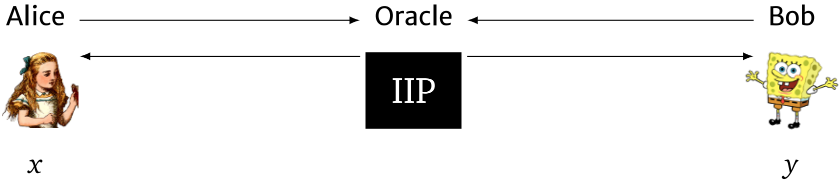
Claim A function with 1-mass α and 1-rectangles of size at most β has perimeter $\alpha/\sqrt{\beta}$.

Claim IIP_6 has 1-mass at least $\geq 2^{2n}/N^2$.

Claim IIP_6 has all 1-rectangles of size at most N^6.

Hierarchy

- What if we had an IIP oracle?



Hierarchy

- What if we had an IIP oracle?

Alice → Oracle ← Bob

IIP

x y

Theorem

For each t exists t' such that $\mathsf{P}^{\mathsf{IIP}_t}$ cost of $\mathrm{IIP}_{t'}$ is $\Omega(n)$

$$\mathsf{P}^{\mathsf{EQ}} \subsetneq \mathsf{P}^{\mathsf{IIP}_{t_1}} \subsetneq \mathsf{P}^{\mathsf{IIP}_{t_2}} \subsetneq \cdots \subsetneq \mathsf{BPP}$$

Take Home

Remarks

- $P^{EQ} \neq BPP$ even for total functions
- Hierarchy $P^{EQ} \subsetneq P^{IIP_{t_1}} \subsetneq P^{IIP_{t_2}} \subsetneq \cdots \subsetneq BPP$

Take Home

Remarks

- $\mathsf{P}^{\mathsf{EQ}} \neq \mathsf{BPP}$ even for total functions
- Hierarchy $\mathsf{P}^{\mathsf{EQ}} \subsetneq \mathsf{P}^{\mathsf{IIP}_{t_1}} \subsetneq \mathsf{P}^{\mathsf{IIP}_{t_2}} \subsetneq \cdots \subsetneq \mathsf{BPP}$

Open problems

- Is $\mathsf{BPP} \subset \mathsf{P}^{\mathsf{NP}}$? (for total functions)
- In particular do BPP functions always have large rectangles?

Take Home

Remarks

- $\mathsf{P}^{\mathsf{EQ}} \neq \mathsf{BPP}$ even for total functions
- Hierarchy $\mathsf{P}^{\mathsf{EQ}} \subsetneq \mathsf{P}^{\mathsf{IIP}_{t_1}} \subsetneq \mathsf{P}^{\mathsf{IIP}_{t_2}} \subsetneq \cdots \subsetneq \mathsf{BPP}$

Open problems

- Is $\mathsf{BPP} \subset \mathsf{P}^{\mathsf{NP}}$? (for total functions)
- In particular do BPP functions always have large rectangles?

Thanks!