10^{nd} Week

Average-Case Complexity and Real Computability

Synopsis.

- Average-Case Complexity
- Complexity of Distributions
- Real Computability
- Nearly-BPP

June 11, 2018. 23:59

Course Schedule: 16 Weeks

Subject to Change

- Week 1: Basic Computation Models
- Week 2: NP-Completeness, Probabilistic and Counting Complexity Classes
- Week 3: Space Complexity and the Linear Space Hypothesis
- Week 4: Relativizations and Hierarchies
- Week 5: Structural Properties by Finite Automata
- Week 6: Stype-2 Computability, Multi-Valued Functions, and State Complexity
- Week 7: Cryptographic Concepts for Finite Automata
- Week 8: Constraint Satisfaction Problems
- Week 9: Combinatorial Optimization Problems
- Week 10: Average-Case Complexity
- Week 11: Basics of Quantum Information
- Week 12: BQP, NQP, Quantum NP, and Quantum Finite Automata
- Week 13: Quantum State Complexity and Advice
- Week 14: Quantum Cryptographic Systems
- Week 15: Quantum Interactive Proofs
- Week 16: Final Evaluation Day (no lecture)

YouTube Videos

- This lecture series is based on numerous papers of T. Yamakami. He gave conference talks (in English) and invited talks (in English), some of which were video-recorded and uploaded to YouTube.
- Use the following keywords to find a playlist of those videos.
- YouTube search keywords:

Tomoyuki Yamakami conference invited talk playlist

Conference talk video

Main References by T. Yamakami

- ✎ R. Schuler and T. Yamakami. Sets computable in polynomial time on average. In the Proc. of COCOON'95, LNCS, vol. 959, pp. 400-409 (1995).
- ✎ R. Schuler and T. Yamakami. Structural average-case complexity theory. J. Comput. Systems Sci. 52, 308-327, (1996)
- ✎ T. Yamakami. Average Case Computational Complexity. Ph.D. dissertation, University of Toronto (1997)
- ✎ T. Yamakami. Polynomial time samplable distributions. J. Complexity, 15, 557-574 (1999)
- ✎ T. Yamakami. Nearly bounded error probabilistic sets (extended abstract). In Proc. of CIAC 2003, LNCS, vol. 2653, pp. 213-226 (2003)

I. Polynomial on Average

1. Worst-Case and Average-Case Analysis
2. Distributions and Density Functions
3. Standard Distributions
4. Polynomial-Time Computable Distributions
5. Distributional Decision problems
6. t on μ-Average
7. Polynomial on Average
8. Average P, Average NP, and Average BPP

Worst-Case and Average-Case Analysis

- There are a few reasons that we usually concentrate on finding only the worst-case running time, that is, the longest running time for any input of size n.
  - The worst-case running time of an algorithm is an upper bound on the running time for any input.
  - For some algorithms, the worst case occurs fairly often.
- In some particular cases, we shall be interested in the average-case (or expected) running time of an algorithm.
- For average-case analysis, we need to discuss distributional problems whose inputs occur according to certain probability distributions.

Distributions and Density Functions I

- Let $\Sigma = \{ 0, 1 \}$.
- We use the lexicographic order over $\{0,1\}^*$, defined as

  $\lambda < 0 < 1 < 00 < 01 < 10 < 11 < 000 < 001 < \ldots$
- Here, "polynomials" are to have integer coefficients.

- A semi-distribution μ is an increasing function from Σ^* to $R^{\geq 0}$ (i.e., set of nonnegative real numbers).

- A distribution μ is a semi-distribution that satisfies

$$\lim_{x \to \infty} \mu(x) = 1$$

where "$x \to \infty$" means that x is becoming "larger" according to the lexicographic order, described above.

Distributions and Density Functions II

- In other words, a distribution μ is an increasing function from Σ^* to [0,1] such that $\lim_{x\to\infty}\mu(x)=1$

- A (probability) density function μ^* is defined by

$$\mu^*(x)=\begin{cases}\mu(\lambda) & \text{if } x=\lambda,\\ \mu(x)-\mu(x^-) & \text{otherwise}\end{cases}$$

- A probability density function is also called a probability distribution.

- (Claim) $\mu(x)=\Sigma_{z\leq x}\mu^*(z)$ holds, where $\leq$ is the lexicographic ordering.

Notational Remarks

- We use an appropriate encoding $\langle x,0^i \rangle$ of pair x and 0^i.
- Our algorithm (or a machine) M takes inputs of the form $\langle x,0^i \rangle$ and eventually enters either accepting or rejecting states.
- Although we actually use encoded strings $\langle x,0^i \rangle$, for the sake of convenience, we write $M(x,0^i)$ instead of $M(\langle x,0^i \rangle)$ for an algorithm (or a machine) M.

Standard Distribution on {0,1}* I

- Let llog(n) = $\lfloor \log_2(n+1) \rfloor$.
- llog(0)=0, llog(1)=1, llog(2)=1, llog(3)=2, ...

- Here is the standard density function on {0,1}*.

$$\nu^*_{\text{stand}}(x) = 2^{-|x|} \cdot 2^{-2\,llog(|x|)-1}$$

- This means that we pick a natural number at random and pick a string of length n at random.

$$\frac{1}{8(|x|+1)^2 2^{|x|}} \le \nu^*_{\text{stand}}(x) \le \frac{1}{2(|x|+1)^2 2^{|x|}}$$

Standard Distribution on {0,1}* II

- Its distribution is shown as

$$\nu_{\text{stand}}(x) = 1 - \frac{3}{2^{\text{llog}(|x|-1)+1}} + \frac{|x|+1}{2^{2\text{llog}(|x|-1)+1}} + \frac{k+1}{2^{2\text{llog}(|x|)+|x|+1}}$$

when x is the k-th string.

- Recall the lexicographic order:

λ < 0 < 1 < 00 < 01 < 10 < 11 < 000 < 001 < ...

0 1 2 3 4 5 6 7 8 ....

Standard Distribution on {0}*

- A string over a single alphabet is called tally.
- Here is the standard density function on {0}*.

$$\nu^{*}_{tally}(x) = \begin{cases} 1/2 & \text{if } x = \lambda, \\ 2^{-2\operatorname{llog}(n)-1} & \text{if } \exists n > 0[x = 0^{n}], \\ 0 & \text{otherwise.} \end{cases}$$

- This means that we pick a natural number at random.
- Its distribution is shown as

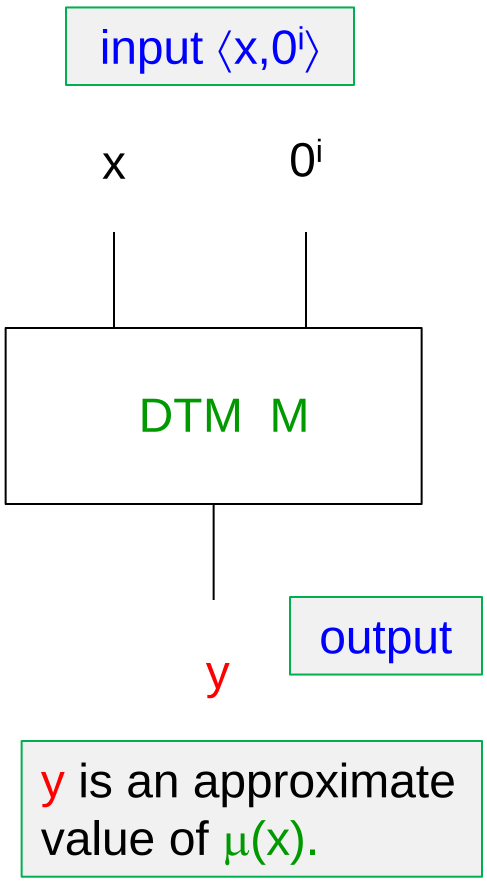
$$\nu^{*}_{tally}(0^{n}) = \begin{cases} 1/2 & \text{if } n = 0; \\ 2^{-2\operatorname{llog}(n)-1} & \text{otherwise.} \end{cases}$$

Polynomial-Time Computable Distributions

- Let $\mu: \Sigma^* \to [0,1]$ be any distribution.
- μ is polynomial-time computable $\Leftrightarrow$ there is a polynomial-time deterministic Turing machine (DTM) with an output tape such that

$$| \mu(x) - M(x,0^i) | \leq 2^{-i}$$

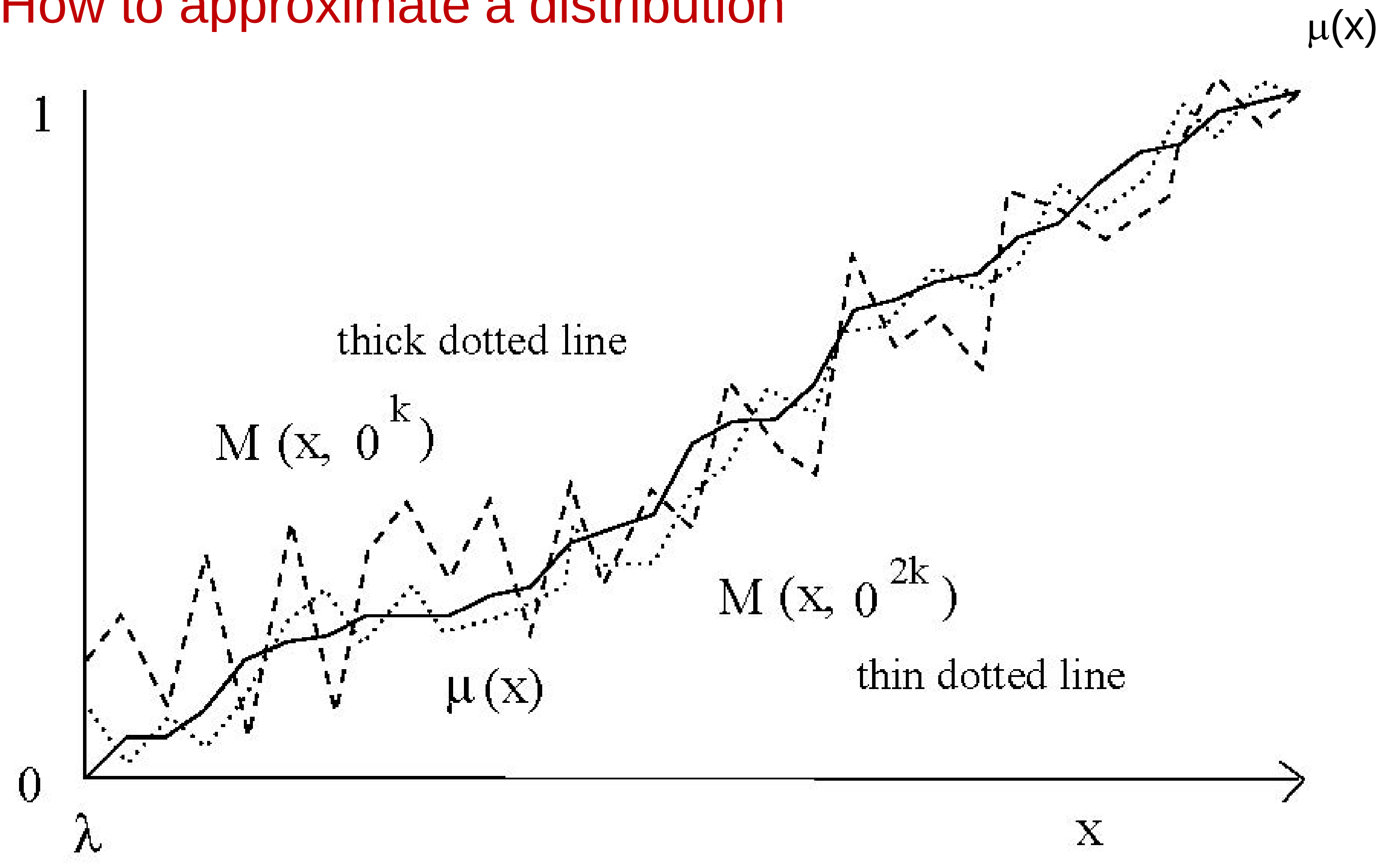
for any $x \in \Sigma^*$ and $i \in N$.
- Let P-comp be the collection of all polynomial-time computable distributions.



$$|\mu(x) - y| \leq 2^{-i}$$

Approximation of Distributions

- How to approximate a distribution



As we increase k, M(x,0k) is approaching to $\mu(x)$

Distributions Versus Density Functions

- We have defined the polynomial-time computable distributions and we will use them as a basis of our polynomial-time computability in average-case complexity theory.
- It could be possible to introduce polynomial-time computable density functions and develop average-case complexity theory. However, we did not use density functions in place of distributions.
- This is because:
  - If P $\neq$ NP (as many researchers believe), there exists a density function that is computable in polynomial time but its associated distribution is not polynomial-time computable.

Distributional Decision Problems

- A distributional decision problem is a pair (D,μ), where D is a language and μ is a distribution.
- Recall P (deterministic polynomial-time class) and NP (nondeterministic polynomial-time class) from Week 1.

- Let F be a class of distributions.

- Dist(P,F) consists of all distributional decision problem (D,μ) such that $D \in P$ and $\mu \in F$.

- Dist(NP,F) consists of all distributional problems (D,μ) with $D \in NP$ and $\mu \in F$.

DistNP

- In the definition of Dist(NP,F), if we choose F = all distributions, we write Dist(NP,*) for { (D,μ) | D$\in$NP,μ: arbitrary }.
- Thus, Dist(NP,F) $\subseteq$ Dist(NP,*) holds for any set F.

- Dist(NP,P-comp) is the collection of all distributional decision problem (D,μ) such that D$\in$NP and $\mu\in$P-comp.
- In this case, we write DistNP instead of Dist(NP,P-comp).

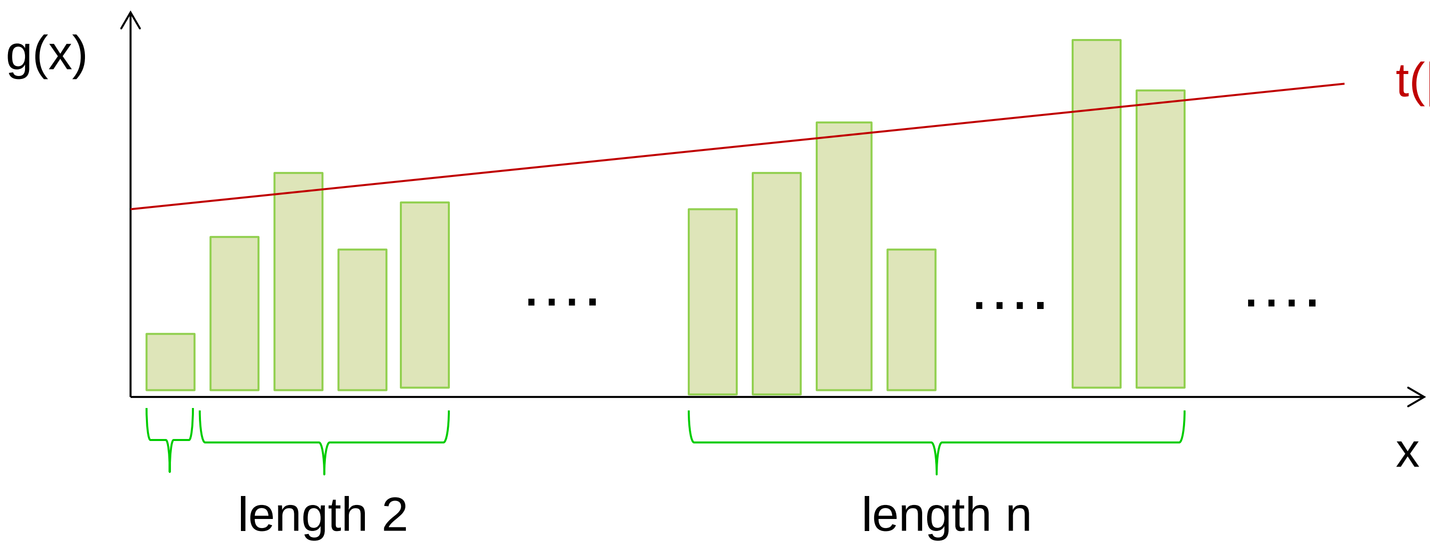
t on μ-Average

- Let $R^+ = \{ r \in R \mid r \geq 0 \}$ and $R^{+\infty} = R \cup \{\infty\}$.
- Schapire (1990) considered the following. Let $t: R^+ \to R^+$.

- A function $g: \Sigma^* \to R^{+\infty}$ is t on μ-average

$\Leftrightarrow$ for any positive real number r,

$$\mu^*\left(\left\{x \in \Sigma^* \mid g(x) > t(|x| \cdot r)\right\}\right) < \frac{1}{r}$$



Polynomial on Average

- From the previous definition, we obtain:
- (Claim) If g is t on μ-average, then

$$g(x) \leq t(|x|/\mu^*(x))$$

holds for all x with $\mu^*(x)>0$.

- Let T be a set of functions from R^+ to R^+.
- A function $g: \Sigma^* \rightarrow R^{+\infty}$ is T on μ-average

$\Leftrightarrow$ for any $t \in T$, g is t on μ-average.

- In particular, if T = all positive polynomials, we obtain the notion of "polynomial on μ-average."

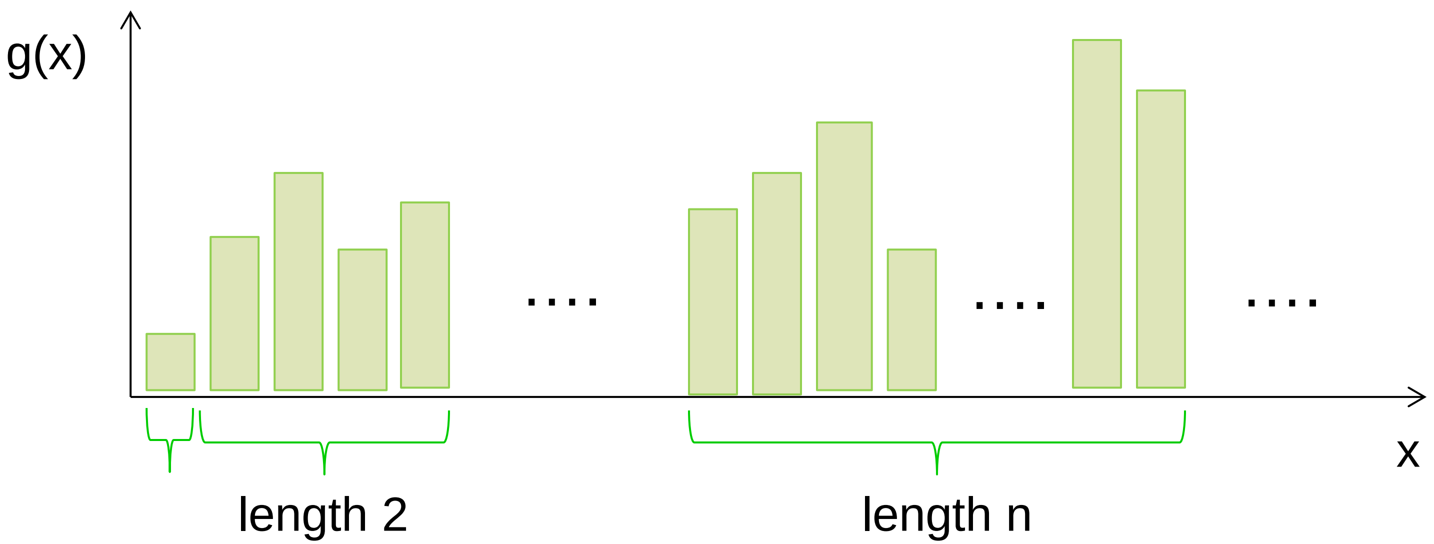
Levin's Definition

- Levin (1984) took the following definition.

- A function g: $\Sigma^* \to R^{+\infty}$ is polynomial on μ-average

  $\Leftrightarrow$ there exists a real number $k \geq 1$ such that

$$\sum_{x:|x|>0} \frac{g(x)^{1/k}}{|x|} \mu^*(x) < \infty$$



Equivalence Between Two Definitions

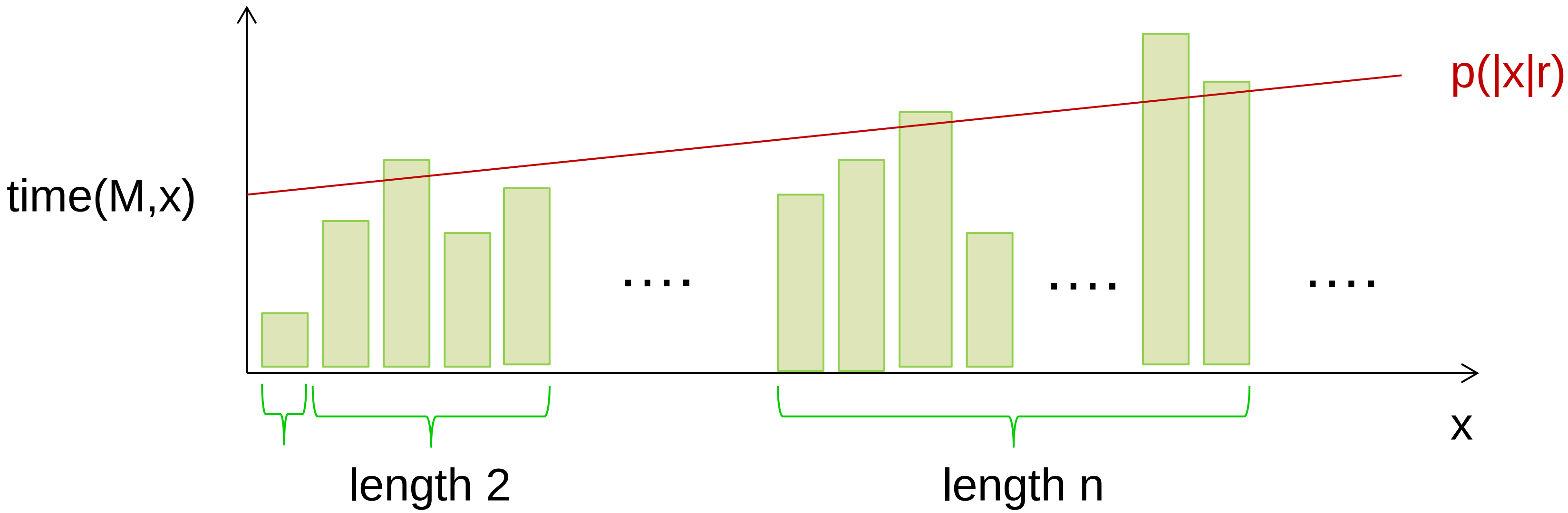
- By Schapire (1990) and Impagliazzo (1995), we obtain the following equivalence between the previous two definition on "polynomial on μ-average."

- (Claim) The following two definitions are logically equivalent.
  1. g is polynomial on μ-average.
  2. There exists a real number $k \geq 1$ such that

$$\sum_{x:|x|>0} \frac{g(x)^{1/k}}{|x|} \mu^*(x) < \infty$$

Polynomial-Time on Average

- For a deterministic Turing machine (DTM) M and an input x, time(M,x) means the running time of M on input x.
- Let D be a language over alphabet Σ.
- We say that M recognizes D in polynomial-time on μ-average if (i) M recognizes D and (ii) the function time(M,•) is polynomial on μ-average.



Average P

- Let F be a class of distributions.
- Average(P,F) consists of all distributional decision problems (D,μ) such that (i) $\mu \in$ F and (ii) a certain DTM M recognizes D in polynomial-time on μ-average.
- If F is the set of all distributions, we write Average(P,*).
- When F = P-comp, we obtain Average(P,P-comp). This class is often written as Average-P.
- (Claim) For any set F of distributions with $\nu_{tally} \in$ F, Average(P,F) $\not\subseteq$ Dist(NP,*). [Wang-Belanger (1995)]

Average NP

- Let F be a class of distributions.
- Average(NP,F) consists of all distributional decision problems (D,μ) such that (i) $\mu \in$ F and (ii) certain NTM M recognizes D in polynomial-time on μ-average.
- When F = P-comp, we obtain Average(NP,P-comp). This class is often written as Average-NP.
- (Claim) Dist(NP) $\subseteq$ Average(NP,P-comp)
- Theorem: [Schuler-Yamakami (1992)]

  Average(P,*) $\neq$ Average(NP,*)

Average BPP

- Let F be a class of distributions.
- Average(BPP,F) consists of all distributional decision problems (D,μ) such that (i) $\mu \in$ F and (ii) certain PTM M recognizes D with bounded-error probability in polynomial-time on μ-average.
- When F = P-comp, we obtain Average(BPP,P-comp). This class is often written as Average-BPP.
- Claim:
  1. If P $\neq$ BPP, then Average(P,*) $\neq$ Average(BPP,*).
  2. If P = PP, then Average(P,F) = Average(BPP,F) for any set F of distributions

Open Problems

- At this moment, we do not know whether all distributional problems in DistNP can be solved deterministically in average polynomial time.
- In other words,
- (Open Question) Is DistNP $\subseteq$ Average-P?

- More generally, we can ask the following question.
- (Open Question)
  - Prove or disprove that Dist(NP,F) $\subseteq$ Average(P,F) for each choice of natural distribution class F.

II. Complete Distributional Problems

1. Domination Relations
2. Average Domination
3. Equivalence Relations
4. Polynomial-Time Many-One Reductions
5. Properties of $\leq_m^p$
6. Average Polynomial-Time Many-One Reductions
7. Hard Problems and Complete Problems
8. (RBTB,μ_{RBTB}) is Complete for Dist(NP,P-comp)

Domination Relations I

- We introduce a notion of "domination."
- A function $f : \{0,1\}^* \to R^{\geq 0}$ is polynomially bounded (or p-bounded) $\Leftrightarrow$ there exists a polynomial p such that, for all $x \in \{0,1\}^*$, $f(x) \leq p(|x|)$.
- Let μ,ν be distributions and let $t : \{0,1\}^* \to R^{\geq 0}$.
- We say that ν t-dominates μ if, for all x,

$$t(x)\nu^*(x) \geq \mu^*(x).$$

- We say that ν polynomially dominates (or p-dominates) μ ($\mu \leq^p \nu$) if there is a certain polynomially-bounded function t and ν t-dominates μ .

Domination Relations II

- Let μ,ν be distributions.

- (Claim) If $\mu_1 \leq^{p} \mu_2$ and $\mu_2 \leq^{p} \mu_3$, then $\mu_1 \leq^{p} \mu_3$.
- (Claim) If $\mu_1 \leq^{avp} \mu_2$ and $\mu_2 \leq^{avp} \mu_3$, then $\mu_1 \leq^{avp} \mu_3$.

- (Claim) Assume that ν p-dominates μ. If an algorithm A requires polynomial time on ν-average, then A also requires polynomial time on μ-average.

Average Domination

- Let μ,ν be distributions and let $t : \{0,1\}^* \to R^{\geq 0}$.

- We say that ν average t-dominates μ if there exists a function $f : \{0,1\}^* \to R^{\geq 0}$ such that f is t on μ-average and ν f-dominates μ.

- We say that ν average polynomially dominates (or avp-dominates) μ ($\mu \leq^{avp} \nu$) if there exists a polynomial t such that ν average t-dominates μ.

- (Claim) Assume that ν avp-dominates μ. If an algorithm A requires polynomial time on ν-average, then A also needs polynomial time on μ-average.

Equivalence Relations

- Let μ,ν be two distributions.

- We say that μ p-equivalent to ν ($\nu \approx^{p} \mu$) if μ p-dominates ν and ν p-dominates μ.

- We say that μ average p-equivalent to ν ($\nu \approx^{avp} \mu$) if μ avp-dominates ν and ν avp-dominates μ.

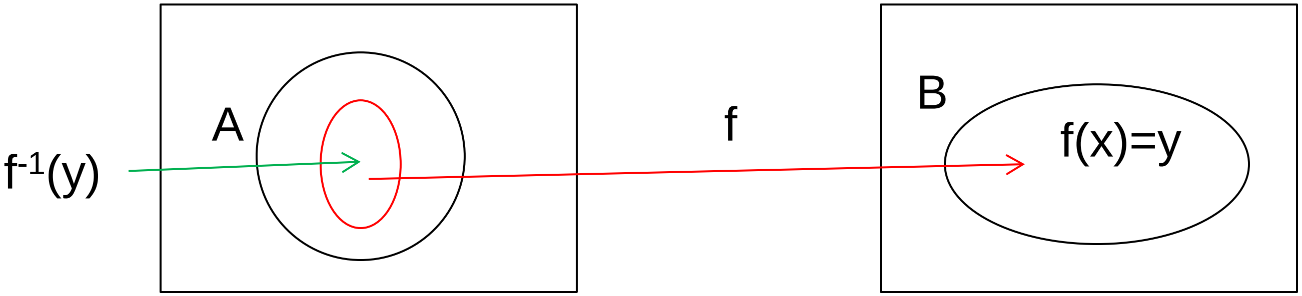
A Useful Condition on Domination

- Let η be a distribution and f : $\Sigma^* \to \Sigma^*$ be a function.
- Define $\eta_{f\text{-}1}$ as $\eta_{f\text{-}1}{}^*(x) = \eta(\{ z \mid f(z) = x \})$ for all strings $x \in \Sigma^*$.
- We say that ν^* majorizes μ^* (denoted $\nu^* \geq \eta^*$) if $\nu^*(x) \geq \mu^*(x)$ holds for all $x \in \{0,1\}^*$.

- (Claim) The following statements are logically equivalent.
  1. There exists a semi-distribution η s.t. $\mu \leq^p \eta$ and $\nu^* \geq \eta_{f\text{-}1}{}^*$.
  2. There exists a p-bounded positive function p : $\{0,1\}^* \to R^{\geq 0}$ s.t., for all y, $$\nu^*(y) \geq \sum_{x \in f^{-1}(y)} \frac{\mu^*(x)}{p(x)}$$

Polynomial-Time Many-One Reductions

- Let (A,μ), (B,ν) be any distributional decision problems.
- (A,μ) is polynomial-time many-one reducible (or p-m-reducible) to (B,ν) iff there exists a function f such that
  - (Efficiency) $f \in FP$,
  - (Validity) for every x, $x \in A \leftrightarrow f(x) \in B$
  - (Domination) for a certain semi-distribution η, $\mu \leq^p \eta$ and $\nu^* \geq \eta_{f^{-1}}{}^*$.
- In this case, we write $(A,\mu) \leq_m^p (B,\nu)$.



$\mu \leq^p \eta$
$\nu^* \geq \eta_{f^{-1}}{}^*$

Properties of $\leq_m^p$

- The following properties hold.

- (Reflexive) $(A,\mu) \leq_m^p (A,\mu)$
- (Transitive) If $(A,\mu) \leq_m^p (B,\nu)$ and $(B,\nu) \leq_m^p (C,\eta)$, then $(A,\mu) \leq_m^p (C,\eta)$.

- Hence, $\leq_m^p$ forms a partial order.

Average Polynomial-Time Many-One Reductions

- Let (A,μ), (B,ν) be any distributional decision problems.

- (A,μ) is average polynomial-time many-one reducible (or avp-m-reducible) to (B,ν) $\Leftrightarrow$ there exists a function f : $\{0,1\}^* \to \{0,1\}^*$ such that
  - (Efficiency) $(f,\mu) \in$ Average(FP,*),
  - (Validity) for every x, $x \in A \leftrightarrow f(x) \in B$
  - (Domination) for a certain η, $\mu \leq^{avp} \eta$ and $\nu^* \geq \eta_{f''}{}^*$.
- In this case, we write $(A,\mu) \leq_m^{avp} (B,\nu)$.

- (Claim) $(A,\mu) \leq_m^{p} (B,\nu)$ implies $(A,\mu) \leq_m^{avp} (B,\nu)$.

Properties

- Let (A,μ), (B,ν) be any distributional decision problems.

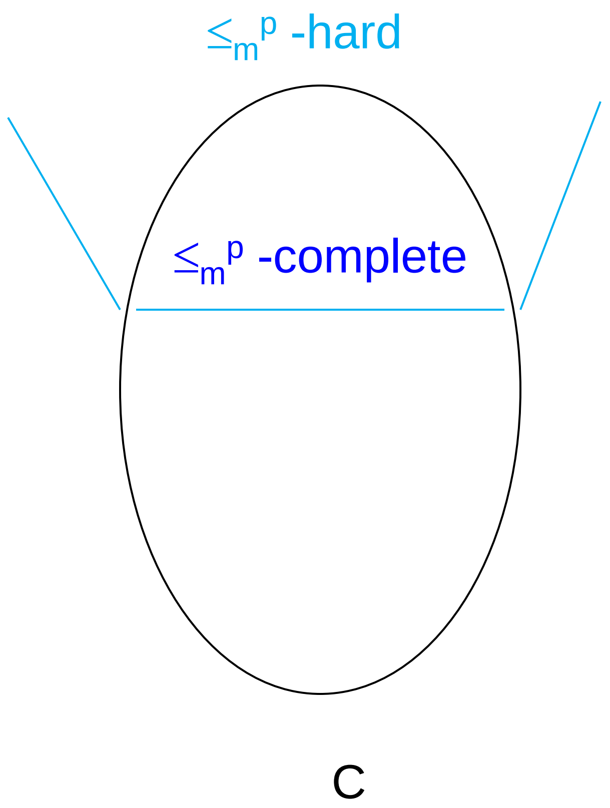
- (Claim) For any $C \in \{P,NP,BPP,PSPACE\}$, Average(C,*) is closed (downward) under $\leq_m^{avp}$-reductions.

  Namely, if $(A,\mu) \leq_m^{avp} (B,\nu)$ and $(B,\nu) \in$ Average(C,*), then we obtain $(A,\mu) \in$ Average(C,*).

Hard Problems and Complete Problems

- Let (A,μ), (B,ν) be any distributional decision problems.
- Let C be a class of distributional problems.

- (A,μ) is $\leq_m^p$ -hard for C if every distributional problem in C is p-m-reducible to (A,μ).
- (A,μ) is $\leq_m^p$ -complete for C if (A,μ) is in C and it is $\leq_m^p$ -hard for C.



Decision Problems vs. Distributional Problems

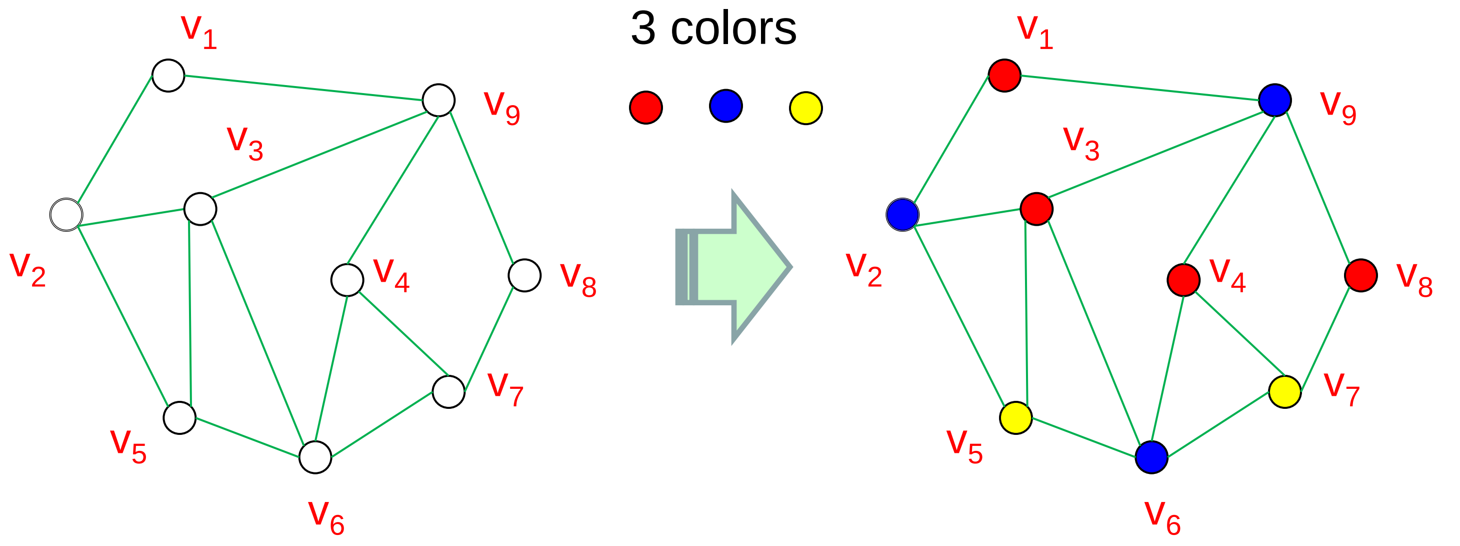
- We can ask whether all NP-complete decision problems are also DistNP-complete distributional problems.

- Unfortunately, this statement may not be true, because:
  - 3COL is NP-complete.
  - Wilf (1985) showed that $(3COL, \mu_{3COL}) \in$ Average(P,*).

- In the next slide, we will explain $(3COL, \mu_{3COL})$.

Randomized 3-Colorability Problem

- Randomized 3-Colorability Problem (3COL)
  - 3COL = { ⟨G⟩ | G is a graph that is 3-colorable }
  - $\mu_{3COL}^*(\langle G \rangle) = \nu_{tally}^*(1^{|V|})2^{-(n \text{ choose } 2)}$
  - (Choose the number of vertices at ransom and then choose edges between pairs of distinct vertices at random.)



Randomized 3-Satisfiability Problem

- Recall that 3SAT is NP-complete.
- Randomized 3-Satisfiability Problem (3SAT)
  - 3SAT = { $\langle(p_1,q_1,r_1),\ldots,(p_n,q_n,r_n)\rangle$ | formula $\wedge_{i=1}^{n}(p_i \vee q_i \vee r_i)$ is satisfiable }
  - $\mu_{3SAT}{}^*(\langle(p_1,q_1,r_1),\ldots,(p_n,q_n,r_n)\rangle)$
    $= \nu_{tally}{}^*(1^n)\Sigma_{i=1}^{n}2^{-(|pi|+|qi|+|ri|)}$
  - (Pick up n at random and pick up n triples of variables at random.)
- A formula $\wedge_{i=1}^{n}(p_i \vee q_i \vee r_i)$ is satisfiable $\Leftrightarrow$ $\exists\sigma$:truth assignment s.t. $\wedge_{i=1}^{n}(\sigma(p_i)\vee \sigma(q_i)\vee\sigma(r_i))$ equals 1

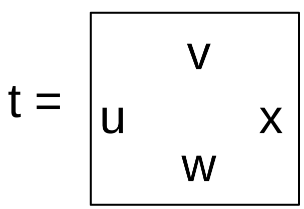
Tiles and Tilings I

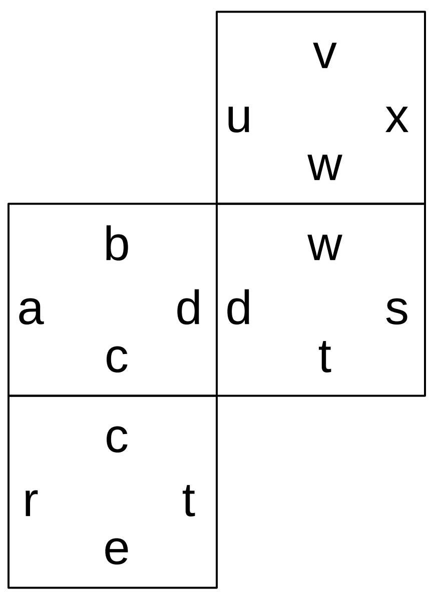
- A tile is a quadruple [u,v,x,w] of strings, where u is “left”, v is “top”, x is “right”, and w is “bottom”.
- We write left[u,v,x,w] for u, top[u,v,x,w] for v, right[u,v,x,w] for x, and bottom[u,v,x,w] for w.
- Let S_n be the $n \times n$ square $\{1,\ldots,n\} \times \{1,\ldots,n\}$.
- Let T be a set of tiles.
- A function $f: S_n \to T$ is a T-tiling of S_n if left[f(i+1,j)] = right[f(i,j)] and bottom[f(i,j+1)] = top[f(i,j)] for all i,j with $1 \leq i,j \leq n$.
- A sequence $\langle t_1,t_2,\ldots,t_k \rangle$ is a T-row of length k if $t_i \in T$ for all i with $1 \leq i \leq n$ and left[t_{j+1}] = right[t_j] for all j with $1 \leq j \leq n$.

Tiles and Tilings II

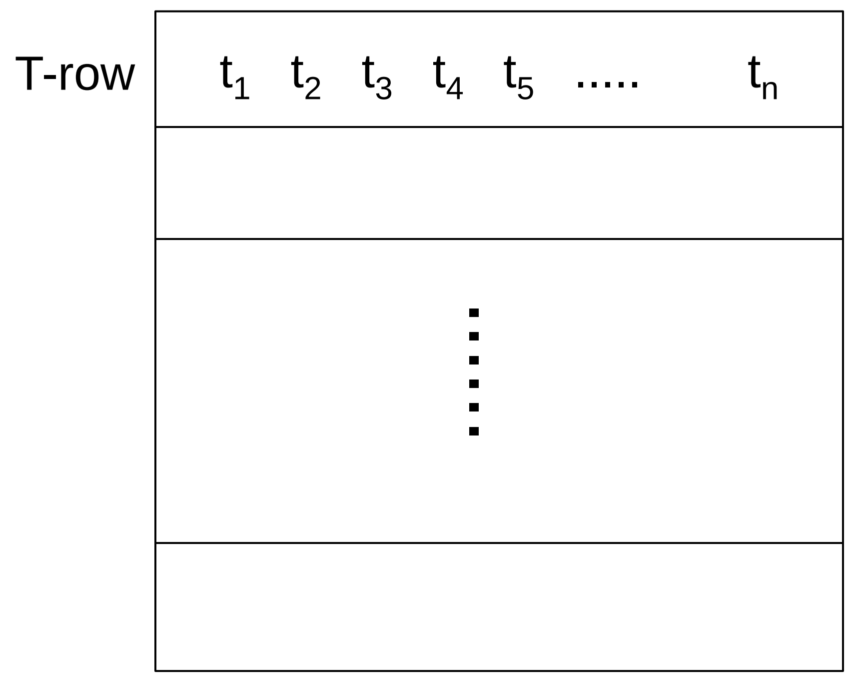
- T-tiling $f: S_n \rightarrow T$

tile





$S_n = \{1,2,..,n\} \times \{1,2,...,n\}$



Tiling Problem

- Levin (1984) discussed the distributional problem $(\mathrm{RBTP}, \mu_{\mathrm{RBTP}})$.
- Randomized Bounded Tiling Problem (RBTP)
  - instance: a set T of tiling, size n, a T-row $<t_1, t_2, \ldots, t_k>$ of length k with $1 \le k \le n$
  - question: is there a T-tiling f of S_n such that $f(1,i) = t_i$ for any i with $1 \le i \le n$?
- Distribution μ_{RBTP} (with a fixed positive $\mu \in$ P-comp)

$$\mu_{RBTP}\left(\left\langle T, 1^n, 1^k, \left\langle t_1, t_2, \ldots, t_k \right\rangle \right\rangle\right) = \begin{cases} \mu^*(T)\nu_{tally}(1^n)\frac{1}{n}\prod_{i=1}^{k}\frac{1}{|T_i|} & \text{if } \underline{\text{ condition A}} \\ 0 & \text{otherwise} \end{cases}$$

where $T_i = \{ t \in T \mid \mathrm{left}[t] = \mathrm{right}[t_i] \}$.

- Condition A: $1 \le k \le n$ and $T_i \neq \emptyset$ for all i with $1 \le i \le k$

(RBTB,μ_{RBTB}) is Complete for Dist(NP,P-comp)

- Levin (1984) demonstrated the following completeness result.

- (Claim) Distributional Problem (RBTP,μ_{RBTP}) is $\leq_m^p$-complete for Dist(NP,P-comp). [Levin (1984)]

- Note that the tiling problem is NP-complete.

Randomized Bounded Halting Problem

- We show another complete distributional problem.

- Randomized Bounded Halting Problem (RBHP)
  - BHP = { $\langle s_i,x,1^n\rangle$ | M_i accepts x in less than n steps }
  - $\mu_{BHP}{}^*(s_i,x,1^n) = \nu_{st}{}^*(s_i)\nu_{st}{}^*(x)\nu_{tally}{}^*(1^n)$
  - (Pick up string s_i at random, pick up x at random, and pick up 1^n at random.)

- (Claim) $(RBHP,\mu_{BHP})$ is $\leq_m{}^p$-complete for Dist(NP,P-comp). [Gurevich-Shelah (1987)]

Open Problems

- There are numerous problems that have not yet solved.

1. Find natural distributional problems that are complete for Dist(NP,P-comp).
2. Similarly, find natural distributional problems that are complete for Dist(NP,P-samp).

- P-samp will be discussed in the next section.

III. Complexity of Distributions

1. P-Computable Distributions
2. Polynomial-Time Samplable Distributions
3. #P-Computable Distributions
4. E-Computable Distributions
5. Properties of Distribution Classes
6. avP-Samplable Distributions

P-Computable Distributions (revisited)

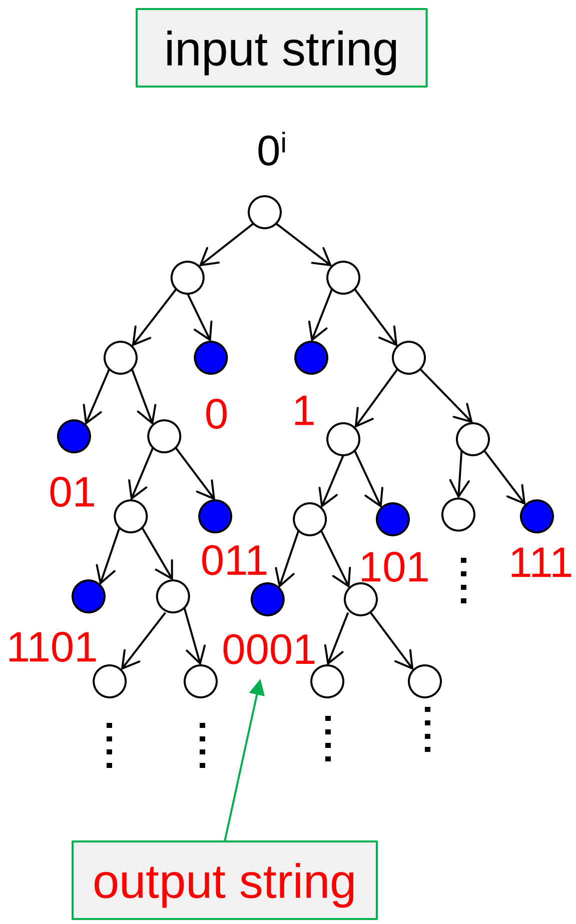
- Let $\mu: \Sigma^* \rightarrow [0,1]$ be a distribution.
- Recall that μ is polynomial-time computable $\Leftrightarrow$ there is a polynomial-time deterministic Turing machine (DTM) with an output tape such that $| \mu(x) - M(x,0^i) | \leq 2^{-i}$. for any $x \in \Sigma^*$ and $i \in N$.
- Let P-comp be the collection of all polynomial-time computable distributions.

Polynomial-Time Samplable Distributions

- We introduce another type of distribution.

- A distribution μ is polynomial-time samplable (or P-samplable) $\Leftrightarrow$ there are a polynomial p and a probabilistic Turing machine (PTM) that take input 0^i and produces strings satisfying, for every x,

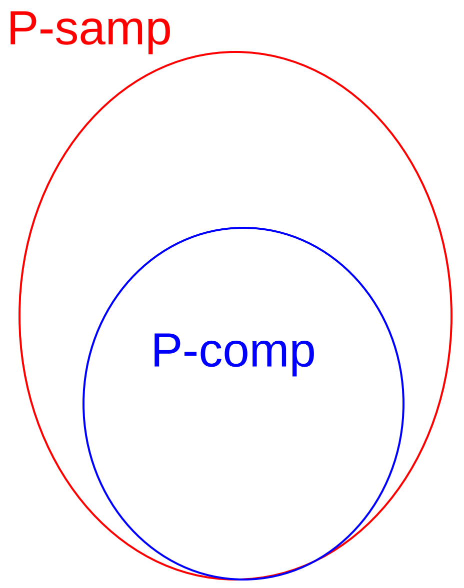
  $| \mu^*(x) - \mathrm{Prob}_M[\, M(0^i) \text{ produces } x \text{ within time } p(|x|,i)\,] | \leq 1/2^i$.



P-Samp I

- Let P-samp denote the collection of all polynomial-time samplable distributions.

- (Claim) P-comp $\subseteq$ P-samp.
- (Claim) P $\neq$ NP $\Rightarrow$ P-comp $\neq$ P-samp. [Ben-David-Chor-Goldreich-Luby (1992)]
- (Claim) P = PP $\Leftrightarrow$ P-comp = P-samp. [Milterson (1993)]



Many believe in this way

P-Samp II

- Recall the notion of (strong) one-way function from Week 7.

- (Claim) Assume that every distribution in P-samp is p-dominated by certain distributions in P-comp. Then, there is no strong one-way function [Ben-David-Chor-Goldreich-Lubby (1992)]

Complete Problem for Dist(NP,P-samp)

- We show the existence of complete distributional problem for Dist(NP,P-samp).
- Randomized Bounded halting Problem (RBHP)
  - BHP = $\{ \langle s_i, x, 1^n \rangle \mid M_i$ accepts x in less than n steps $\}$
- Distribution μ_U
  - Let $\{ \eta_i \}_{i \in N}$ be an effective enumeration of all O(n)-time samplable distributions.
  - $\mu_U^*(z) = \Sigma_{i=0}^{\infty} 2^{-2\mathrm{llog}(i)-1} \eta_i^*(z)$
  - (Pick up i at random and pick up z according to η_i^*.)
- (Claim) (RBHP,μ_U) is $\leq_m^p$-complete for Dist(NP,P-samp). [Ben-David-Chor-Goldreich-Luby (1992)]

Θ_2^p-Samplable Distributions

- A P-samplable distribution is approximated by running a certain PTM starting with input 0^i and produces strings x within time $p(|x|,i)$.

- A distribution μ is Θ_2^p-samplable if there exist a polynomial p, a constant c>0, a language A $\in$ NP, and an oracle PTM M such that (1) M starts with no input and A as an oracle and (2) for every x,

  $| \mu^*(x) - \mathrm{Prob}_M[\ M^A(0^i)$ produces x within time $p(|x|,i)$, making at most $c\log|x|+c$ queries to A $] | \le 1/2^i$.

- Let Θ_2^p-samp to denote the class of all Θ_2^p-samplable distributions.

Invertibly P-Samplable Distributions

- Recall that $\eta_{f^{-1}}$ is defined as $\eta_{f^{-1}}{}^*(x) = \eta(\{ z \mid f(z) = x \})$ for all strings $x \in \Sigma^*$.
- A distribution μ is invertibly polynomial-time samplale (or invertible P-samplable) if there exists a distribution $\nu \in$ P-comp and a p-honest function $f \in$ FP such that $\mu = \nu_{f^{-1}}$.
- Let IP-samp to denote the class of all invertibly P-samplable distributions
- Let IP_1-samp = $\{\nu_{f^{-1}} \mid \nu \in$ P-comp, f is one-one $\}$
- (Claim) P-comp $\subseteq IP_1$-samp $\subseteq$ IP-samp

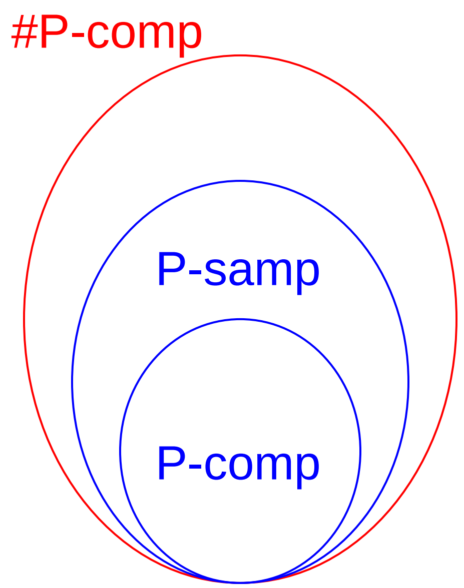
#P-Computable Distributions

- Recall that we always identify {0,1}* with N.
- A distribution μ is #P- computable $\Leftrightarrow$ there is a function f : {0,1}* $\times$ N $\rightarrow$ N in #P such that, for all pairs (x,i),

$$\left| \mu^*(x) - \frac{f(x,0^i)}{2^{p(|x|,i)}} \right| \leq 2^{-i}$$

- Let #P-comp be the collection of all #P-computable distributions.
- (Claim)

  P-comp $\subseteq$ P-samp $\subseteq$ #P-comp



Many believe in this way

E-Computable Distributions

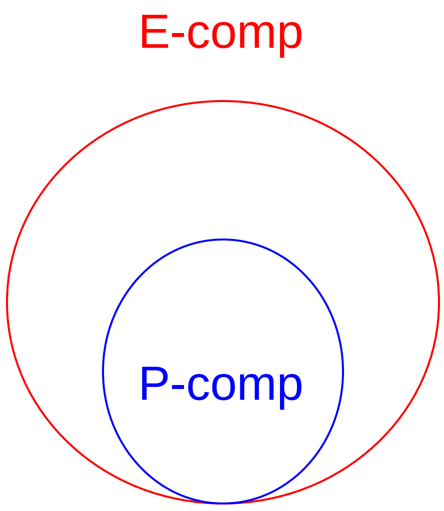
- Let $\mu: \Sigma^* \to [0,1]$ be a distribution.

- μ is E- computable $\Leftrightarrow$ there is a DTM M such that, for all pairs (x,i), M runs in time $2^{c(|x|+i)}$ and satisfies

$$| \mu(x) - M(x,0^i) | \le 2^{-i}.$$

- Let E-comp be the collection of all E-computable distributions.

- (Claim) P-comp $\subseteq$ E-comp



Many believe in this way

Properties of Distribution Classes I

- We have known the following properties of and relationships among distribution classes.
- Given a μ, $[\mu]_p$ denotes the equivalence class $\{ \xi \mid \xi =^p \mu \}$.
- Given two distribution sets F and G, we say that G p-includes F (denoted by $F \subseteq^p G$) if $F/=^p \subseteq G/=^p$.
- (Claim) #P-comp $\subseteq^p$ $\Theta_2{}^p$-samp. [Schuler-Watanabe (1995)]

Properties of Distribution Classes II

- We can show the following relationships about #P-computable distributions and various P-samplable distributions.

- Theorem: [Yamakami (1999)]

  P = PP $\Leftrightarrow$ P-comp = #P-comp

- Theorem: [Yamakami (1999)]

  P = PP $\Leftrightarrow$ P-comp = IP_1-samp $\Leftrightarrow$ P-comp = IP-samp

avP-Samplable Distributions

- A distribution μ is average polynomial-time samplable (or avP-samplable) if there exists a DTM with an output tape (computing a function f : $\{0,1\}^* \times \{0\}^* \rightarrow \{0,1\}^*$) s.t.
  1. $\mathrm{Time}_M(x,0^i)$ is polynomial on $\nu_{st} \circ \nu_{tally}$-average, and
  2. $\left|\mu^*(x) - \xi_M^{(i)}(x)\right| \leq 2^{-i}$

  where $\xi_M^{(i)}(x) = \nu^*_{\text{stand}}\left(\left\{y \in \{0,1\}^* \mid M(y,0^i) = x\right\}\right)$

  $$(\nu_{\text{stand}} \circ \nu_{tally})^*(x,0^i) = \nu^*_{\text{stand}}(x)\nu^*_{tally}(0^i)$$

- Let avP-samp denote the set of all avP-samplable distributions.

- (Claim) P-samp $\subseteq$ avP-samp

Open Problems

- There are numerous problems that have not yet solved.

1. Does #P-comp $=^p$ SpanP-comp imply PP=UP?
2. Does avP-samp $\subseteq_{av}$ P-comp imply P-samp $\subseteq_{av}$ P-comp?

IV. Real Computability

1. Real Computability
2. Complexity Class P_F
3. Properties of $P_{P\text{-comp}}$
4. Properties of $P_{P\text{-samp}}$
5. Complexity Class BPP_F

Real Computability

- We have discussed what decision problems A are solved in average polynomial-time for a reasonable distribution μ.
- In other words, $(A,\mu) \in$ Average(P,F), where F is a class of distribution.

- Let us consider decision problems that are solved in average polynomial-time for all distributions μ in F.
- Such problems are called “real” computable problems.

Complexity Class P_F

- Let F be a class of distributions.

- P_F = collection of all languages L that are polynomial-time computable on μ-average for every $\mu \in F$.
- In other words,

  $L \in P_F \iff (L,\mu) \in \mathrm{Average}(P,F)$ holds for any $\mu \in F$.

- By taking P-comp, P-samp, E-comp as F, for example, we naturally obtain $P_{\text{P-comp}}$, $P_{\text{P-samp}}$, $P_{\text{E-comp}}$, etc.

- (Claim)
  - $P \subseteq P_{\text{P-samp}} \subseteq P_{\text{P-comp}}$ (since P-comp $\subseteq$ P-samp).
  - $P \subseteq P_{\text{E-comp}} \subseteq P_{\text{P-comp}}$ (since P-comp $\subseteq$ E-comp).

Properties of $P_{\text{P-comp}}$

- Here is a short list of properties known today.

1. $P = P_{\text{E-comp}}$ [Schuler-Yamakami (1995)]
2. $P \neq P_{\text{P-comp}}$ [Schuler (1995)]
3. $P_{\text{P-comp}} \not\subset P/cn$ for any fixed c>0 [Schuler-Yamakami (1995)]
4. $NP \subseteq P_{\text{P-comp}}$ implies P=BPP. [Buhrman-Fortnow-Pavan (2005)]
5. $NP \subseteq P_{\text{P-comp}}$ implies E = NE [Ben-Divid-Chor-Goldreich-Lubby (1992)]
6. $NP \subseteq P_{\text{P-comp}}$ implies MA = NP [Köbler-Schuler (2004)]
7. $\Delta_3^p \subseteq P_{\text{P-comp}}$ implies $\Sigma_3^p \cap \Pi_3^p \cap P/poly = P$ [Köbler-Schuler (2004)]

Properties of $P_{P\text{-samp}}$

- Here is a short list of properties known today.

1. $P \subseteq P_{P\text{-samp}} \subseteq E$ and $P \neq P_{P\text{-samp}} \neq E$ [Schuler (1995)]
2. $NP \subseteq P_{P\text{-comp}}$ implies $NP \subseteq P_{P\text{-samp}}$. [Buhrman-Fortnow-Pavan (2005)]
3. $NP \subseteq P_{P\text{-samp}}$ implies $\Theta_2^p \subseteq P_{P\text{-samp}}$ [Ben-Divid-Chor-Goldreich-Lubby (1992), Schuler-Watnabe (1995)]

Complexity Class BPP_F

- Let F be any set of distributions.
- BPP_F is composed of all languages L such that, for every $\mu \in F$, there is a probabilistic Turing machine (PTM) M that recognizes L with probability at least 2/3 in time polynomial on μ-average.
- (Claim) $BPP \subseteq BPP_F \subseteq BPE$ if $\nu_{st} \in F$. [Yamakami (1999)]
- (Claim) $MA \subseteq BPP_{P\text{-comp}} \rightarrow MA_E \subseteq BPE$. [Yamakami (1999)]
- (Claim) $NP \subseteq BPP_{P\text{-comp}} \rightarrow NE \subseteq BPE$. [Schuler-Yamakami (1992)]

Open Problems I

- Here is a short list of open problems associated with real computability.

1. Is $P_{\text{P-comp}} \subseteq$ P/poly?
2. Is $P_{\text{P-comp}} \subseteq \oplus$P?
3. Does BPP $\subseteq P_{\text{P-comp}}$ imply P = BPP?
4. Does NP $\subseteq P_{\text{P-comp}}$ imply P = NP?
5. Is MA $\subseteq \text{BPP}_{\text{P-comp}}$?
6. Is BPP $\neq \text{BPP}_{\text{P-comp}}$?
7. Does NP $\subseteq P_{\text{P-comp}}$ imply P-samp $\leq^{p}$ P-comp?

Open Problems II

- Here is a short list of open problems associated with real computability.

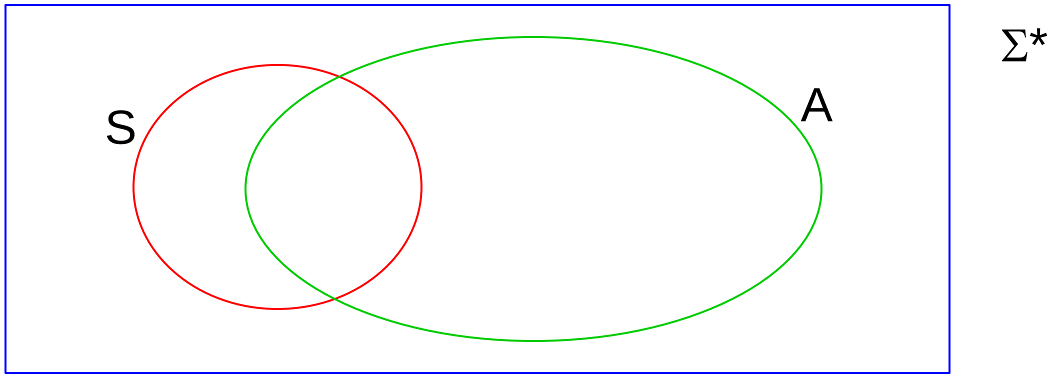
1. Is $MA \subseteq BPP_{P\text{-comp}}$?
2. Is $P_{P\text{-comp}} \subseteq \oplus P$?
3. Is $MA \subseteq P_{P\text{-comp}}$ equivalent to $MA \subseteq P_{P\text{-samp}}$?
4. avP-samp Does $BPP \subseteq P_{P\text{-comp}}$ imply $P = BPP$?
5. Does $NP \subseteq P_{P\text{-comp}}$ imply $P = NP$?
6. Is $MA \subseteq BPP_{P\text{-comp}}$?
7. Is $BPP \neq BPP_{P\text{-comp}}$?
8. Does $NP \subseteq P_{P\text{-comp}}$ imply P-samp $\leq^p$ P-comp?

V. Nearly BPP

1. Nearly BPP Sets
2. Properties of Nearly-BPP

Nearly-BPP Sets

- A language A is said to be nearly-BPP if, for every polynomial p, there exist a set S and a polynomial-time probabilistic Turing machine M such that, for each x,
  1. $x \in \Sigma^* - S \rightarrow \mathrm{Prob}_M[\, M(x) \neq A(x)\,] \leq 1/3$, and
  2. $\mathrm{Prob}_{x\in\Sigma^n}[\, x \in S\,] < 1/p(n)$ for almost all n.



- Let Nearly-BPP be the class of all nearly-BPP languages.

Properties of Nearly-BPP

- We show several properties of Nearly-BPP.
- The notation $\neq^{\mathrm{avp}}$ is the negation of $\approx^{\mathrm{avp}}$ discussed earlier.

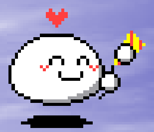
- Theorem: [Yamakami (1999)]

1. $\mathrm{BPP}_{\text{P-comp}} \subseteq$ Nearly-BPP.
2. NP $\not\subset$ Nearly-BPP, then P-comp $\neq^{\mathrm{avp}}$ IP_1-samp.
3. If strong one-way function exists, then NP $\not\subset$ Nearly-BPP.

Open Problems

- There are numerous open problems.

1. Does NP $\subseteq$ Nearly-BPP?
2. Does $\Delta_2^p \subseteq$ Nearly-BPP?
3. Does $\oplus$P $\subseteq$ Nearly-BPP?
4. Develop a nice theory of complexity classes Nearly-C for reasonable class C?



Thank you for listening

Q & A

I’m happy to take your question!

END