Space Bounded Randomized Complexity Classes

one-sided error, log space bounded classes

handy techniques for probabilistic reasoning

RLP

- A language L is in RLP if there is an log-space *and poly-time* PTM M such that
  - if $x \in L$ then $\Pr[M \text{ accepts } x] \geq 2/3$ and
  - if $x \notin L$ then $\Pr[M \text{ accepts } x] = 0$

UPATH is in RLP

- UPATH = { (G,s,t) | node t can be reached from node s in an *undirected* graph G}

UPATH is in RLP

UPATH Algorithm:

- On input (G,s,t), follow a random path from s
  - If t is reached at some step, halt and accept
  - If t is not reached within 6e(n-1) steps, halt and reject

- The algorithm is correct if t is not reachable from s, since it must reject

- What if t is reachable from s?

Analysis of UPATH

- Let $T(G,s,t)$ be the number of edges of G that are traversed on a random walk from s to t
- Claim: Expected value of $T(G,s,t) \leq 2e(n-1)$
- We can use the claim and Markov's inequality to show that the random walk algorithm accepts yes instances of UPATH with probability at least 2/3

Analysis of UPATH

- *Markov's Inequality*: If X is a nonnegative random variable and k is a positive real then

  $$\text{Prob}[X \geq k\, E[X]\,] \leq 1/k$$

- Let X be T(G,s,t), i.e., the number of edges of G that are traversed on a random walk from s to t

- Since the expected value of T(G,s,t) ≤ 2e(n-1), then the probability that a random walk from s takes at least 6e(n-1) steps to reach t is at most 1/3

Analysis of UPATH

- Let T(G,s,t) be the number of edges of G that are traversed on a random walk from s to t

- We still need to prove the claim that the expected value of T(G,s,t) $\leq$ 2e(n-1)

- We need some background on *Markov Chains*

Background on Markov Chains

A finite *Markov chain* with discrete time and stationary transition probabilities is an infinite sequence of random variables over some state space S

$X_0, X_1, X_2, \ldots,$

Background on Markov Chains

A finite *Markov chain* with discrete time and stationary transition probabilities is an infinite sequence of random variables over some state space S

$X_0, X_1, X_2, \ldots,$

such that for all i, j in S, $\text{Prob}[X_k = j \mid X_{k-1} = i] = P_{ij}$, where P_{ij} may depend on i and j but not on k

The matrix P is called the *transition matrix*

Background on Markov Chains

A finite *Markov chain* with discrete time and stationary transition probabilities is an infinite sequence pf random variables over some state space S

$X_0, X_1, X_2, \ldots,$

such that for all i, j in S, $\mathrm{Prob}[X_k = j \mid X_{k-1} = i] = P_{ij}$, where P_{ij} may depend on i and j but not on k

P_{ij}^{m} is the probability of reaching j from i in exactly m steps (there is an easy proof by induction on m)

Background on Markov Chains

A Markov Chain is *irreducible* if for all states i and j, there exists k such that

$$\text{Prob}[X_k = j \mid X_0 = i] > 0$$

Theorem: Let P be the transition matrix of an irreducible Markov Chain. Then $\boldsymbol{\pi}P = \boldsymbol{\pi}$ has a unique solution $\boldsymbol{\pi}$ up to constant multiplicative factors

If $\sum_i \boldsymbol{\pi}_i = 1$, $\boldsymbol{\pi}$ is sometimes referred to as the *stationary distribution* of the Markov chain

Markov Chains and Random Walks on Graphs

- For an undirected connected graph $G = (V,E)$, let
  - $N(u)$ be the set of neighbours of node u
  - $d(u) = |N(u)|$ be the degree of node u
- A random walk on G is an irreducible Markov chain with state space equal to V and with
  - $P_{uv} = 1/d(u)$, if $\{u,v\}$ is in E
  - $P_{uv} = 0$, if $\{u,v\}$ is not in E
- The stationary distribution $\boldsymbol{\pi}$ of this random walk is such that $\boldsymbol{\pi}_u = d(u)/2e$

Analysis of UPATH: Random Commutes

A *random commute* from i to j in G is a random walk starting at i that ends the first time it returns to i after having at some point visited j

Let θ_{ijuv} be the expected number of times edge {u,v} is visited from u to v on a random commute from i to j

Analysis of UPATH: Random Commutes

Claim: θ_{ijuv} is independent of v: for all v′ in N(u),

$$\theta_{ijuv} = \theta_{ijuv'}$$

Analysis of UPATH: Random Commutes

Claim: θ_{ijuv} is independent of v: for all v′ in N(u),

$$\theta_{ijuv} = \theta_{ijuv'}$$

Proof follows from fact that each time u is visited, it is equally likely that v or v' is visited next

Analysis of UPATH: Random Commutes

Claim: Let θ_{iju} be θ_{ijuv} for any v. Then θ_{iju} is independent of u.

Analysis of UPATH: Random Commutes

Claim: Let θ_{iju} be θ_{ijuv} for any v. Then θ_{iju} is independent of u.

Proof: The following identity holds for any u in V:

$$d(u)\ \theta_{iju} = \sum_{v \in N(u)} \theta_{ijv}$$

expected number of times a random commute from i to j leaves u

expected number of times a random commute from i to j enters u

Analysis of UPATH: Random Commutes

Claim: Let θ_{iju} be θ_{ijuv} for any v. Then θ_{iju} is independent of u.

Proof: The following identity holds for any u in V:

$$d(u)\ \theta_{iju} = \sum_{v \in N(u)} \theta_{ijv}$$
$$= \sum_{v \in N(u)} d(v)\ \theta_{ijv}\ 1/d((v)$$

expected number of times a random commute from i to j leaves u

expected number of times a random commute from i to j enters u

Analysis of UPATH: Random Commutes

Claim: Let θ_{iju} be θ_{ijuv} for any v. Then θ_{iju} is independent of u.

Proof: The following identity holds for any u in V:

$$
\begin{aligned}
d(u)\ \theta_{iju} &= \textstyle\sum_{v \in N(u)} \theta_{ijv} \\
&= \textstyle\sum_{v \in N(u)} d(v)\ \theta_{ijv}\ 1/d((v) \\
&= \textstyle\sum_{v \in V} d(v)\ \theta_{ijv}\ P_{vu}
\end{aligned}
$$

expected number of times a random commute from i to j leaves u

expected number of times a random commute from i to j enters u

Analysis of UPATH: Random Commutes

Claim: Let θ_{iju} be θ_{ijuv} for any v. Then θ_{iju} is independent of u.

Proof: The following identity holds for any u in V:

$$\begin{aligned} d(u)\ \theta_{iju} &= \textstyle\sum_{v \in N(u)} \theta_{ijv} \\ &= \textstyle\sum_{v \in N(u)} d(v)\ \theta_{ijv}\ 1/d((v) \\ &= \textstyle\sum_{v \in V} d(v)\ \theta_{ijv}\ P_{vu} \end{aligned}$$

Analysis of UPATH: Random Commutes

Claim: Let θ_{iju} be θ_{ijuv} for any v. Then θ_{iju} is independent of u.

Proof: The following identity holds for any u in V:

$$\begin{aligned} d(u)\ \theta_{iju} &= \textstyle\sum_{v \in N(u)} \theta_{ijv} \\ &= \textstyle\sum_{v \in N(u)} d(v)\ \theta_{ijv}\ 1/d((v) \\ &= \textstyle\sum_{v \in V} d(v)\ \theta_{ijv}\ P_{vu} \end{aligned}$$

So, the vector of terms $d(u)\ \theta_{iju}$ is a constant times the stationary distribution $\boldsymbol{\pi}$, where the constant is independent of u (but depends on i and j).

Analysis of UPATH: Back to T(G,s,t)

For an edge {i,j} of G, let T_{ij} be the expected time to reach j from i on a random walk starting at i

Claim: $T_{ij} \leq 2e$.

Proof: $T_{ij} \leq \sum_{\{u,v\}\in E} (\theta_{ijuv} + \theta_{ijvu}) = 2e\ \theta_{ijij} \leq 2e$

Analysis of UPATH: Back to $T(G,s,t)$

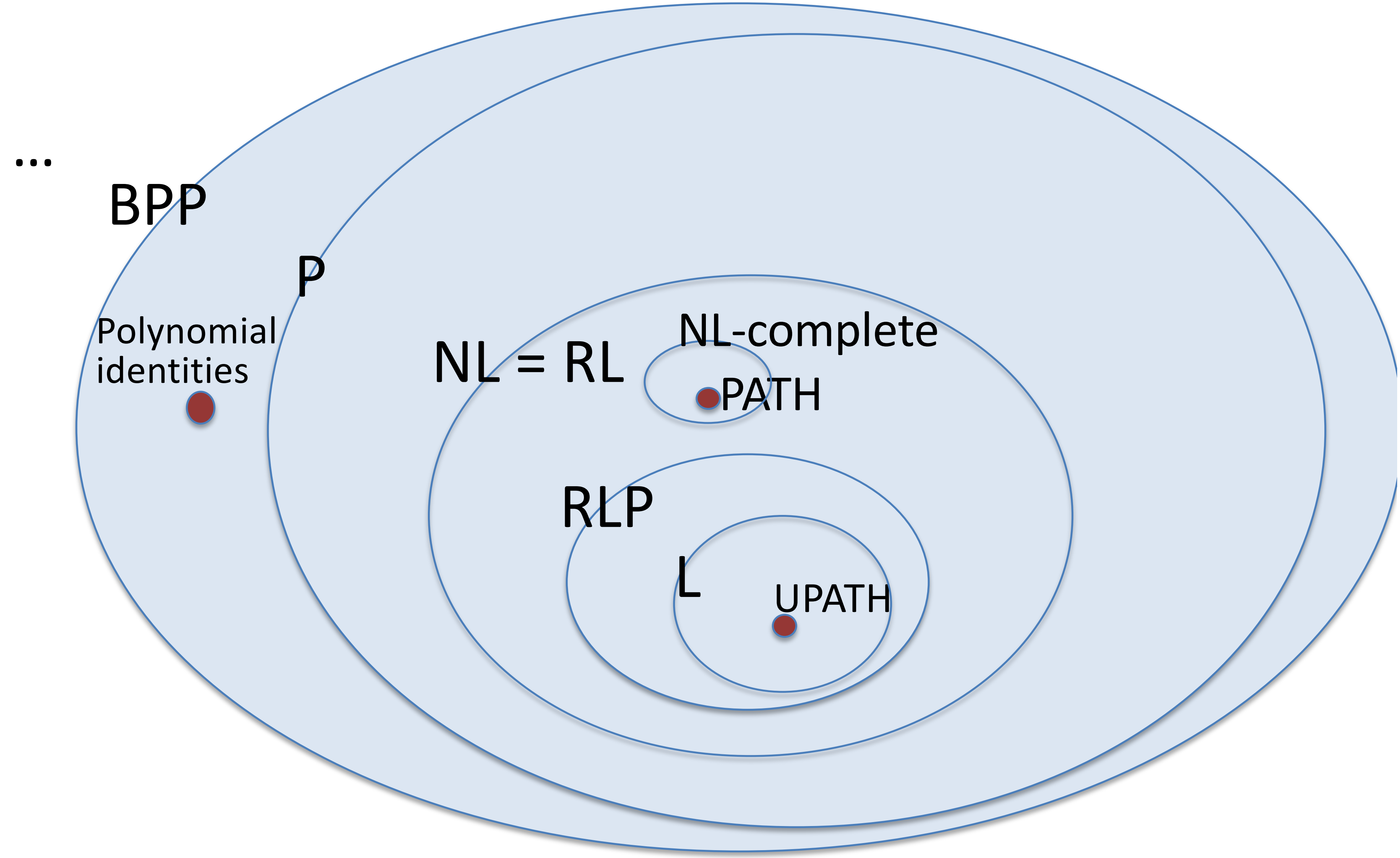
For an edge $\{i,j\}$ of G, let T_{ij} be the expected time to reach j from i on a random walk starting at i

Claim: $T_{ij} \leq 2e$.

Proof: $T_{ij} \leq \sum_{\{u,v\}\in E} (\theta_{ijuv} + \theta_{ijvu}) = 2e\ \theta_{ijij} \leq 2e$.

Finally: if p is a path of length at most n-1 from s to t, then $T(G,s,t) \leq \sum_{\{i,j\}\in p} T_{ij} \leq 2e(n-1)$

Summary



In fact, UPATH is in Log Space: Shown by Omer Reingold, 2004.

Summary

- Many conjecture that
  - BPP = P
  - RLP = L (here L is “log space”, see Reingold, Trevisan, Vadhan 2004)
- Reingold’s proof uses theory of graph expanders
- There’s an extensive body of work on pseudorandom generators, motivated in part by the goal of resolving these conjectures (see appendix of Arora-Barak)