The Complexity of Complexity

Eric Allender
Rutgers University

RodFest, January 5, 2017

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

The Complexity of Complexity
New Insights on the (Non)hardness of Circuit Minimization and Related Problems

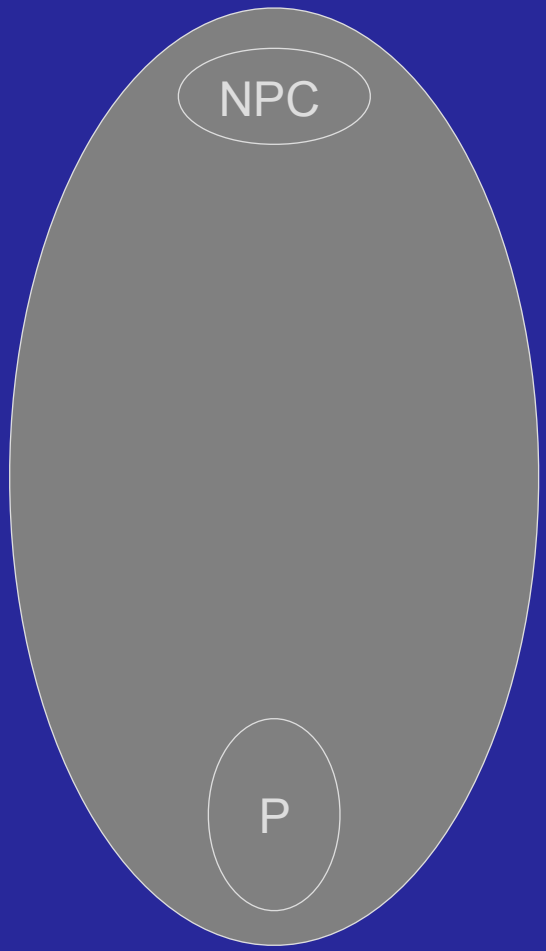
Eric Allender
Rutgers University

Joint work with
Shuichi Hirara (U. Tokyo)

RodFest, January 5, 2017

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

NP-Intermediate Problems



NP-Intermediate Problems

Ladner (1975) showed that intermediate problems exist unless P=NP.

But these problems are "unnatural".

NP-Intermediate Problems

Some prominent candidates were studied early on…

NP-Intermediate Problems

Some prominent candidates were studied early on…

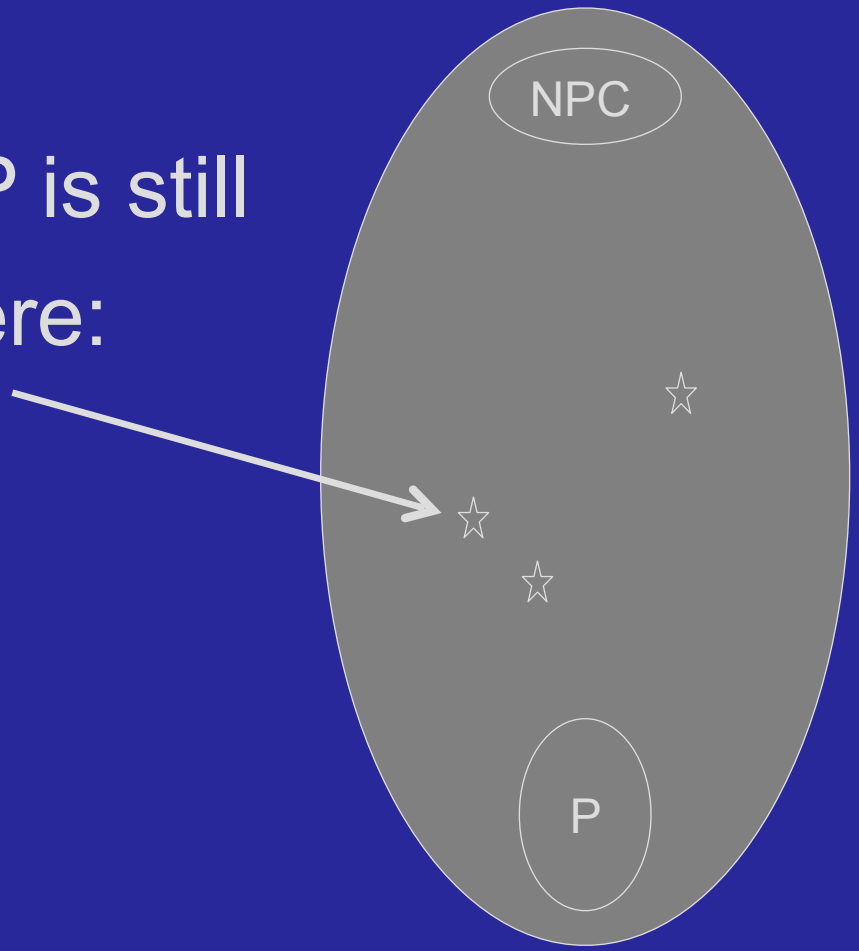
Graph Genus

Linear Programming

…but subsequently "moved".

NP-Intermediate Problems

MCSP is still here:



The Context

- The Minimum Circuit Size Problem (MCSP) = {(f,i) : f is the truth-table of a function that has a circuit of size ≤ i}.
- That is, MCSP is the overgraph of the "circuit size" complexity measure SIZE(f).

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

The Context

- The Minimum Circuit Size Problem (MCSP) = {(f,i) : f is the truth-table of a function that has a circuit of size ≤ i}.
- In NP, but not known (or widely believed) to be NP-complete. [Kabanets, Cai], [Murray, Williams], [A, Holden, Kabanets], [Hirahara, Watanabe]
- Lots of reasons to believe it's not in P.

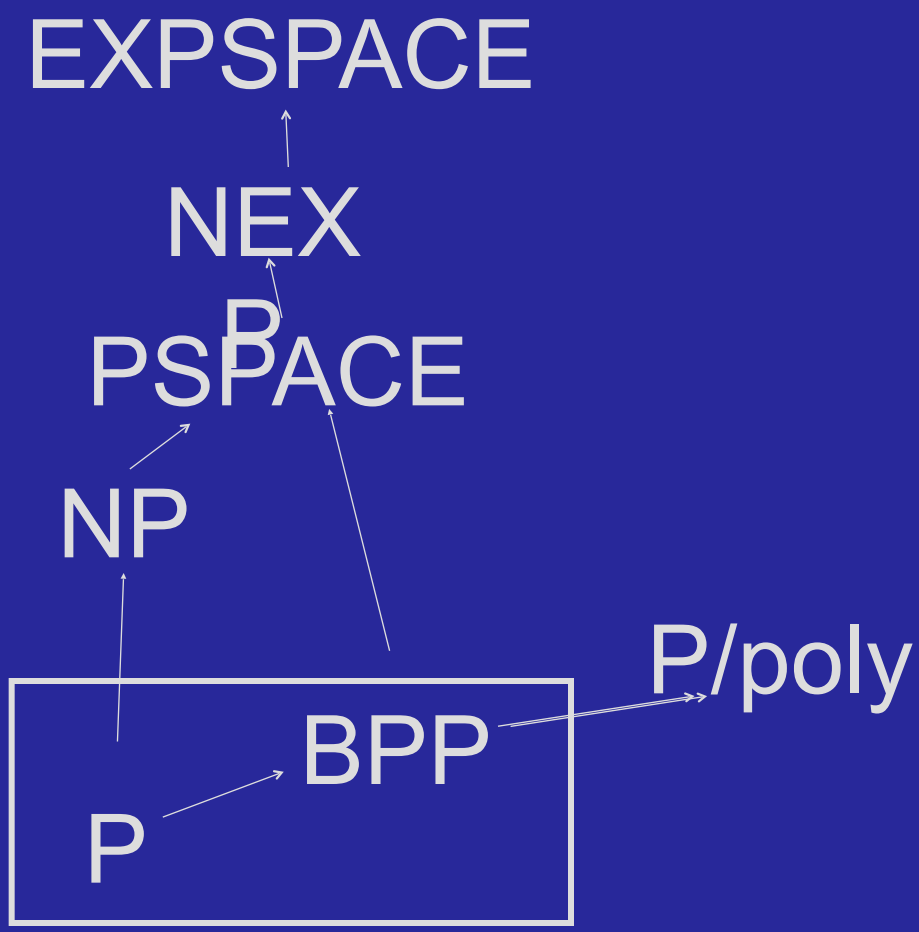
THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

More Context

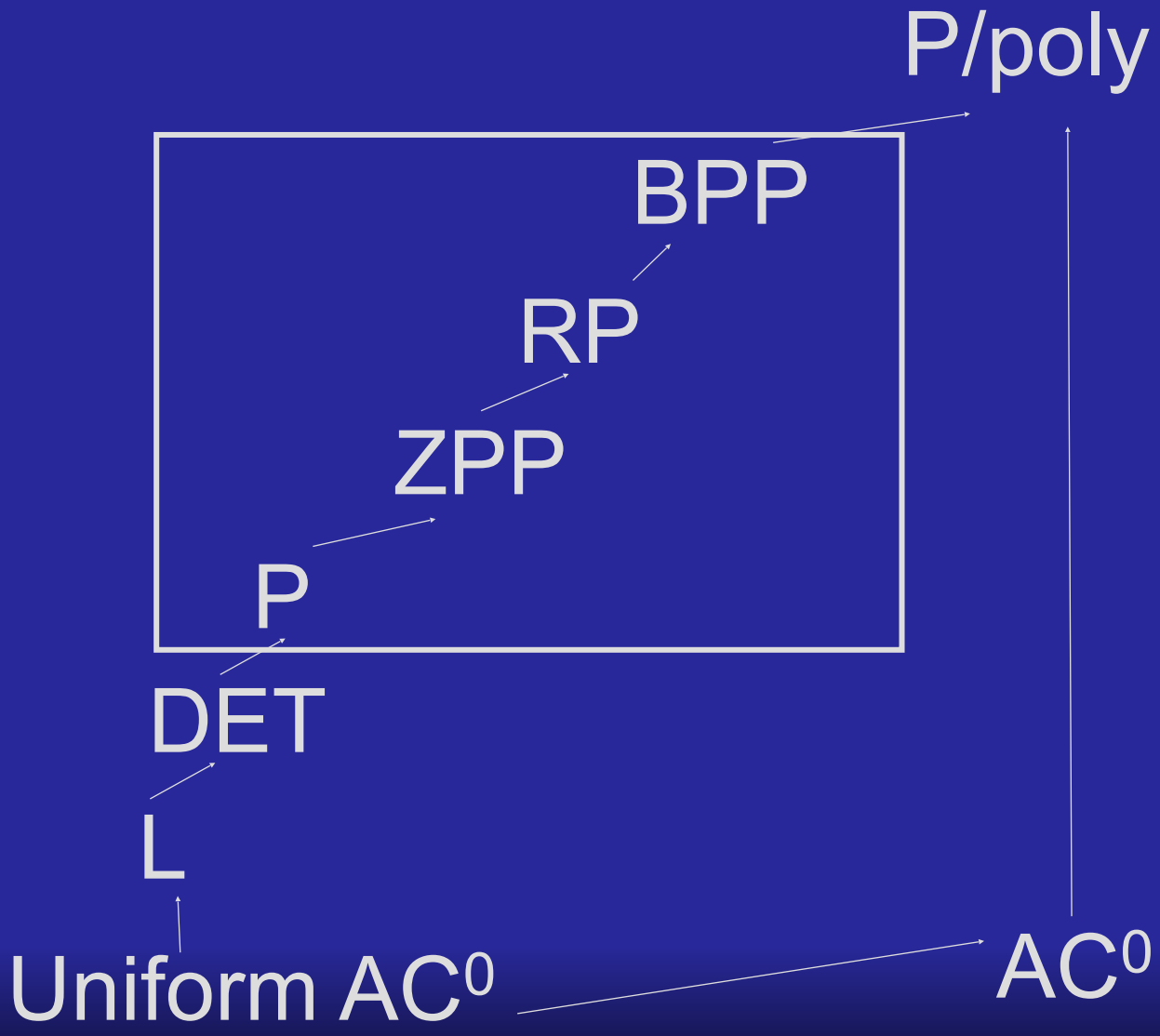
- MCSP is more like a family of problems, than a single problem.
- For instance "size" could mean "# of wires" or "# of gates", or "# of bits to describe the circuit", etc.
- None of these is known to be reducible to any other – but all can stand in for "MCSP".
- One more such variant:
  $O_{KT} = \{(x,i) : KT(x) \leq i\}$

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Complexity Classes



More Complexity Classes



THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Yet More Context

- Factoring and Discrete Log are in ZPP^{MCSP}.
- Graph Isomorphism is in RP^{MCSP}.
- Every promise problem in SZK is in (Promise) BPP^{MCSP}.

- But is MCSP NP-hard?

Statistical Zero Knowledge
SZK is contained in
NP/poly ∩ coNP/poly

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Yet More Context

- Factoring and Discrete Log are in ZPP^{MCSP}.
- Graph Isomorphism is in RP^{MCSP}.
- Every promise problem in SZK is in (Promise) BPP^{MCSP}.

- But is MCSP NP-hard?

All these hardness results use probabilistic reductions.

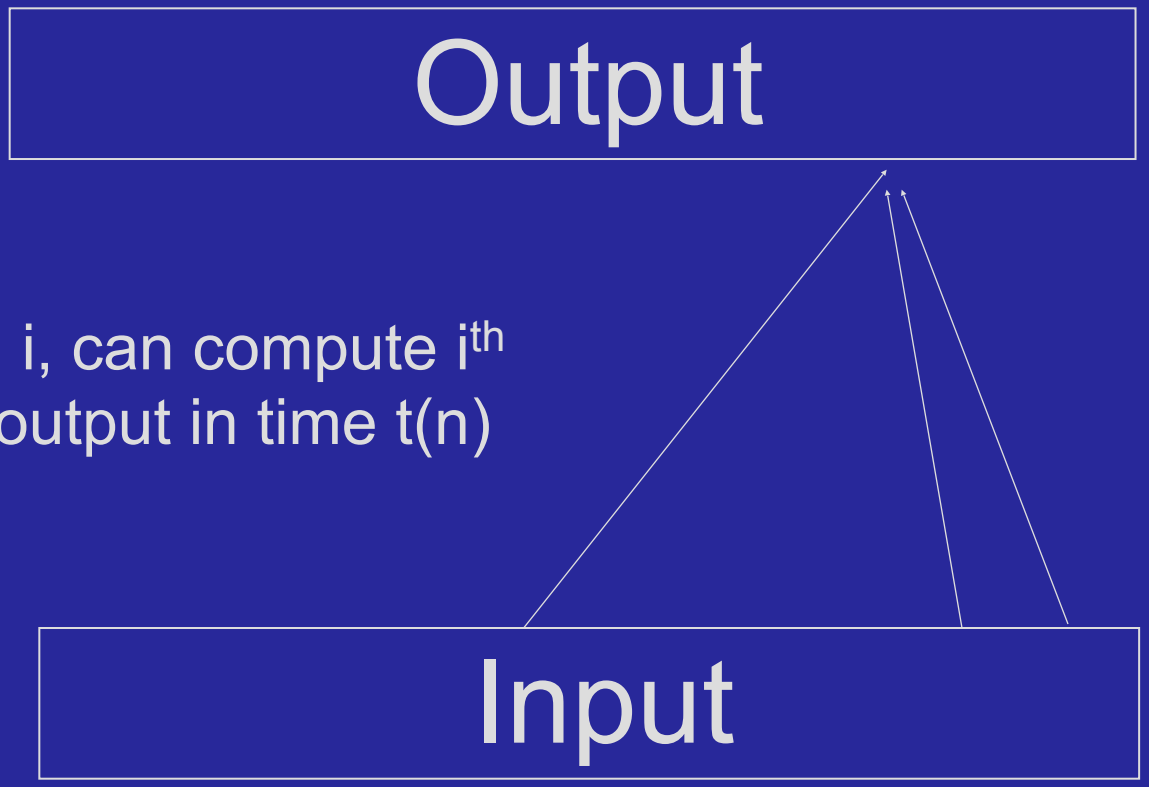
THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Consequences of Hardness

- From [MW],[AHK], we know:
- MCSP NP-hard under $\leq_m^p$ implies EXP ≠ ZPP.
- MCSP NP-hard under $\leq_m^{\log}$ implies PSPACE ≠ ZPP.
- MCSP NP-hard under $\leq_m^{AC^0}$ implies BPP= P, NP not in P/poly, DSPACE(n) not in SIZE($2^{\varepsilon n}$)
- MCSP NP-hard under TIME($\sqrt[3]{n}$) local reductions implies FALSE

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Local Reductions



Given i, can compute i^{th} bit of output in time t(n)

Local Reductions

- SAT is NP-complete under TIME(log n) local reductions.
- PARITY does *not* reduce to MCSP under TIME($\sqrt[3]{n}$) local reductions.
- How about NC^0 reductions?
  - For MCSP we still don't know.
  - For O_{KT}, we have a theorem:
  - O_{KT} *is hard for* DET under non-uniform NC^0 reductions.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

First Theorem

- O_{KT} is hard for DET under non-uniform NC^0 reductions.
- Corollary: O_{KT} is not in $AC^0[p]$ for any prime p.
- Circuit lower bounds imply O_{KT} is hard for DET under *uniform* AC^0–Turing reductions.
- O_{KT} hard for PARITY under these same uniform reductions implies (similar) circuit lower bounds.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

First Theorem

- O_{KT} is hard for DET under non-uniform NC^0 reductions.
- Corollary: O_{KT} is not in $AC^0[p]$ for any prime p.
- Independently, [Oliveira & Santhanam] have shown that DET reduces to MCSP via non-uniform TC^0 reductions. (This still leaves open the question of whether MCSP is in $AC^0[p]$.)

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

First Theorem

- O_{KT} is hard for DET under non-uniform NC^0 reductions.
- Corollary: O_K and O_C are hard for DET under non-uniform NC^0 reductions.
- Open question: Is O_K or O_C hard for P or hard for Σ^0_1 under non-uniform AC^0 or NC^0 $\leq_m$ reductions?
- Non-uniformity is key. No uniform $\leq_m$ reduction can reduce anything nontrivial to O_K or O_C.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

First Theorem

- O_{KT} is hard for DET under non-uniform NC^0 reductions.
- Corollary: O_K and O_C are hard for DET under non-uniform NC^0 reductions.
- Open question: Is O_K or O_C hard for P or hard for Σ^0_1 under non-uniform AC^0 or NC^0 $\leq_m$ reductions?
- O_K and O_C are hard for Σ^0_1 under (non-uniform) P/poly-Turing reductions [ABKMR].

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Three Bizarre Inclusions

- NEXP is contained in NP^{O_K} (for every U).

- PSPACE is contained in P^{O_K} (for every U).
- BPP is contained in $P_{tt}^{O_K}$ (for every U).
  - The decidable sets that are in $P_{tt}^{O_K}$ for every U are in PSPACE. [AFG11]
  - [CDELM] The sets that are in $P_{tt}^{O_K}$ for every U are decidable.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Three Bizarre Inclusions

- NEXP is contained in NP^{O_K} (for every U).
  - The sets that are in NP^{O_K} for every U are in EXPSPACE.
- PSPACE is contained in P^{O_K} (for every U).
- BPP is contained in $P_{tt}^{O_K}$ (for every U).
  - The sets that are in $P_{tt}^{O_K}$ for every U are in PSPACE.
- Thus there are reasons to care about efficient reductions to O_K and O_C.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Context for the 2nd Theorem

- Recall: Every promise problem in SZK is in (Promise) BPP^{MCSP}.
- SZK is usually defined in terms of "promise problems".

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Promise Problems

Ordinary decision problems.

Promise Problems

A "solution"

Ordinary decision problems.

Promise Problems.

Promise Problems

- A promise problem (Y,N) is NP-hard if SAT reduces to *every* solution.
- $Gap_\varepsilon MCSP$:
  - $Y = \{(f,s) : SIZE(f) < s/|f|^{1-\varepsilon(|f|)}\}$
  - $N = \{(f,s) : SIZE(f) > s\}$
- Note: $Gap_\varepsilon MCSP$ becomes easier when ε is smaller.
- If $\varepsilon(n) = o(1)$, then $Gap_\varepsilon MCSP \in DTIME(2^{n^{o(1)}})$.
- Related to Natural Proofs for $SIZE(2^{o(n)})$.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

The 2nd Theorem

- If cryptographically-secure one-way functions exist, then there is a function $\varepsilon(n)=o(1)$ such that
  - $\text{Gap}_{\varepsilon}\text{MCSP}$ is not in P/poly, and
  - $\text{Gap}_{\varepsilon}\text{MCSP}$ is not NP-hard under P/poly-Turing reductions.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

The 2nd Theorem

- If cryptographically-secure one-way functions exist, then there is a function $\varepsilon(n)=o(1)$ such that
  - $\mathrm{Gap}_{\varepsilon}\mathrm{O}_{\mathrm{KT}}$ is not in P/poly, and
  - $\mathrm{Gap}_{\varepsilon}\mathrm{O}_{\mathrm{KT}}$ is not NP-hard under P/poly-Turing reductions.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Three Bizarre Inclusions, Reprise

- NEXP is contained in NP^{GapO_K}, which is contained in EXPSPACE.
- PSPACE is contained in P^{GapO_K}.
- BPP is contained in $P_{tt}^{GapO_K}$, which is contained in PSPACE.
- I'm on record as conjecturing BPP = $P_{tt}^{O_K}$
- Might it be easier to show BPP = $P_{tt}^{GapO_K}$?
- In particular, is there an easier way than [CDELM] to show that $P_{tt}^{GapO_K}$ is decidable?

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

1st theorem (O_{KT} hard for DET)

- [Toran] showed that DET AC^0-reduces to the isomorphism problem for rigid graphs.
- [A,Grochow,Moore] showed that rigid graph isomorphism is in $RP^{O_{KT}}$. We'll modify that proof.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

1st Theorem: Proof

- On input (G_0, G_1)
  - Randomly pick a bit string $w = w_1 w_2 \ldots w_t$.
  - Pick random permutations $\pi_1 \ldots \pi_t$.
  - Let $z = w\pi_1(G_{w_1})\pi_2(G_{w_2})\ldots\pi_t(G_{w_t})$
- If G_0 and G_1 are not isomorphic, then z allows us to reconstruct w and $\pi_1 \ldots \pi_t$, so that z has (non-time-bounded) K-complexity around t+ts (where s = log n!), whp. Hence KT(z) > t+ts.
- Otherwise, KT(z) is around n^2+ts.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

1st Theorem: Proof

- On input (G_0,G_1)
  - Randomly pick a bit string $w=w_1w_2\ldots w_t$.
  - Pick random permutations $\pi_1\ldots\pi_t$.
  - Let $z= w\pi_1(G_{w_1})\pi_2(G_{w_2})\ldots\pi_t(G_{w_t})$
- The mapping $(G_0,G_1,\pi_1,\pi_2,\ldots\pi_t) \rightarrow z$ is computable in AC^0 if the permutations are presented as a list of the form $(i,\pi(i))$.
- But a random bit string is *not* going to encode a sequence of permutations.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

1st Theorem: Proof

- On input (G_0, G_1)
  - Randomly pick a bit string $w = w_1 w_2 \ldots w_t$.
  - Pick random permutations $\pi_1 \ldots \pi_t$.
  - Let $z = w\pi_1(G_{w_1})\pi_2(G_{w_2})\ldots\pi_t(G_{w_t})$
- Solution: There is a logspace-computable function f that takes $(nt)^{O(1)}$ random bits and with high probability outputs a (nearly)-uniformly random sequence $\pi_1, \pi_2, \ldots \pi_t$.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

1st Theorem: Proof

- On input (G_0,G_1)
  - Randomly pick a bit string $w=w_1w_2\ldots w_t$.
  - Pick random permutations $\pi_1\ldots\pi_t$.
  - Let $z= w\pi_1(G_{w_1})\pi_2(G_{w_2})\ldots\pi_t(G_{w_t})$
- Thus there is an AC^0 function g such that $g(G_0,G_1,f(r))$ is a probabilistic reduction from Rigid Graph Isomorphism to O_{KT}. Hardwiring in a good choice of f(r) yields a non-uniform AC^0 reduction.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

1st Theorem: Proof

- On input (G_0, G_1)
  - Randomly pick a bit string $w = w_1 w_2 \ldots w_t$.
  - Pick random permutations $\pi_1 \ldots \pi_t$.
  - Let $z = w\pi_1(G_{w_1})\pi_2(G_{w_2})\ldots\pi_t(G_{w_t})$
- Combining this with [Toran], O_{KT} is hard for DET under AC^0 reductions.
- Now, by [Agrawal,A,Rudich], O_{KT} is also hard for DET under NC^0 reductions.

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS

Congratulations, Rod!

- *Thanks!*

THE STATE UNIVERSITY OF NEW JERSEY RUTGERS