Relativizing Small Complexity Classes and their Theories

Klaus Aehlig, Stephen Cook, Phuong Nguyen

Relativisation

- Bounded Arithmetic theories corresponding to complexity classes
  ...and proof theory knows how to analyse arithmetic theories

? So why not use this to learn about computational complexity?

- need relativised theories
  ...and therefore relativised complexity classes

- Wishlist for relativising complexity classes
  - good closure properties (composition at the very least)
  - preserve known inclusions like $\mathsf{NC}^1 \subseteq \mathsf{L} \subseteq \mathsf{NL} \subseteq \mathsf{AC}^1$

Non-Determinism

- So, where's the problem—just add an oracle tape?
  (write only, not counted towards space restriction, ...)
- Consider the following NL^{L} algorithm for SAT
  - copy input, i.e., the formula φ to the oracle tape
  - non-deterministically write an assignment η to the oracle tape
  - in L can solve "given φ, η, does $\eta \models \varphi$?"
- But an L-oracle shouldn't be of any help to NL!

Non-Determinism: RST-restriction

- So, what went wrong?
- oracle tape exploited as additional storage
- shouldn't allow a query tape not accounted for

$\therefore$ Should think of the query as some "decoding of the work tape"
(note: queries might be longer than logarithmic)

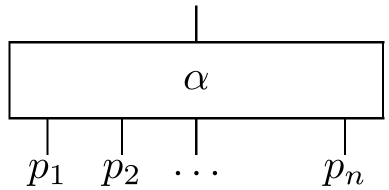
$\leadsto$ behave deterministic, unless the query tape is empty
(a restriction introduced by Ruzzo, Simon and Tompa)

$\boxed{\textbf{Composition}}$

- Want L^A to be closed under composition—*recall why* L *is*
- If M_1 and M_2 are L-TMs, we can compute the composition in L
  - just start simulating M_2
  - if the output of M_1 is used…
    re-run M_1 on a separate part of the work tape
    …till the needed output symbol is found
- But what if M_2 is in the in the middle of composing a query?
  Note: M_1 *does queries as well!*

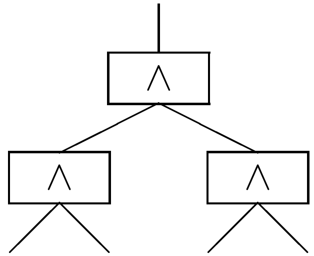
$\therefore$ Need more than one oracle tape
finitely many, organised stack like, suffice

$\boxed{\mathsf{AC}^k(\alpha)}$



- Back to circuits: less flexibility
- Oracle gate α with inputs $p_1, \dots, p_n$ *answers whether* $p_1 \dots p_n \in A \subset \{0,1\}^*$
- in the AC^k-hierarchy *all* gates have unbounded fan-in, *so just count it as a normal gate!*
- So, $\mathsf{AC}^k(\alpha)$ are (uniform) families of polynomial-size circuits of height $\leq C \cdot \log^k(n)$

$\mathsf{NC}^k(\alpha)$



- in NC^k only *binary* $\wedge$ and $\vee$-gates are allowed
- But binary oracle gates don't make sense!
  so, how to account for them?
- Use the embedding $\mathsf{AC}^k \subseteq \mathsf{NC}^{k+1}$ as guideline
  fan-in ℓ *gates translate to a group of height* $\log(\ell)$

! But still, the nesting depth of oracles remains $\log^k(n)$

- Count oracle gates always as height $\log n$
  …independent of the number of inputs
  think of it as asking for an element of $\alpha \subset \bigcup_{\ell \leq n} \{0,1\}^\ell$

Back to L^A and NL^A

- noticed already: L^A needs a stack of oracle tapes of at least constant height
- constant height is enough to get $\mathsf{NC}^1(\alpha) \subset \mathsf{L}^\alpha$
  - usual depth-first-search traversal of the circuit
  - note that NC^k has oracle nesting only $C \cdot \log^{k-1}(n)$
- ...and can't allow more if we want $\mathsf{NL}^\alpha \subset \mathsf{AC}^1(\alpha)$
  - Note "get the i'th symbol written on the oracle tape" is L-complete
  - hence: need circuit height $\log n$ for that
  - in total $d \cdot \log(n)$ for nesting depth d of the oracle gates

$\therefore$ oracle stack height $O(1)$ seems the "right" choice for L^A and NL^A

Complete Problems under $\mathsf{AC}^0(\alpha)$-reductions

- Recall: "what is the i'th symbol of the next oracle query" for an L-machine with only one query tape is an L-problem
- Hence $\mathsf{AC}^0(\alpha, \mathrm{LINE})$ can define the "big-step" graph of an L-machine with one query tape
- But given this graph, the problem for a two tape-machine…
  …and so on

$\therefore$ Line-reachability is L^α-complete under $\mathsf{AC}^0(\alpha)$-reductions
the <u>unrelativised</u> reachability problem!

- similar: graph-reachability for NL^α
- Corollary: NL^α closed under complement

Beyond the Definitions...

- Have seen: some unrelativised problems remain complete even for the relativised class
  ...so we can't expect relativisation here to help separating
- For the $\mathsf{AC}^k(\alpha)$-hierarchy can find a separating oracle
  (essentially iterate a function coded by this oracle)
- $\mathsf{AC}^0(\alpha)$ is first-order reduction with a new predicate symbol α
  so the complete problems canonically give rise to theories