Logarithmic space complexity and the conjugacy problem

Svetla Vassileva
McGill University
Joint work with A. Miasnikov

Group Theory International Webinar
October 31, 2013

The complexity zoo

- Google it! It's fun!
- "There are now 495 classes and counting"
- Questions.
  - Which is the right class for my needs?
  - Which classes are popular?
  - Why?
  - What makes a 'good' class?

What makes a complexity class 'good'?

- Robustness (e.g., closed under composition)
- Containing interesting problems
- Based on a 'reasonable' model of computation

A visitor's guide to the zoo

What are the characteristics of a complexity class?

- The model of computation
  - Turing machine
  - Boolean circuit
  - Random Access Machine (RAM)
- The resource being restricted
  - Time
  - Space
  - Depth
  - Fan-in
- The type of problem
  - decision problem
  - counting problem
  - function problem (aka search problem)
  - promise problem

Who is popular?

- P – the class of polynomial-time decidable functions
- NP – the class of functions decidable in polynomial time by a non-deterministic Turing machine.
- L – the class of functions decidable by a Turing machine using only space of logarithmic size in the input.
- TC^0 – the class of functions decidable by a boolean circuit of polynomial size and constant depth.

The 'right' complexity class

So every beast finds a mate, and from the same fact comes the proverb, 'There is no [problem], however ugly, that does not one day find a [class]. (Balzac, The maid of Thilouse)

- Reducing problems.
  - Given $A, B \subseteq \mathbb{N}$ and a set of functions $\mathcal{F}$, closed under composition, A is *reducible* to B if

$$\exists f \in \mathcal{F} \quad \forall x \in \mathbb{N}, \quad x \in A \Leftrightarrow f(x) \in B$$

  - A is $\mathcal{F}-$*equivalent* to B if A is reducible to B and B is reducible to A.
- Completeness. A problem P is complete in a class $\mathcal{C}$ if it is equivalent to every problem in this class with a 'suitable' choice for $\mathcal{F}$.
- 'suitable': the functions from $\mathcal{F}$ have to be 'efficient' with respect to the given class.

Examples of completeness from group theory

- Undecidable problems (void: they are all impossible)
  - some word problems (Novikov and Boone)
  - membership in free solvable groups of degree ≥ 3 (Umirbaev)
- NP-complete problems
  - The word problem for a (specific, complicated) finitely presented group (Birget, Olshanskii, Rips, Sapir)
  - The solvability problem for quadratic equations over free /hyperbolic groups (Kharlampovich, Lysenok, Miasnikov, Touikan /Kharlampovich, Mohajeri, Taam, Vdovina)
  - The subset sum problem in $\mathrm{BS}(1,2)$, $\mathbb{Z} \wr \mathbb{Z}$, free metabelian groups, Thompson's group (Miasnikov, Nikolaev, Ushakov)
- P-space complete problems
  - The existential theory of equations with rational constraints in free groups (Diekert, Gutierrez, Hagenah)
- TC^0-complete problems
  - Conjugacy problem in $\mathrm{BS}(1,2)$ (Diekert, Miasnikov, Weiss)
  - Nothing else known

The next best thing

- Completeness is precious and hard to prove
- Prove the lowest possible upper bound
- A typical progression

  polynomial time $\Rightarrow$ 'linear time' $\Longrightarrow$ logarithmic space $\Longrightarrow$ TC^0

Why space?

- Handling large data sets.
  - RAM vs. external storage
  - DNA sequencing
  - working with databases
  - the internet graph

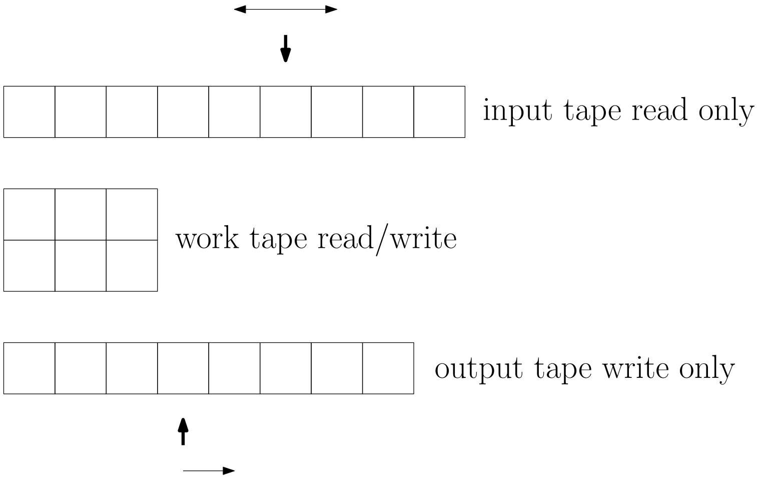
- Time complexity can really be due to space issues.
  - Gröbner bases
  - Start with basis for ideal and "blow it up" by adding polynomials
  - The $\underbrace{\text{number of polynomials}}_{space}$ we add is large

    $\Rightarrow$ the time complexity is large

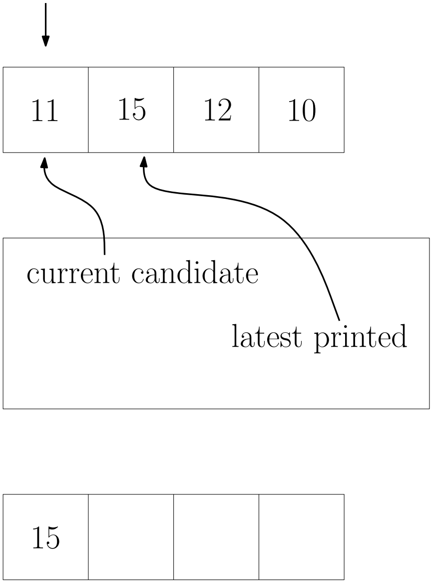
Log-space ⇒ P-time.

- Configurations cannot be repeated.
- Total number of configurations $\leq k(n + 2^{c \log n}) \sim n^c$
- P-time $\overset{?}{\Rightarrow}$ log-space: open problem.

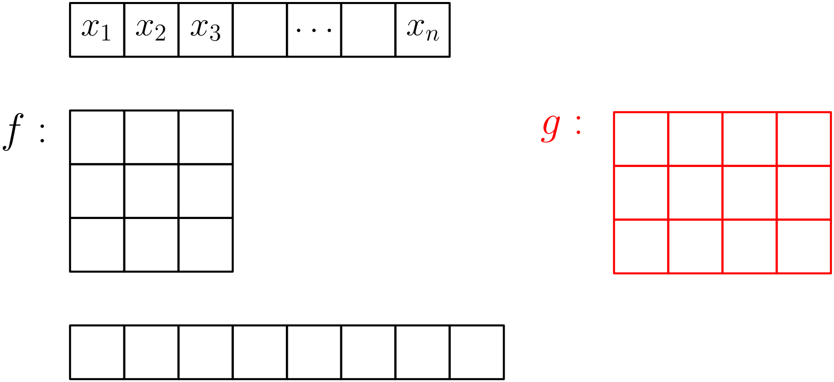
Log-space transducers



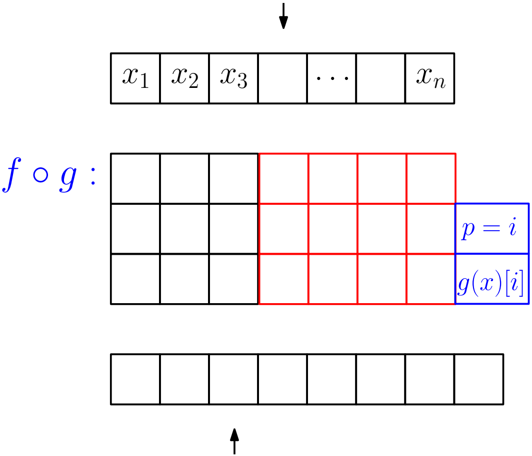
Example: sorting is in log-space



Log-space functions can be composed



Log-space functions can be composed



Some log-space computable problems

- WP in linear groups is log-space decidable (Zalcstein, Lipton).
- Normal forms in free groups are log-space computable (Lohrey, Ondrush/ Elder, Elston, Ostheimer).
- Normal forms in abelian groups are log-space computable (Elder, Elston, Ostheimer).
- Normal forms in wreath products are log-space computable (Elder, Elston, Ostheimer).
- Normal forms in RAAG are log-space computable (Diekert, Kausch, Lohrey).
- Normal forms in free metabelian groups (V.)

The conjugacy problem in log-space

- Grigorchuk group (Miasnikov, V.)
  - Double exponential time upper bound (Grigorchuk)
  - Polynomial time (Lysenok, Miasnikov, Ushakov)
  - Log-space (Miasnikov, V.)
- Wreath products
  - Decidable (Matthews)
  - Polynomial time (V.)
  - Log-space (Miasnikov, V.)
- Free solvable groups
  - Decidable (Remeslennikov, Sokolov)
  - Polynomial time (V.)
  - Log-space (Miasnikov, V.)

Conjugacy in Wreath Products and Important Corollaries

Wreath products

The *restricted wreath product* is the group:

$$A \wr B = \{bf \mid b \in B,\ f \in A^{(B)}\},$$

with multiplication defined by

$$bf \cdot cg = bc\, f^c g,$$

where

- $f^c(x) = f(xc^{-1})$ for $x \in B$.
- $A^{(B)}$ is the set of all functions from B to A of *finite support*.
- Multiplication in $A^{(B)}$ is given by $f \cdot g(x) = f(x)g(x)$.
- $1_{A^{(B)}}$ is the function $1 : B \to 1_A$.

Remark. B acts on $A^{(B)}$, so $A \wr B \simeq B \ltimes A^{(B)}$

A presentation for $A \wr B$

Let $A = \langle X \mid R_A \rangle$, $B = \langle Y \mid R_B \rangle$. Then

$$A \wr B = \left\langle X \cup Y \mid R_A,\ R_B,\ [a_1^{b_1}, a_2^{b_2}] \right\rangle,$$

where $a_1, a_2 \in A$ and $b_1, b_2 \in B$.

$$a^b \leftrightsquigarrow f_{a,b}(x) = \begin{cases} a & \text{if } x = b \\ 1 & \text{otherwise.} \end{cases}$$

- Any function $f \in A^{(B)}$ can be given as $\{(b_1, a_1), \ldots, (b_n, a_n)\}$
- Equivalently, $f = f_{a_1,b_1} \ldots f_{a_n,b_n} = f_{a_1,1}^{b_1} \ldots f_{a_n,1}^{b_n} \leftrightsquigarrow a_1^{b_1} \ldots a_n^{b_n}$.

Conjugacy in wreath products

- Let $x = bf, y = cg \in A \wr B$ be given.
- There exists $z = dh \in A \wr B$ such that $z^{-1}xz = y$ iff

$$d^{-1}bd = c \text{ and } g^d = h^b f h^{-1}.$$

- $g^d = h^b f h^{-1} \Leftrightarrow \forall x \in B, g^d(x) = h^b f h^{-1}(x).$
- Problems:
  - $\forall x \in B$ is a lot of elements to check for (but finite support).
  - Get rid of h.
  - Get rid of d.

A conjugacy criterion

- $T = \{t_i\}$ – set of $\langle b \rangle$- coset representatives for $\text{supp}(f) \cup \text{supp}(g)$
- $S = \{s_i\}$ – set of $\langle c \rangle$- coset representatives for $\text{supp}(f) \cup \text{supp}(g)$
- Define

$$\beta_i(f) = \prod_j f(t_i b^j) \text{ and } \gamma_i(f) = \prod_j f(s_i c^j).$$

Theorem (Matthews (modified))

In $A \wr B$, $bf \sim cg$ if and only if

- *$b \sim c$ in B and*
- *$\beta_i(f) \sim \gamma_i(g)$ in A for all i.*

CP in wreath products

Theorem (Miasnikov, V.)

Suppose that

- *the conjugacy problem in A is log-space decidable,*
- *the conjugacy problem in B is log-space decidable and*
- *the power problem in B is computable in log-space.*

Then the conjugacy problem in $A \wr B$ is also log-space decidable.

Power problem in G: Given two words x and y in generators of G, find the smallest integer n such that $x^n = y$.

Direct corollaries

Corollary

The conjugacy problem in a wreath product of two abelian groups is log-space decidable.

Example. The conjugacy problem in the lamplighter group $\mathbb{Z} \wr \mathbb{Z}_2$ is decidable in log-space.

Corollary

The conjugacy problem in the wreath product $F \wr \mathbb{Z}^2$ of a free group F and a free abelian group is decidable in log-space.

Iterated wreath products

Definition

The *left iterated wreath product*, $A^{n} \wr B$, of two groups A and B inductively as follows.

- $A^{1} \wr B = A \wr B$
- $A^{n} \wr B = A \wr (A^{n-1} \wr B)$

Corollary

Suppose that

- *the conjugacy problem in A is log-space decidable,*
- *the conjugacy problem in B is log-space decidable and*
- *the power problem in A and B is computable in log-space.*

Then the conjugacy problem in $A^{n} \wr B$ is also log-space decidable.

Free solvable groups

Definition

- The n^{th} *derived (commutator) subgroup* of a group G is
$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}],$$
where $G^{(1)} = G' = [G, G] = \langle [g, g'] \mid g, g' \in G \rangle$.
- The *free solvable group* $S_{d,r}$ of degree d and rank r is given by
$$S_{d,r} = {}^{F_r}\big/_{F_r^{(d)}}.$$

Conjugacy in free solvable groups

Corollary

The conjugacy problem in a free solvable group, $S_{d,r}$, of fixed rank r and degree d is decidable in logarithmic space.

Proof.

- The Magnus embedding is a map $\phi : S_{d,r} \hookrightarrow \mathbb{Z}^r \wr S_{d-1,r}$.
- The Magnus embedding is a Frattini embedding, i.e.,

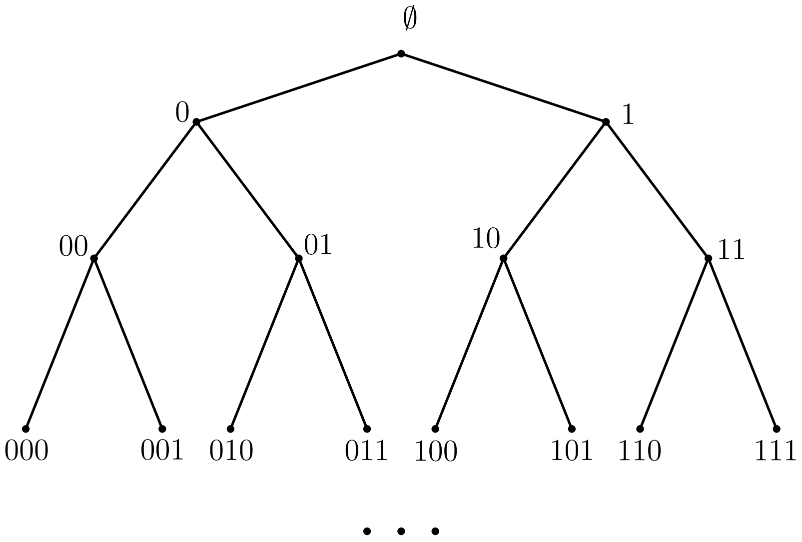
$$x \sim_{S_{d,r}} y \iff \phi(x) \sim_{\mathbb{Z}^r \wr S_{d-1,r}} \phi(y).$$

- Iterate the embedding to get

$$\begin{aligned} S_{d,r} &\hookrightarrow \mathbb{Z}^r \wr S_{d-1,r} \hookrightarrow \mathbb{Z}^r \wr \left(\mathbb{Z}^r \wr S_{d-2,r}\right) = {\mathbb{Z}^r}^2 \wr S_{d-2,r} \hookrightarrow \\ &\quad \ldots \\ &\hookrightarrow {\mathbb{Z}^r}^{d-1} \wr S_{1,r} = {\mathbb{Z}^r}^{d-1} \wr \mathbb{Z}^r. \end{aligned}$$

Conjugacy in the Grigorchuk group

The binary tree, $\mathcal{T}$



Automorphisms of the binary tree

- a acts by swapping the subtrees rooted at 0 and 1.
- $\psi : \mathrm{St}_{\mathrm{Aut}(\mathcal{T})}(1) \longrightarrow \mathrm{Aut}(\mathcal{T}) \times \mathrm{Aut}(\mathcal{T})$
- For $\alpha \in \mathrm{St}_{\mathrm{Aut}(\mathcal{T})}(1)$, write (α_0, α_1)
- Properties. For $g, h \in \mathrm{St}_{\mathrm{Aut}(\mathcal{T})}(1)$
  - $gh = (g_0 h_0, g_1 h_1)$
  - $aga = (g_1, g_0)$

The Grigorchuk group, Γ

$$\Gamma = \langle a, b, c, d \rangle$$

- a swaps subtrees rooted at 0 and 1.
- $b, c, d \in \mathrm{St}(1)$, with

$$b = (a, c), \quad c = (a, d), \quad d = (1, b).$$

- Obvious relations:
    - $a^2 = b^2 = c^2 = d^2 = 1$
    - $bc = cb = d$

Reduced words

- $\langle a \rangle \simeq \mathbb{Z}_2$, $\langle b, c, d \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathcal{F} = \mathbb{Z}_2 * \left(\mathbb{Z}_2 \times \mathbb{Z}_2\right)$
- $\Gamma = \mathcal{F}/S$.
- Every $w \in \mathcal{F}$ can be written as

$$w = u_0 a u_1 a \dots u_{k-1} a u_k,$$

$u_i \in \{b, c, d\}$ and u_0, u_k maybe trivial

The stabilizer subgroup and splitting

$$\mathrm{St}_{\Gamma}(1) = \mathrm{St}_{\mathrm{Aut}(\mathcal{T})}(1) \cap \Gamma$$

$\mathrm{St}_{\Gamma}(1) = \langle b, c, d, aba, aca, ada \rangle$

$$\psi : \mathrm{St}_{\Gamma}(1) \longrightarrow \Gamma \times \Gamma$$

- ψ is an injective homomorphism
- It is not surjective.

Conjugacy reduction

Let $u, v \in \mathcal{F}$ be two given reduced words.

- Assume (for simplicity) $u, v \in \mathrm{St}_\Gamma(1)$.
- If $\exists x\ x^{-1}ux = v$,
    - $x \in \mathrm{St}_\Gamma(1)$, so $x = (x_0, x_1)$.

$$\begin{aligned} x^{-1}ux = v \quad &\Leftrightarrow \quad (x_0^{-1}u_0x_0, x_1^{-1}u_1x_1) = (v_0, v_1) \\ &\Leftrightarrow \quad u_0 \sim v_0 \ \text{ and } \ u_1 \sim v_1 \end{aligned}$$

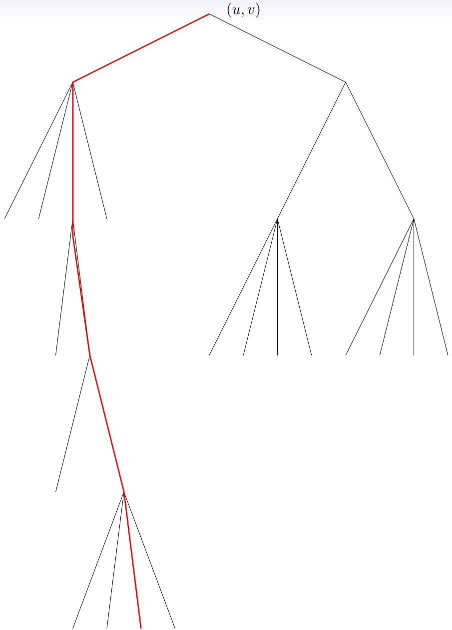
    - $x \notin \mathrm{St}_\Gamma(1)$, $ax = (y_0, y_1)$.

$$\begin{aligned} x^{-1}ux = v \quad &\Leftrightarrow \quad (x^{-1}a)(aua)(ax) = v \\ &\Leftrightarrow \quad (y_0^{-1}, y_1^{-1})(u_1, u_0)(y_0, y_1) = (v_0, v_1) \\ &\Leftrightarrow \quad u_1 \sim v_0 \ \text{ and } \ u_0 \sim v_1 \end{aligned}$$

Conjugacy reduction (ctd)

- If $u, v \in \mathrm{St}_\Gamma(1)$, we can deduce the conjugacy of u and v by considering conjugacy between u_0, u_1, v_0, v_1.
- If $u, v \notin \mathrm{St}_\Gamma(1)$, similar situation.
- If one of u, v is in $\mathrm{St}_\Gamma(1)$ and the other is not, then $u \nsim v$.

- Question. How much do we need to split?


(u, v)

- The height of this tree is logarithmic
  - Introduce a notion of length
  - Show this length decreases by half every time we split
- This means the tree can be traversed in log-space
- It follows we can deduce information about the root using the tree in log-space