Complexity Theory

Jan Křetínský

Chair for Foundations of Software Reliability
and Theoretical Computer Science
Technical University of Munich

Summer 2016

Based on slides by Jörg Kreiker

Lecture 11

Lower Bounds for SAT

Agenda

- big picture
- **TISP**
- lower bound for satisfiability

What is complexity all about?

- formalize the notion of computation
- resource consumption of computations
- depending on input size
- in the worst-case
- computing precise solutions

What is complexity all about?

- formalize the notion of computation
- resource consumption of computations
- depending on input size
- in the worst-case
- computing precise solutions

complexity classes

separation
lower bounds

Satisfiability

We cannot rule out that SAT could be solved in

- linear time or
- logarithmic space

Satisfiability

We cannot rule out that SAT could be solved in

- linear time or
- logarithmic space

Situation similar for many **NP**-complete problems.

What about restricting time and space simultaneously?

TISP

Definition (TISP)

Let $S, T : \mathbb{N} \to \mathbb{N}$ be constructible functions. A language $L \subseteq \{0,1\}^*$ is in the complexity class **TISP**$(T(n), S(n))$ if there exists a TM M deciding L in time $T(n)$ and space $S(n)$.

Note: **TISP**$(T(n), S(n)) \neq$ **DTIME**$(T(n)) \cap$ **SPACE**$(S(n))$

Agenda

- big picture ✓
- **TISP** ✓
- lower bound for satisfiability
- big picture

Lower Bound for Satisfiability

Theorem

SAT $\notin$ **TISP**$(n^{1.1}, n^{0.1})$.

In order to decide SAT we need

- either more than linear time
- or more than logarithmic space
- due to completeness this translates to any other problem in **NP**
- stronger results known (see further reading)

Proof – Big Picture

Proof is by contradiction. So assume

0. SAT $\in$ **TISP**$(n^{1.1}, n^{0.1})$
1. This implies **NTIME**$(n) \subseteq$ **TISP**$(n^{1.2}, n^{0.2})$
2. This implies **NTIME**$(n^{10}) \subseteq$ **TISP**(n^{12}, n^{02}) by padding
3. 1. also implies **NTIME**$(n) \subseteq$ **DTIME**$(n^{1.2})$
4. which implies $\mathbf{\Sigma_2}$**TIME**$(n^{8}) \subseteq$ **NTIME**$(n^{9.6})$
5. separately we can show **TISP**$(n^{12}, n^{2}) \subseteq$ $\mathbf{\Sigma_2}$**TIME**(n^{8})
6. (2,4,5) together establish **NTIME**$(n^{10}) \subseteq$ **NTIME**$(n^{9.6})$ contradicting the non-deterministic time hierarchy theorem

Proof – Part 1

- can be proven by careful observation of the Cook-Levin reduction.
- problem decided in **NTIME**$(T(n))$ can be formulated as satisfiability problem of size $T(n)\log(T(n))$
- every output bit of reduction computable in polylogarithmic time and space
- hence if SAT $\in$ **TISP**$(n^{1.1}, n^{0.1})$ then **NTIME**$(n) \subseteq$ **TISP**$(n^{1.2}, n^{0.2})$

Proof – Part 2 (padding)

- let $L \in \textbf{NTIME}(n^{10})$

Proof – Part 2 (padding)

- let $L \in \mathbf{NTIME}(n^{10})$
- define $L' = \{x1^{|x|^{10}} \mid x \in L\}$

Proof – Part 2 (padding)

- let $L \in \mathbf{NTIME}(n^{10})$
- define $L' = \{x1^{|x|^{10}} \mid x \in L\}$
- then $L' \in \mathbf{NTIME}(n)$

Proof – Part 2 (padding)

- let $L \in \mathbf{NTIME}(n^{10})$
- define $L' = \{x1^{|x|^{10}} \mid x \in L\}$
- then $L' \in \mathbf{NTIME}(n)$
- by part 1 of proof: $L' \in \mathbf{TISP}(n^{1.2}, n^{0.2})$
- thus $L \in \mathbf{TISP}(n^{12}, n^{2})$

Proof – Part 3

By definition of **TISP**.

Proof – Part 4

Definition

A language L is in $\mathbf{\Sigma_2 TIME}(n^8)$ iff there exists a TM M running in time $\mathcal{O}(n^8)$ and constants c, d such that

$$x \in L \text{ iff } \exists u \in \{0,1\}^{c|x|^8}.\ \forall v \in \{0,1\}^{d|x|^8}.\ M(x,u,v) = 1$$

Proof – Part 4

Definition

A language L is in $\mathbf{\Sigma_2 TIME}(n^8)$ iff there exists a TM M running in time $\mathcal{O}(n^8)$ and constants c, d such that

$$x \in L \text{ iff } \exists u \in \{0,1\}^{c|x|^8}.\ \forall v \in \{0,1\}^{d|x|^8}.\ M(x,u,v) = 1$$

- let $L \in \mathbf{\Sigma_2 TIME}(n^8)$

Proof – Part 4

Definition

A language L is in $\mathbf{\Sigma_2 TIME}(n^8)$ iff there exists a TM M running in time $\mathcal{O}(n^8)$ and constants c, d such that

$$x \in L \text{ iff } \exists u \in \{0,1\}^{c|x|^8}.\ \forall v \in \{0,1\}^{d|x|^8}.\ M(x,u,v) = 1$$

- let $L \in \mathbf{\Sigma_2 TIME}(n^8)$
- define $L' = \{(x,u) \mid \forall v \in \{0,1\}^{d|x|^8}.\ M(x,u,v) = 1\}$

Proof – Part 4

Definition

A language L is in $\mathbf{\Sigma_2 TIME}(n^8)$ iff there exists a TM M running in time $\mathcal{O}(n^8)$ and constants c, d such that

$$x \in L \text{ iff } \exists u \in \{0,1\}^{c|x|^8}.\ \forall v \in \{0,1\}^{d|x|^8}.\ M(x,u,v) = 1$$

- let $L \in \mathbf{\Sigma_2 TIME}(n^8)$
- define $L' = \{(x,u) \mid \forall v \in \{0,1\}^{d|x|^8}.\ M(x,u,v) = 1\}$
- hence $\overline{L'} \in \mathbf{NTIME}(n^8)$

Proof – Part 4

Definition

A language L is in $\mathbf{\Sigma_2 TIME}(n^8)$ iff there exists a TM M running in time $\mathcal{O}(n^8)$ and constants c, d such that

$$x \in L \text{ iff } \exists u \in \{0,1\}^{c|x|^8}. \forall v \in \{0,1\}^{d|x|^8}. M(x,u,v) = 1$$

- let $L \in \mathbf{\Sigma_2 TIME}(n^8)$
- define $L' = \{(x,u) \mid \forall v \in \{0,1\}^{d|x|^8}. M(x,u,v) = 1\}$
- hence $\overline{L'} \in \mathbf{NTIME}(n^8)$
- by premise we obtain $\overline{L'} \in \mathbf{DTIME}(n^{1.2*8})$ and also L'

Proof – Part 4

Definition

A language L is in $\mathbf{\Sigma_2 TIME}(n^8)$ iff there exists a TM M running in time $\mathcal{O}(n^8)$ and constants c, d such that

$$x \in L \text{ iff } \exists u \in \{0,1\}^{c|x|^8}.\ \forall v \in \{0,1\}^{d|x|^8}.\ M(x,u,v) = 1$$

- let $L \in \mathbf{\Sigma_2 TIME}(n^8)$
- define $L' = \{(x,u) \mid \forall v \in \{0,1\}^{d|x|^8}.\ M(x,u,v) = 1\}$
- hence $\overline{L'} \in \mathbf{NTIME}(n^8)$
- by premise we obtain $\overline{L'} \in \mathbf{DTIME}(n^{1.2*8})$ and also L'
- since $L = \{\exists u \in \{0,1\}^{c|x|^8} \mid (x,u) \in L'\}$ we obtain $L \in \mathbf{NTIME}(n^{9.6})$

Proof – Part 5

- let $L \in \textbf{TISP}(n^{12}, n^2)$

Proof – Part 5

- let $L \in \mathbf{TISP}(n^{12}, n^2)$
- then there exists a TM M such that $x \in \{0,1\}^n$ is accepted iff there is a path of length n^{12} in the configuration graph from C_{start} to C_{accept}

Proof – Part 5

- let $L \in \mathbf{TISP}(n^{12}, n^2)$
- then there exists a TM M such that $x \in \{0,1\}^n$ is accepted iff there is a path of length n^{12} in the configuration graph from C_{start} to C_{accept}
- where each configuration takes space $\mathcal{O}(n^2)$
- this is the case iff
  - there exist configurations $C_0, \ldots, C_{n^6}$ such that
  - $C_0 = C_{start}, C_{n^6} = C_{accept}$
  - for all $1 \leq i \leq n^6$ C_{i+1} is reachable from C_i in n^6 steps

Proof – Part 5

- let $L \in \mathbf{TISP}(n^{12}, n^2)$
- then there exists a TM M such that $x \in \{0,1\}^n$ is accepted iff there is a path of length n^{12} in the configuration graph from C_{start} to C_{accept}
- where each configuration takes space $\mathcal{O}(n^2)$
- this is the case iff
  - there exist configurations $C_0, \ldots, C_{n^6}$ such that
  - $C_0 = C_{start}$, $C_{n^6} = C_{accept}$
  - for all $1 \leq i \leq n^6$ C_{i+1} is reachable from C_i in n^6 steps
- this implies $L \in \mathbf{\Sigma_2 TIME}(n^8)$
- which can be equivalently characterized using alternating TMs

Agenda

- big picture ✓
- **TISP** ✓
- lower bound for satisfiability ✓

Summary of today's result

- SAT cannot be decided in linear time and, simultaneously, logarithmic space
- neither can any other problem in **NP**
- lower bounds are hard
- nice combination of proof techniques
  - padding
  - reductions
  - splitting paths in the configuration graph

Further Reading

- AB, Theorem 5.11
- original lower bound by *Fortnow*, Time-space tradeoffs for satisfiability, CCC 1997.
- current record: SAT $\notin$ **TISP**$(n^c, c^{\mathcal{O}(1)})$ for any $c < 2\cos(\pi/7)$
- by *R. Williams* Time-space tradeoffs for counting NP solutions modulo integers, CCC 2007.