The Complexity of Theorem-Proving Procedures

Stefanos Mitsis-Koutoukis

ALMA

February 2022

Query TMs

- Query Machine
  multitape TM
  query tape, query state

Query TMs

- Query Machine
  multitape TM
  query tape, query state
- T-computation
  set of strings T
  TM in query state, s in query tape
  $s \in T \Rightarrow$ TM in "yes" state
  $s \notin T \Rightarrow$ TM in "no" state

P-reducibility

S,T sets of strings
S P-red to T iff there is

P-reducibility

S,T sets of strings
S P-red to T iff there is

- qTM M
- polynomial $Q(n)$

P-reducibility

S,T sets of strings
S P-red to T iff there is

- qTM M
- polynomial $Q(n)$

T-computation of M with input w halts within $Q(|w|)$ steps

P-reducibility

S,T sets of strings
S P-red to T iff there is

- qTM M
- polynomial $Q(n)$

T-computation of M with input w halts within $Q(|w|)$ steps
P-red transitive
$(S, T) \in E$ iff S,T P-red to each other
E equivalence relation, deg(S) equivalence class containing S

P-reducibility

S,T sets of strings
S P-red to T iff there is

- qTM M
- polynomial $Q(n)$

T-computation of M with input w halts within $Q(|w|)$ steps
P-red transitive
$(S, T) \in E$ iff S,T P-red to each other
E equivalence relation, deg(S) equivalence class containing S
deg(S) polynomial degree of difficulty of S

P-reducibility

S,T sets of strings
S P-red to T iff there is

- qTM M
- polynomial $Q(n)$

T-computation of M with input w halts within $Q(|w|)$ steps
P-red transitive
$(S, T) \in E$ iff S,T P-red to each other
E equivalence relation, deg(S) equivalence class containing S
deg(S) polynomial degree of difficulty of S
$\mathcal{L}_* = deg(\{0\})$

Special sets of strings

- {subgraph pairs}

Special sets of strings

- {subgraph pairs}
- {isomorphic graphpairs}

Special sets of strings

- {subgraph pairs}
- {isomorphic graphpairs}
- {primes}

Special sets of strings

- {subgraph pairs}
- {isomorphic graphpairs}
- {primes}
- {DNF tautologies}

Special sets of strings

- $\{$subgraph pairs$\}$
- $\{$isomorphic graphpairs$\}$
- $\{$primes$\}$
- $\{$DNF tautologies$\}$
- D_3

Tautologyhood

M nondeterministic, accepts a set S of strings in time $Q(n)$
input w, $|w| = n$

Tautologyhood

M nondeterministic, accepts a set S of strings in time $Q(n)$
input w, $|w| = n$
$\{\sigma_1, \cdots, \sigma_l\}$ tape alphabet of M
$\{q_1, \cdots, q_r\}$ states of M
$T = Q(N)$ number of steps of the computation

Tautologyhood

- $P^i_{s,t}$, $i \in [1, l]$, $s, t \in [1, T]$
  true iff at step t, cell s contains σ_i

Tautologyhood

- $P^i_{s,t}$, $i \in [1, l]$, $s, t \in [1, T]$
  true iff at step t, cell s contains σ_i
- Q^j_t, $t \in [1, T]$, $j \in [1, r]$
  true iff at step t M is in state q_j

Tautologyhood

- $P^i_{s,t}$, $i \in [1, l]$, $s, t \in [1, T]$
  true iff at step t, cell s contains σ_i
- Q^j_t, $t \in [1, T]$, $j \in [1, r]$
  true iff at step t M is in state q_j
- $S_{s,t}$, $s, t \in [1, T]$
  true iff at step t M is scanning cell s

Tutologyhood

$B_t = (S_{1,t} \vee \cdots \vee S_{T,t}) \wedge (\bigwedge_{1 \leq i,j \leq T}(\neg(S_{i,t} \vee S_{j,t}))$ is true iff at step t M scans exactly one cell

$B = B_1 \wedge \cdots \wedge B_T$

Tutologyhood

$B_t = (S_{1,t} \vee \cdots \vee S_{T,t}) \wedge (\bigwedge_{1 \leq i,j \leq T}(\neg(S_{i,t} \vee S_{j,t}))$ is true iff at step t M scans exactly one cell

$B = B_1 \wedge \cdots \wedge B_T$

$C_{s,t}$ true iff at step t there exists exactly one symbol in cell s

$C = \bigwedge_{1 \leq s,t \leq T} C_{s,t}$

Tutologyhood

$B_t = (S_{1,t} \vee \cdots \vee S_{T,t}) \wedge (\bigwedge_{1 \leq i,j \leq T}(\neg(S_{i,t} \vee S_{j,t}))$ is true iff at step t M scans exactly one cell
$B = B_1 \wedge \cdots \wedge B_T$
$C_{s,t}$ true iff at step t there exists exactly one symbol in cell s
$C = \bigwedge_{1 \leq s,t \leq T} C_{s,t}$
D true iff at every step M is in exactly one state

Tutologyhood

$B_t = (S_{1,t} \vee \cdots \vee S_{T,t}) \wedge (\bigwedge_{1 \leq i,j \leq T}(\neg(S_{i,t} \vee S_{j,t}))$ is true iff at step t M scans exactly one cell

$B = B_1 \wedge \cdots \wedge B_T$

$C_{s,t}$ true iff at step t there exists exactly one symbol in cell s

$C = \bigwedge_{1 \leq s,t \leq T} C_{s,t}$

D true iff at every step M is in exactly one state

$E = Q_1^1 \wedge S_1^1 \wedge P_{1,1}^{i_1} \wedge \cdots \wedge P_{n,1}^{i_n} \wedge P_{n+1,1}^1 \wedge P_{T,1}^1$

$w = \sigma_{i_1} \cdots \sigma_{i_n}$, q_1 initial state, $\sigma_1 = \epsilon$

E true iff initial conditins for M are met

Tutologyhood

$B_t = (S_{1,t} \vee \cdots \vee S_{T,t}) \wedge (\bigwedge_{1 \leq i,j \leq T}(\neg(S_{i,t} \vee S_{j,t}))$ is true iff at step t M scans exactly one cell

$B = B_1 \wedge \cdots \wedge B_T$

$C_{s,t}$ true iff at step t there exists exactly one symbol in cell s

$C = \bigwedge_{1 \leq s,t \leq T} C_{s,t}$

D true iff at every step M is in exactly one state

$E = Q_1^1 \wedge S_1^1 \wedge P_{1,1}^{i_1} \wedge \cdots \wedge P_{n,1}^{i_n} \wedge P_{n+1,1}^1 \wedge P_{T,1}^1$

$w = \sigma_{i_1} \cdots \sigma_{i_n}$, q_1 initial state, $\sigma_1 = \epsilon$

E true iff initial conditins for M are met

F, G, H true iff truth values of P,Q,S are updated properly

Tutologyhood

$B_t = (S_{1,t} \vee \cdots \vee S_{T,t}) \wedge (\bigwedge_{1 \leq i,j \leq T}(\neg(S_{i,t} \vee S_{j,t}))$ is true iff at step t M scans exactly one cell

$B = B_1 \wedge \cdots \wedge B_T$

$C_{s,t}$ true iff at step t there exists exactly one symbol in cell s

$C = \bigwedge_{1 \leq s,t \leq T} C_{s,t}$

D true iff at every step M is in exactly one state

$E = Q_1^1 \wedge S_1^1 \wedge P_{1,1}^{i_1} \wedge \cdots \wedge P_{n,1}^{i_n} \wedge P_{n+1,1}^1 \wedge P_{T,1}^1$

$w = \sigma_{i_1} \cdots \sigma_{i_n}$, q_1 initial state, $\sigma_1 = \epsilon$

E true iff initial conditins for M are met

F, G, H true iff truth values of P,Q,S are updated properly

I true iff M is at "yes" state at some step $t \in [1, T]$

Tautologyhood

$$A(w) = B \wedge C \wedge D \wedge E \wedge F \wedge G \wedge H \wedge I$$

Tautologyhood

$A(w) = B \wedge C \wedge D \wedge E \wedge F \wedge G \wedge H \wedge I$
A satisfiable iff M accepts W, A in CNF

Tautologyhood

$A(w) = B \wedge C \wedge D \wedge E \wedge F \wedge G \wedge H \wedge I$
A satisfiable iff M accepts W, A in CNF
$\neg A$ tautology iff $w \notin S$, $\neg A$ in DNF

Tautologyhood

$A(w) = B \wedge C \wedge D \wedge E \wedge F \wedge G \wedge H \wedge I$
A satisfiable iff M accepts W, A in CNF
$\neg A$ tautology iff $w \notin S$, $\neg A$ in DNF
Clearly, the whole construction can be carried out in time bounded by a polynomial of $|w|$

Tautologyhood

$A(w) = B \wedge C \wedge D \wedge E \wedge F \wedge G \wedge H \wedge I$
A satisfiable iff M accepts W, A in CNF
$\neg A$ tautology iff $w \notin S$, $\neg A$ in DNF
Clearly, the whole construction can be carried out in time bounded by a polynomial of $|w|$
S is P-reducible to {DNF tautologies}
As a corollary, each of the "special sets of strings" is P-reducible to {DNF tautologies}

Reductions

$\{$tautologies$\}$, $\{$DNF tautologies$\}$, D_3, $\{$subgraph pairs$\}$
P-red to each other
By the previous corollary, each of the sets is P-red to $\{$DNF tautologies$\}$.

Reductions

$\{$tautologies$\}$, $\{$DNF tautologies$\}$, D_3, $\{$subgraph pairs$\}$
P-red to each other
By the previous corollary, each of the sets is P-red to $\{$DNF tautologies$\}$.
Obviously, $\{$DNF tautologies$\}$ is P-red to $\{$tautologies$\}$.

Reductions

$A = B_1 \vee \cdots \vee B_k$, $B_1 = R_1 \wedge \cdots_s$, each R_i atom or negation of an atom, $s > 3$
A in DNF

Reductions

$A = B_1 \vee \cdots \vee B_k$, $B_1 = R_1 \wedge \cdots_s$, each R_i atom or negation of an atom, $s > 3$
A in DNF
A is a tautology iff A' is a tautology, where
$A' = P \wedge R_3 \wedge \cdots_s \vee \neg P \wedge R_1 \wedge R_2 \wedge B_2 \wedge \cdots \wedge B_k$

Reductions

$A = B_1 \vee \cdots \vee B_k$, $B_1 = R_1 \wedge \cdots_s$, each R_i atom or negation of an atom, $s > 3$
A in DNF
A is a tautology iff A' is a tautology, where
$A' = P \wedge R_3 \wedge \cdots_s \vee \neg P \wedge R_1 \wedge R_2 \wedge B_2 \wedge \cdots \wedge B_k$
reduced number of conjuncts in B_1
process repeated until a formula with at most three conjuncts per disjunct is reached.

Reductions

$A = B_1 \vee \cdots \vee B_k$, $B_1 = R_1 \wedge \cdots_s$, each R_i atom or negation of an atom, $s > 3$
A in DNF
A is a tautology iff A' is a tautology, where
$A' = P \wedge R_3 \wedge \cdots_s \vee \neg P \wedge R_1 \wedge R_2 \wedge B_2 \wedge \cdots \wedge B_k$
reduced number of conjuncts in B_1
process repeated until a formula with at most three conjuncts per disjunct is reached.
This process is time-bounded by a polynomial in the length of A

Reductions

A formula in D_3, $A = C_1 \vee \cdots \vee C_k$, where $C_i = R_{i1} \wedge R_{i2} \wedge R_{i3}$

Reductions

A formula in D_3, $A = C_1 \vee \cdots \vee C_k$, where $C_i = R_{i1} \wedge R_{i2} \wedge R_{i3}$
$G_1 = K_k$ with vertices $\{v_1, \cdots, v_k\}$

Reductions

A formula in D_3, $A = C_1 \vee \cdots \vee C_k$, where $C_i = R_{i1} \wedge R_{i2} \wedge R_{i3}$
$G_1 = K_k$ with vertices $\{v_1, \cdots, v_k\}$
G_2 is the graph with vertices $\{u_{ij}\}$, $1 \leq i \leq k$, $1 \leq j \leq 3$ such that u_{ij} is connected by edge to u_{rs} iff $i \neq r$ and (R_{ij}, R_{rs}) not an opposite pair of literals.

Reductions

A formula in D_3, $A = C_1 \vee \cdots \vee C_k$, where $C_i = R_{i1} \wedge R_{i2} \wedge R_{i3}$
$G_1 = K_k$ with vertices $\{v_1, \cdots, v_k\}$
G_2 is the graph with vertices $\{u_{ij}\}$, $1 \leq i \leq k$, $1 \leq j \leq 3$ such that u_{ij} is connected by edge to u_{rs} iff $i \neq r$ and (R_{ij}, R_{rs}) not an opposite pair of literals.
Thus, there is a falsifying truth assignment to A iff there is a graph homomorphism $\phi : G_1 \longrightarrow G_2$ such that for each i, $\phi(i) = u_{ij}$ for some j

Predicate Calculus

TM M_Q and recursive function $T_Q(k)$. M_Q is of type Q and runs for $T_Q(k)$ steps iff
$M_Q(A)$ halts iff A is unsatisfiable, and for all k, if $\phi(A) \leq k$ and $|A| \leq log_2 k$, then M_Q halts within $T_Q(k)$ steps.
In this case, we will say that $T_Q(k)$ is of type Q.

Predicate Calculus

TM M_Q and recursive function $T_Q(k)$. M_Q is of type Q and runs for $T_Q(k)$ steps iff
$M_Q(A)$ halts iff A is unsatisfiable, and for all k, if $\phi(A) \leq k$ and $|A| \leq log_2 k$, then M_Q halts within $T_Q(k)$ steps.
In this case, we will say that $T_Q(k)$ is of type Q.
For any $T_Q(k)$ of type Q, $\frac{T_Q(k)}{\sqrt{k}/(log k)^2}$ is unbounded

Predicate Calculus

TM M_Q and recursive function $T_Q(k)$. M_Q is of type Q and runs for $T_Q(k)$ steps iff
$M_Q(A)$ halts iff A is unsatisfiable, and for all k, if $\phi(A) \leq k$ and $|A| \leq log_2 k$, then M_Q halts within $T_Q(k)$ steps.
In this case, we will say that $T_Q(k)$ is of type Q.
For any $T_Q(k)$ of type Q, $\frac{T_Q(k)}{\sqrt{k}/(logk)^2}$ is unbounded
There exists $T_Q(k)$ of type Q such that $T_Q(k) \leq k2^{k(logk)^2}$

ty

Thank you!