

Def: A Quantified Boolean Formula (QBF or qbf) Ψ has quantifiers $\forall x_i$ and $\exists x_i$ in addition to \neg, \vee, \wedge over variables. Usually we suppose all quantifiers are in front: $\Psi = (\exists x_1)(\exists x_2)(\forall x_3)(\exists x_4)\dots(\forall x_n)\phi$ where ϕ is an ordinary Boolean formula in $x_1 \dots x_n$ without quantifiers. Define TQBF = $\{ \text{QBFs } \Psi : \Psi \text{ is true} \}$. (Usually people drop the 'T' and just call it QBF)

We can kind-of consider SAT and TAUT to be subsets of QBF because:
 $\phi(x_1, \dots, x_n)$ is satisfiable iff the QBF $(\exists x_1)(\exists x_2)\dots(\exists x_n)\phi$ is true
 $\phi(x_1, \dots, x_n)$ is a tautology iff the QBF $(\forall x_1)(\forall x_2)\dots(\forall x_n)\phi$ is true.

Precisely, $\text{SAT} \leq_m^P \text{TQBF}$ and $\text{TAUT} \leq_m^P \text{TQBF}$ simply by prepending the appropriate quantifiers. In fact \leq_{\log}^m "In fact" they are AC⁰ reductions, but ignore ALR ch 20 §6. All

Theorem: TQBF is complete for PSPACE under \leq_{\log}^m , hence under \leq_m^P .

Proof: "In PSPACE":
 Thus TQBF is in O(n) space. 2^n leaves

Use $O(n)$ space to track the current branch in $\{0,1\}^n$ and the states of the quantified nodes along current branch. Accepted iff the root becomes good. All is done in $O(n)$ space.

$NP = coNP$ if and only if $\text{TAUT} \leq_m^P \text{SAT}$ or vice-versa. Hence if $\text{TQBF} \in NP$ then $\text{TQBF} \leq_m^P \text{SAT}$. So $\text{TAUT} \leq_m^P \text{SAT}$ by transitivity, so NP and coNP would collapse to each other.

$A \leq_{\log}^m B$ means $A \leq_m^P B$ since $L \leq P$.

Completeness: Let any $A \in \text{DSPACE}[S(n)]$ be given, where $S(n) = n^{O(1)}$. Then not only is $A \in \text{DTIME}[2^{O(S(n))}]$ but the maximum length $R(n)$ of any computation path that accepts (without cycling) is $2^{r(n)}$ where $r(n) = O(S(n))$.

Idea: "A Journey of a thousand miles... has a step that is exactly 500 miles from each side."

Take a ^{NTM}DTM M such that $L(M) = A$ and on $x \in \Sigma^n$, any accepting compⁿ has length at most $2^{r(n)}$ steps.

We can write a Boolean formula ϕ_0 with variables representing bit encoding IDs I, J such that an assignment to those variables satisfies ϕ_0 if and only if the corresponding IDs I, J give either $I=J$ or $I \stackrel{r}{\sim} J$.

We write this as $\phi_0(I, J) \equiv I=J \text{ or } I \stackrel{r}{\sim} J$, ie. "I goes to J in at most 1 step".

Now for $k \geq 1$ define a formula $\phi_k(I, J) \equiv I \text{ goes to } J \text{ in at most } 2^k \text{ steps}$ recursively by:

$$\phi_k(I, J) := (\exists K) \phi_{k-1}(I, K) \wedge \phi_{k-1}(K, J)$$

Since M runs in space $S(n)$, we may suppose $k=r$ here.

$\exists z_1, z_2, \dots, z_r$ where z_1, \dots, z_r are on ID

$$(\exists K)(\forall I')(J') [I'=I \wedge J'=K] \vee [I'=K \wedge J'=J] \rightarrow \phi_{k-1}(I', J')$$

$O(r(n))$

$k=r(n)$ down to 0.

Problem: The two-branch recursion blows ϕ_r up to size $2^{r(n)}$, which is too big.

Simple so we $O(\log n)$ Then we $\circ A$ In fact $NL(n)$

not only is $A \in \text{DTIME}[2^{O(S(n))}]$ but PSPACE under \leq_m^{\log} , hence under \leq_m^p .

from each side."

has length at most $2^{r(n)}$ steps.

at an assignment to those $I=J$ or $I \stackrel{r}{\sim} J$.

most 1 step" steps" recursively by:

Problem: The two-branch recursion blows ϕ_r up to $2^{r(n)}$, which is too big.

$$J'=J] \rightarrow \phi_{k-1}(I', J')$$

$k=r(n)$ down to 0.

Not only does this have only one recursive branch, but the recursion to produce the final output formula

$$\phi_{r(n)}(I_0(x), I_f)$$

Simply "unrolls" left-to-right, so we only need to keep track of $O(\log n)$ -sized indices of variables.

Then $x \in A \iff x \in L(M) \iff \phi_{r(n)}$ is true.

$\circ A \leq_m^{\log} \text{TQBF}$.

In fact, M can be an NTM, so $NL(n) \leq_m^p \text{TQBF}$ in $O(n^2)$ time

$n^2(r(n)^2)$ total size

$NP = coNP$

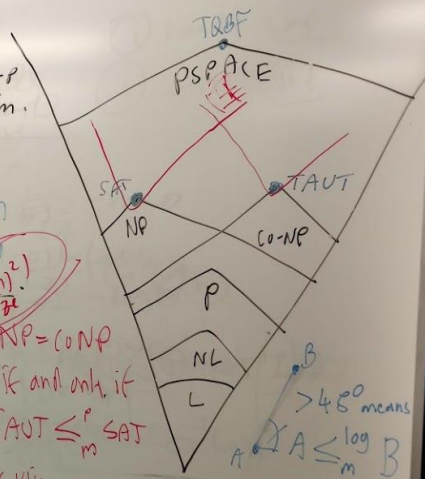
if and only if $\text{TQBF} \leq_m^p \text{SAT}$

or vice-versa

Hence if $\text{TQBF} \in NP$ then $\text{TQBF} \leq_m^p \text{SAT}$

So $\text{TQBF} \leq_m^p \text{SAT}$ by transitivity, so

NP and $coNP$ would collapse together.



hence $A \leq_m^p B$

Since $L \in P$.