

Interesting Fact: If $B \in PSPACE$ then $NP^B \in PSPACE$. Thus $NP^{TQBF} \in PSPACE \subseteq P^{TQBF}$.

Proof: Given any $A \in NP^B$,
 Take a poly-time NDTM N such that $A = L(N)$.
 Take some n^k space $\alpha(n)$ -bounded DTM M such that $L(M) = B$.

Build M' as follows:

Input x is written on a tape. A witness string $w \in \{0,1\}^{poly(n)}$ is written on a separate "Witness Tape".

For each w , simulate $N(x)$ with w as guesses deterministically. For each query y that it writes, simulate $M(y)$ and return the answer from M .

The point is that since $N(x)$ runs within time $poly(n)$, it cannot write any query string longer than that.

Worktapes of M , using up to $q(n) \leq \beta(poly(n))$ space.

All of M' takes up $O(poly(n)) = n^{O(1)}$ space.

$A = L(M')$ without oracle and without nondeterminism.

So $A \in PSPACE$, and since $A \in NP^B$ was arbitrary, $NP^B \in PSPACE$.

$\in PSPACE$. Thus $NP^{TQBF} \in PSPACE \subseteq P^{TQBF}$ because TQBF is complete under \leq_m^P , hence under \leq_T^P reductions.

$A = L(N)$ at $L(M) = B$. Taking $B = TQBF$ makes $NP^B = NP^{TQBF}$!

Meta Fact: Every theorem taught from Week 5 onward remains valid if the TMs concerned are DTMs with any fixed oracle B . E.g.

Thm: $D^B = \{ \langle m \rangle : M^B \text{ does not accept } \langle m \rangle \}$ does not equal $L(Q^B)$ for any DTM Q with oracle B . Hence it is not in RE^B nor "decidable in B ".

Thm: If $t_1(n) \log t_1(n) = o(t_2(n))$ (with $t_1(n) \geq n+1$ being full time (constructible) then for any B , $DTIME^B(t_1(n)) \subsetneq DTIME^B(t_2(n))$. The proof is transparently the same.

$\therefore NP \neq P$ cannot be proved using our basic techniques of metering and juggling inputs and outputs alone.

$NP^B \in PSPACE$ $A = L(M) = A$ without oracle and without nondeterminism.

There are also oracles C such that $NP^C \neq P^C$, so if $NP=P$ happens to be true, we won't be able to prove it by general techniques at the level of this course either.

The (IMO) Simplest Example Where Randomness Saves Time.

INSTANCE: There $n \times n$ matrices A, B, C .

Question: Is $AB = C$?

We can say this problem belongs to $\text{RTIME}[O(n^3)]$.

Doable by matrix multiplication in time $\tilde{O}(n^w)$ where $w \leq 2.3727...$ is best known. (but the " \tilde{O} " is a killer!)

However, if we can stand an ϵ -chance of saying "yes" when it's false, we can get $O(n^2)$ time.

- Guess a vector x of length n .

Computing $[C](x)$ takes only $O(n^2)$ time.

Do the computation $[A][B](x)$

If not equal, then we know $A \cdot B \neq C$, so reject.

Else: try another x' until we feel sure about saying 'yes'.

Fact: Over any field F , if $A \cdot B \neq C$, then

$$\Pr_{x \in F^n} [A \cdot B(x) \neq C(x)] \geq \frac{1}{2}$$

Equals $\frac{1}{2}$ when $F = \text{GF}(2)$, $n=1$.

Defn: A language decidable

• if

• if

If we get

If we get

Note the



Defn: A language A belongs to BPP if there is a witness predicate $R(x, y)$

decidable in $O(|x|^{O(1)})$ time with $|y| \leq q(|x|)$ for some polynomial q , such that:

- if $x \in A$ then $\Pr_{y \in \{0,1\}^{q(n)}} [R(x, y)] > \frac{3}{4}$

- if $x \notin A$ then $\Pr_{y \in \{0,1\}^{q(n)}} [R(x, y)] < \frac{1}{4}$

If we get this with " $= 1$ " in place of " $> 3/4$ " here, then $A \in \text{co-RP}$.

If we get this with " $= 0$ " in place of " $< 1/4$ " here, then $A \in \text{RP}$.

Note that the second condition makes $x \in A \Leftrightarrow \exists y R(x, y)$, so $\text{RP} \subseteq \text{NP}$.

PRIMES used to be the quintessential example for $A \in \text{co-RP}$.

Now we use PI1 Polynomial Identity Testing:

Just: A formula $\phi(x_1, \dots, x_n)$ over \mathbb{Z}_p , and a field F that might have lots of products of sums nested.

Ques: Is ϕ identically zero when multiplied out?

PI1 \in RP.

belongs to

" \tilde{O} " is a killer!

$O(n^2)$ time.

any field F , if then

$$\Pr_{x \in F^n} [A \cdot B(x) \neq C(x)] \geq \frac{1}{2}$$

equals $\frac{1}{2}$ when $F = \text{GF}(2)$, $n=1$.

