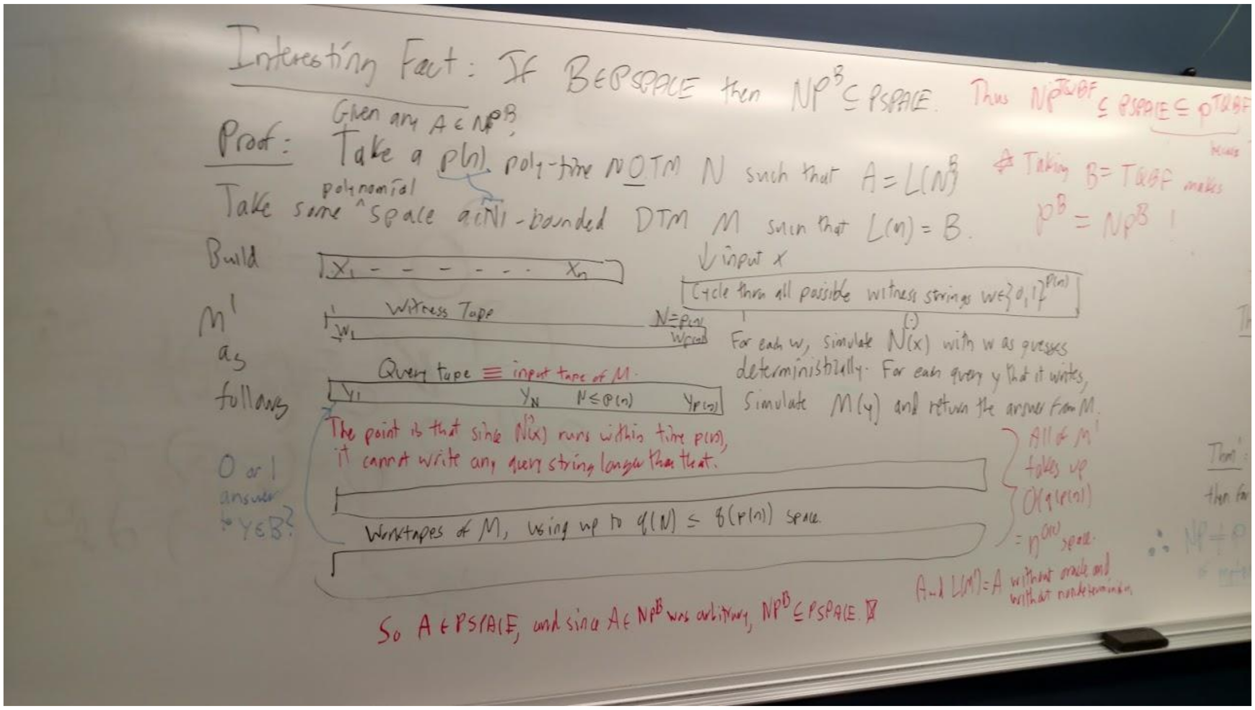
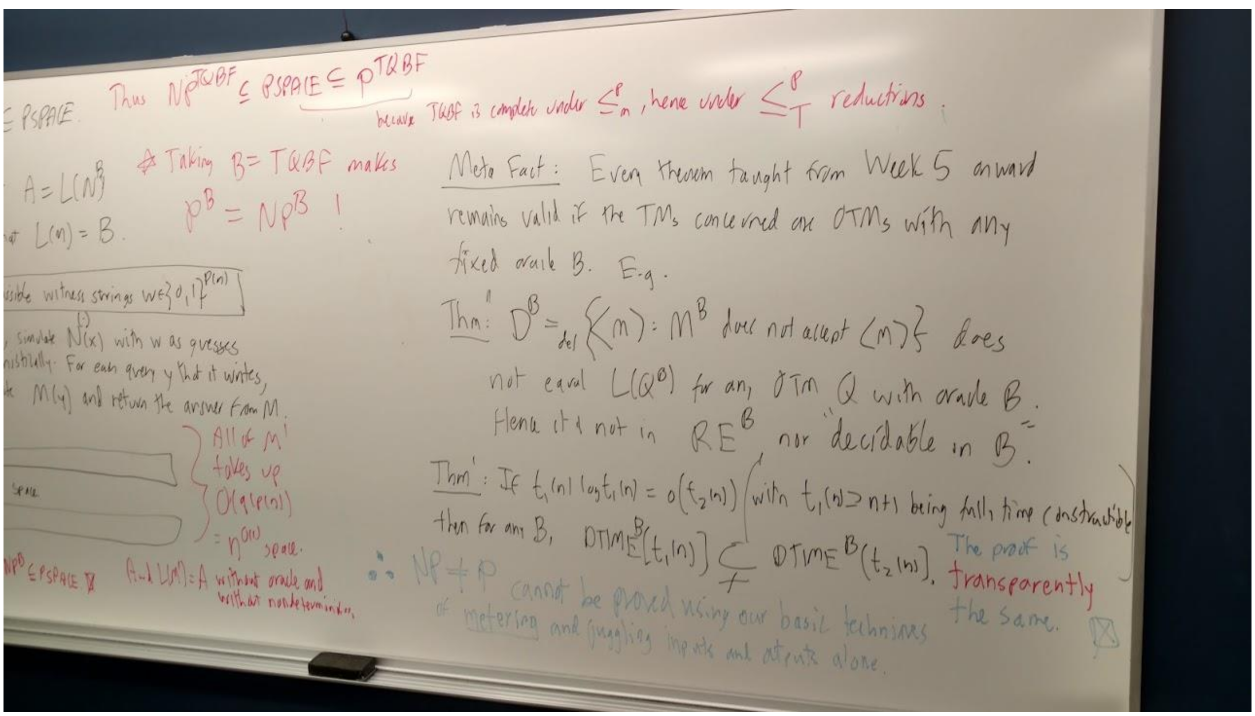
CSE596 Lecture Mon. Nov. 18, 2019





There are also oracles C such that NP^C != 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 (IMHO) Simplest Example Where Randomness Saves Time.

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

Question: Is $AB = C$?

We can say this problem belongs to "RTIME[$O(n^2)$]".

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

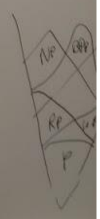
However, if we can stand an ε-chance of saying "yes" when it's false, we can get $O(n^2)$ time.

- Guess a vector x of length n.
  Computing $[C](x)$ takes only $O(n^2)$ time.
  Ditto computing $[A]([B](x))$.
  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

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

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



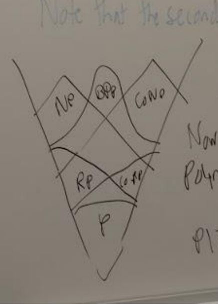
Defn: A language A belongs to BPP if there is a witness predicate $R(x,y)$ decidable in $O(|x|^{O(1)})$ time with $|y| \le q(|x|)$ for some polynomial q, such that:

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

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

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

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



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

Now we use PIT
Polynomial Identity Testing:

Inst: A formula $\phi(x_1, \ldots, x_n)$ over $+, \cdot$, and a field F that might have lots of products of sums nested.

Ques: Is ϕ identically zero when multiplied out?

PIT $\in$ RP.