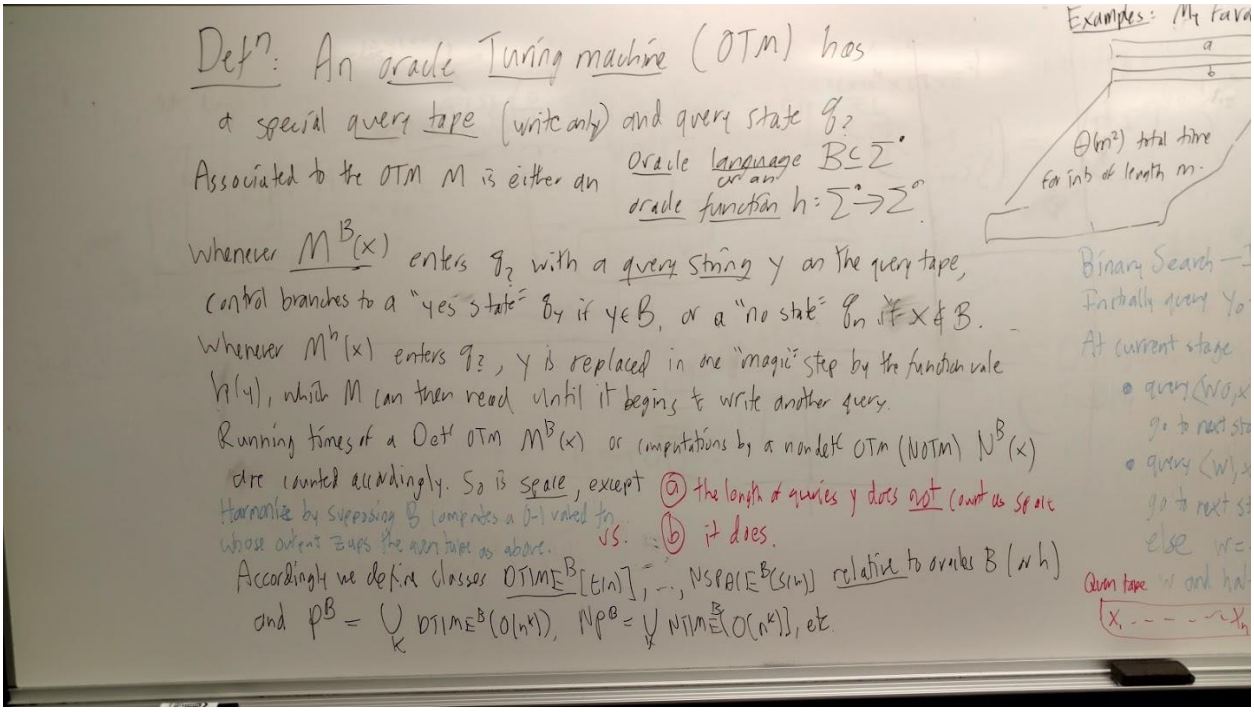
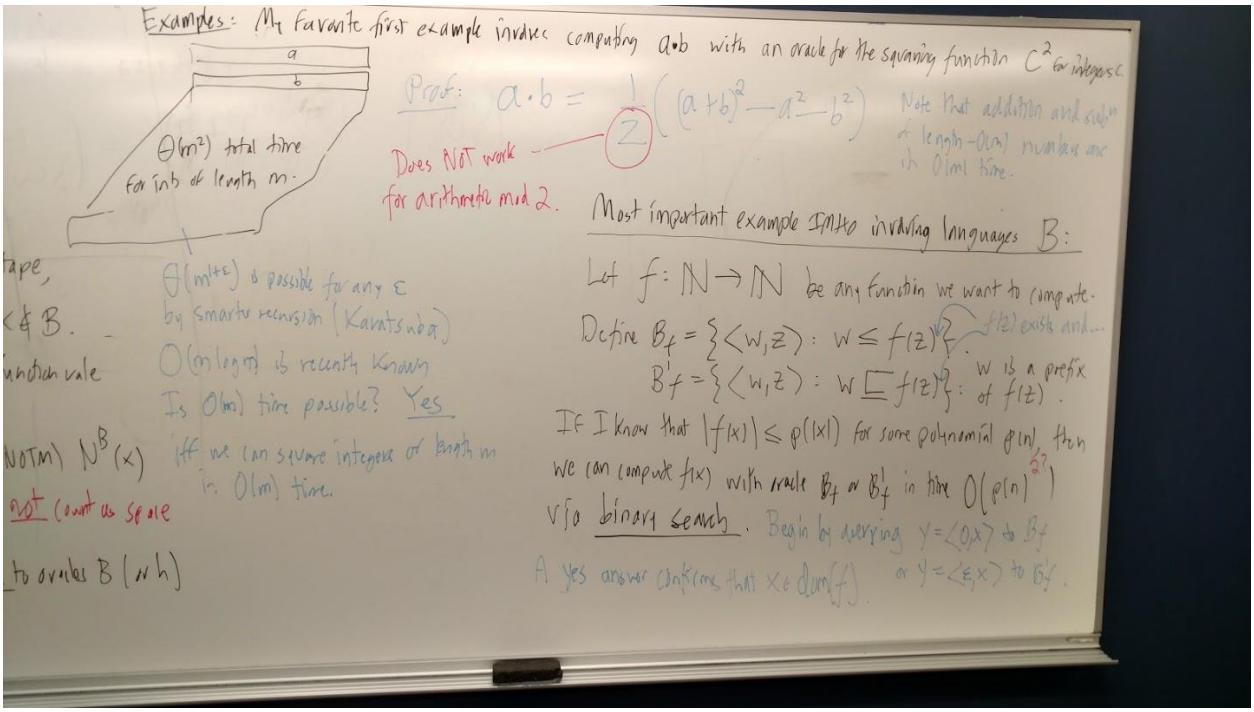
CSE596 Lecture Fri. 11/15/19:





Most important case: $f(m)$ = the unique prime factorization $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ of m.

B_f essentially $\approx \{\langle w, m\rangle : m$ has a prime factor q such that $w \le q\}$

This really pertains to the function $f_0(m)$ = the least prime factor of m ($= m$ if m is prime)

$B_{f'} = \{\langle w, m\rangle : w$ is a prefix of the unique (string encoding of) the prime factorization of $m\}$

FACT: B_f and $B_{f'}$ are both in $NP \cap coNP$.

Proof: To verify $\langle w, m\rangle \in B_f$, guess the unique prime factorization string $y = p_1^{a_1} \cdots p_k^{a_k}$ with each p_i prime and y evaluates to factor m

or $\in B_{f'}$

Verify

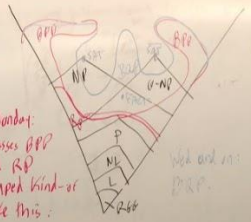
accept iff $w \le p_1$ for B_f

or $w \sqsubseteq y$ for $B_{f'}$.

More easily possible to verify since 2004 when the set of prime numbers was shown to be in P. (AKS 2004)

And to verify $\langle w, m\rangle \notin B_f$ or $\notin B_{f'}$, do the same guess and verify of y, but accept iff $w > p_1$ or if $w \not\sqsubseteq y$.

In both the "yes" and "no" cases the string y is a witness. Either B_f or $B_{f'}$ counts as the "one more" using FACT of course.



Monday: classes BPP and RP shaped kind-of like this:

Defn: A poly-time Turing reduces to B, written $A \le_T^P B$, if $A = L(M^B)$ for some det. oracle TM M that runs in $n^{O(1)}$ time with oracle B.

Then $P^B = \{A : A \le_T^P B\}$ and $A \le_m B \Rightarrow$ both $A \le_T^P B$ and $A \le_T^P \overline{B}$.

We computing $a \cdot b$

$a \cdot b = \frac{1}{2}((a+b)^2 - a^2 - b^2)$

Most important

Let $f: \mathbb{N}$

Define B_f = $B_{f'}$ =

If I know that

we can compute $f(m)$

via binary search

Yes answer confirm

Fact: $(v \le V) \vee (v$