

Defⁿ: An oracle Turing machine (OTM) has a special query tape (write only) and query state $q_?$. Associated to the OTM M is either an oracle language $B \subseteq \Sigma^*$ or an oracle function $h: \Sigma^* \rightarrow \Sigma^*$.

Whenever $M^B(x)$ enters $q_?$ with a query string y on the query tape, control branches to a "yes state" q_y if $y \in B$, or a "no state" q_n if $y \notin B$.

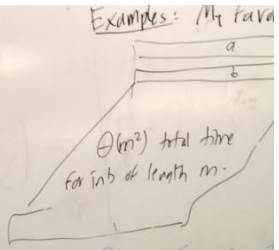
Whenever $M^h(x)$ enters $q_?$, y is replaced in one "magic step" by the function value $h(y)$, which M can then read until it begins to write another query.

Running times of a Det^d OTM $M^B(x)$ or computations by a nondet OTM (NOTM) $N^B(x)$ are counted accordingly. So is space, except the length of queries y does not count as space (vs. it does).

Harmonize by supposing B comprises a 0-1 valued function whose output equals the query tape as above.

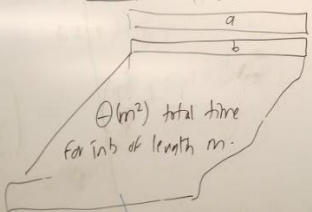
Accordingly we define classes $DTIME^B[\epsilon(n)]$, \dots , $NSPACE^B[\epsilon(n)]$ relative to oracle B (w/h) and $P^B = \bigcup_k DTIME^B(O(kn))$, $NP^B = \bigcup_k NTIME^B(O(kn))$, etc.

Examples: My favorite



Binary Search —
Initially query y_0
At current stage
• query $\langle w, x \rangle$
go to next state
• query $\langle w, x \rangle$
go to next state
else $w = x$
Query tape w and $h(w)$
 $x_1 \dots x_n$

Examples: My favorite first example involves computing $a \cdot b$ with an oracle for the squaring function C^2 for integers.



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

Does Not work for arithmetic mod 2.

Note that addition and subtraction of length- $O(m)$ numbers are in $O(m)$ time.

Most important example involves involving languages B :

Let $f: \mathbb{N} \rightarrow \mathbb{N}$ be any function we want to compute.

Define $B_f = \{ \langle w, z \rangle : w \leq f(z) \}$ (if $f(z)$ exists and...)

$B'_f = \{ \langle w, z \rangle : w \sqsubseteq f(z) \}$ (w is a prefix of $f(z)$)

If I know that $|f(x)| \leq p(|x|)$ for some polynomial $p(n)$, then we can compute $f(x)$ with oracle B_f or B'_f in time $O(p(n))$.

v/o binary search. Begin by querying $y = \langle 0, x \rangle$ to B_f or $y = \langle \epsilon, x \rangle$ to B'_f . A yes answer confirms that $x \in \text{dom}(f)$.

$\Theta(m \log m)$ is possible for any ϵ by smarter recursion (Karatsuba)

$O(m \log m)$ is recently known

Is $O(m)$ time possible? Yes

If we can square integers of length m in $O(m)$ time.

not count as space

to oracle B (w/h)

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

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

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

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

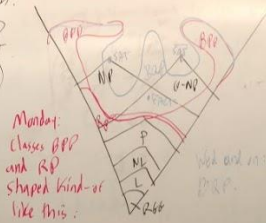
FACT: B_f and $B_{f'}$ are both in $NP \cap coNP$.

Proof: To verify $\langle w, m \rangle \in B_f$, guess the unique prime factorization string $y = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and verify $y = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ with each p_i prime and y evaluates to become m .

And to verify $\langle w, m \rangle \notin B_f$ or $\notin B_{f'}$, assert iff $w \leq p_1$ for B_f or $w \leq y$ for $B_{f'}$.

do the same guess and verify of y , but

accept iff $w > p_1$ or iff $w \not\leq y$. In both the "yes" and "no" cases the string y is a witness. (Either B_f or $B_{f'}$ is in the language since FACT is coNP.)



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

Def'n: A polynomial-time Turing reduces to B, written $A \leq_P B$, if $A = L(M)$ for some deterministic M that runs in polynomial time with oracle B.

Then $P^B = \{ A : A \leq_P B \}$ and $A \leq_m B \Rightarrow$ both $A \leq_P B$ and $A \leq_{P'} B$.

see complexity class

$$a \cdot b = \sum_{i=1}^n a_i b_i$$

Most important

Let $f: \mathbb{N} \rightarrow \mathbb{N}$

Define $B_f = \{ \langle w, m \rangle : m \text{ has a prime factor } q \text{ such that } w \leq q \}$

If I know that f we can compute $f(x)$

v/o binary search

yes answer (string)

Fact: $(w < v) \vee (w > v)$

More easily possible to verify since 2004 when the set of prime numbers was shown to be in P_1 (AKS 2002)