Monday, April 2, 2018 8:17 AM

Computational Resources: running time.
memory / space.
parallelism.
randomness.
rounds of interaction.

Decidability: unlimited resources.

Big Questions:

Comp	Q	
No	$P \stackrel{?}{=} NP$	finding a solution = verifying a solution.
No	$P \stackrel{?}{=} NC$	can every alg be parallelized?
No	$P \stackrel{?}{=} L$	can every efficient alg use a small amt of memory
NO	$EXP \stackrel{?}{\subseteq} P/poly$	are there small circuits to solve ~~the~~ every prob that uses exp time.
YES	$P \stackrel{?}{=} BPP$.	Can every rand alg be de-randomized?

Monday, April 2, 2018 8:17 AM

Encoding:

ex: Graph s, t.

$\Sigma = \{ (\ ) , ; 0, 1, \ldots, 9 \}$

#vertices; $(\_,\_)(\_,\_)(\_,\_)$

No unary encoding.

N in binary $\log(N)$ bits.
in unary N characters.

Given an encoding: computational problem.

$f: \Sigma^* \longrightarrow \Sigma^*$

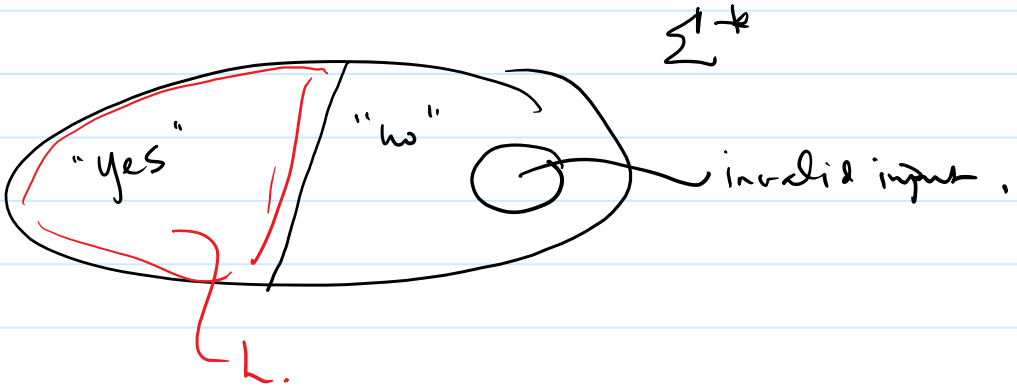
Decision problem: $f: \Sigma^* \longrightarrow \{yes, no\}$.

Search: Input: int N.
Output: prime factorization of N.

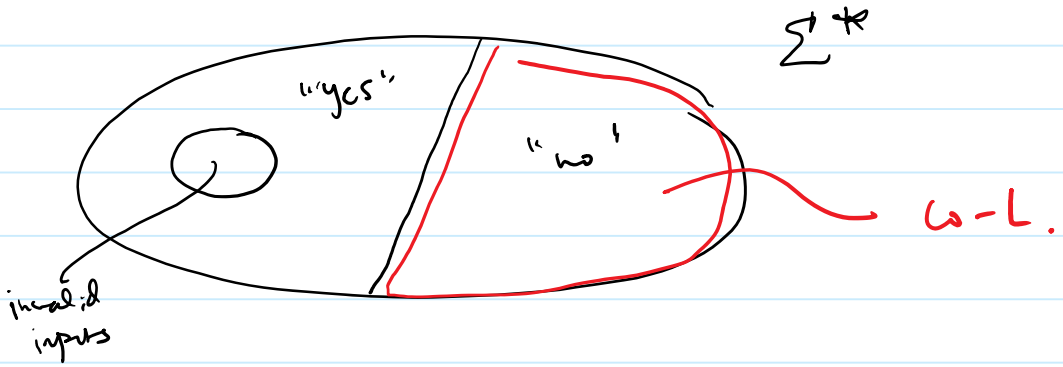
Decision: Input: int N, k
Output: does N have a factor $\leq k$.

Monday, April 2, 2018 8:18 AM

Language L : subset of Σ^* that correspond to "yes" instances.



co-L "complement of L" $\Sigma^* - L$.

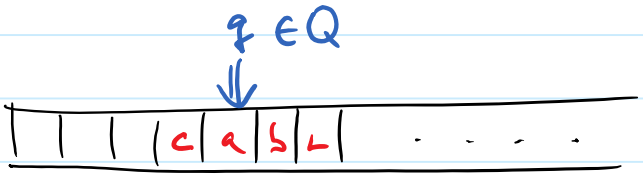


Complexity class : set of languages that can be computed w/ limited resource.

Monday, April 2, 2018 8:18 AM

Complexity class:
- Contain natural / important probs.
- Capture some computational resource.
- Complete problems are natural & important.
- robust under variations in the computational model.
- closed under $\wedge$, $\vee$, $\neg$

Turing Machine

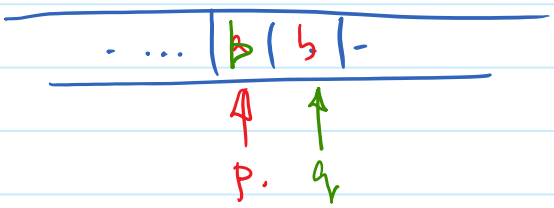


Σ = finite alphabet.
must contain ⊔

Q: set of states (finite)
Σ: finite alphabet.
q_{start} q_{acc} q_{rej}

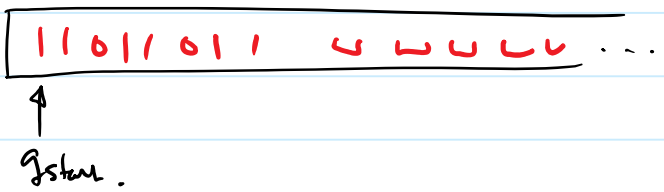
transition function: $\delta : Q \times \Sigma \to Q \times \Sigma \times \{L, R, -\}$

$\delta(p, a) = (q, b, R)$



Monday, April 2, 2018 8:18 AM

Start config:



Halts if q_{acc} or q_{rej} is reached

3 ways to compute: (1) function comp.
output $f(x)$ left on tape when TM halts.

(2) language decision:
TM reaches q_{acc} if $x \in L$.
TM reaches q_{rej} if $x \notin L$.

(3) language recognition
TM reaches q_{acc} if $x \in L$.
TM reaches q_{rej} or never halts if $x \notin L$.