Miller-Rabin(n, s)

- Write $n-1 = 2^k m$, m odd
- Choose a random
  a, $1 \le a \le n-1$
- $b = a^m \bmod n$.
- If $b \equiv 1 \bmod n$
  then return ("n is prime")
- for i ← 0 to k-1
- do { if $b \equiv -1 \bmod n$
  then return
  ("n is prime

{ else $b \leftarrow b^2 \bmod n$.

return ("n is composite")

Repeat s times

If if Miller-Rabin returns
"n is composite", then n must be
composite

Thus if n is prime, then
Miller-Rabin returns "n is prime".

Thus if n is composite then Miller-Rabin
is likely to err.

Thm If $n>2$ is odd & composite

If Miller-Rabin returns "n is composite"
then the integer a is called a "witness"
to the compositeness of n.

Thm If $n > 2$ is odd composite,
then the no. of witnesses is at least

$$\frac{n-1}{2}.$$

Pf We shall show that the no. of non-witnesses is at most $\frac{n-1}{2}$

Fix a non-witness $a \in \mathbb{Z}_n$

If a is a non-witness then $a \in \mathbb{Z}_n^*$

Claim All non-witnesses belong to a proper subgroup B of $\mathbb{Z}_n^*$.

Case 1. Suppose $\exists$ $x \in \mathbb{Z}_n^*$ s.t.

$$\boxed{x^{n-1} \not\equiv 1 \bmod n.}$$

Let $B = \{ b \in \mathbb{Z}_n^* : b^{n-1} \equiv 1 \bmod n \}$.

$B \neq \phi$. Also, B is closed under multiplication modulo n

Hence B is a subgroup of $\mathbb{Z}_n^*$.

Also, all non-witnesses belong to B (Why?)

Also, $x \in \mathbb{Z}_n^* - B$

Thm Hence B is a proper subgroup of $\mathbb{Z}_n^*$.

$\therefore$ # of non-witness $\leq |B| \leq \frac{|\mathbb{Z}_n^*|}{2} \leq \frac{n-1}{2}$

Case 2 For all $x \in \mathbb{Z}_n^*$, $x^{n-1} \equiv 1 \mod n$

In other words, n is a Carmichael number.

Observe that $n-1 = 2^k \cdot m$

of Miller-Rabin algorithm computes the

seq^n $X = \{ a^m, a^{2m}, a^{2^2 m}, \ldots, a^{2^k m} \}$

Fix a pair (c, j) s.t

$$\boxed{a^{2^j m} \equiv -1 \bmod n.} \quad (*)$$

Such a pair exists, since for $j=0$, we have.

$$(n-1)^m \equiv (-1)^m \equiv -1 \bmod n$$

Observe that $n-1 = 2^k \cdot m$

of Miller-Rabin algorithm computes the

seq^n $X = \{ a^m, a^{2m}, a^{2^2 m}, \ldots, a^{2^k m} \}$

Fix a pair (c, j) s.t

$$c^{2^j m} \equiv -1 \bmod n.$$

(*)

Such a pair exists, since for $j=0$, we have.

$$(n-1)^m \equiv (-1)^m \equiv -1 \bmod n$$

Choose j as large as possible.

Let $B = \{ b \in \mathbb{Z}_n^* : b^{n-1} \equiv \pm 1 \mod n \}$.

B forms a closed under multiplication mod n

Hence B is a subgroup of $\mathbb{Z}_n^*$.

Also, all non-witness are in B

Since either the seq $X_0, \ldots, X_d$ consists of 1 only

or for some $j \leq j$, $a^{2^j m} \equiv -1 \mod n$.

Claim n is not a prime power.

Suppose $n = p^e$, p a prime & $e > 1$.

Then $\mathbb{Z}_n^*$ is cyclic & hence $\mathbb{Z}_n^* = \langle g \rangle$

By our assumption $\boxed{g^{n-1} \equiv 1 \mod n.}$

But $o(g) = |\mathbb{Z}_n^*| = \varphi(n) = p^{e-1}(p-1)$.

$\therefore p^{e-1}(p-1) \mid p^e - 1$ Contradiction.

Hence the claim.

Hence $n = n_1 n_2$, where n_1, n_2 are odd $\neq 1$

& $GCD(n_1, n_2) = 1$

By CRT choose w s.t.

$$\begin{cases} w \equiv c \bmod n_1 \\ w \equiv 1 \bmod n_2 \end{cases}$$

Suppose $w \equiv +1 \bmod n \Rightarrow w \equiv +1 \bmod n_1$

$w^{2^i m} \equiv 1 \bmod n_1 \Rightarrow c^{2^i m} \equiv 1 \bmod n_1$,

Contradiction, since $c^{2^i m} \equiv 1 \bmod n$

Suppose $w \equiv -1 \mod n$

Then $w \equiv -1 \mod n_2$

Since $w \equiv +1 \mod n_2$

} Contradiction

Hence $w \notin B$.

$w \equiv c \mod n_1 \Rightarrow w = c + l n_1 \Rightarrow \gcd(w, n_1) = 1$

$w \equiv 1 \mod n_2 \Rightarrow w = 1 + l' n_2 \Rightarrow \gcd(w, n_2) = 1$

$\gcd(w, n) = 1$

$w \in \mathbb{Z}_n^*$

# of non-witnesses $\leq |B| \leq \frac{|\mathbb{Z}_n^*|}{2} \leq \frac{n-1}{2}$

Cor Miller-Rabin algorithm errs with prob. at most $\frac{1}{2^s}$.

$\frac{n-1}{2}$

If M-R errs when n is composite if errs when one choose a non-witness & the prob. of choosing a non-witness in one run is M-R is at most $1/2$

So assume it errs with prob. at most $1/2$

Let A be the event "M-R returns (n is prime) s times"

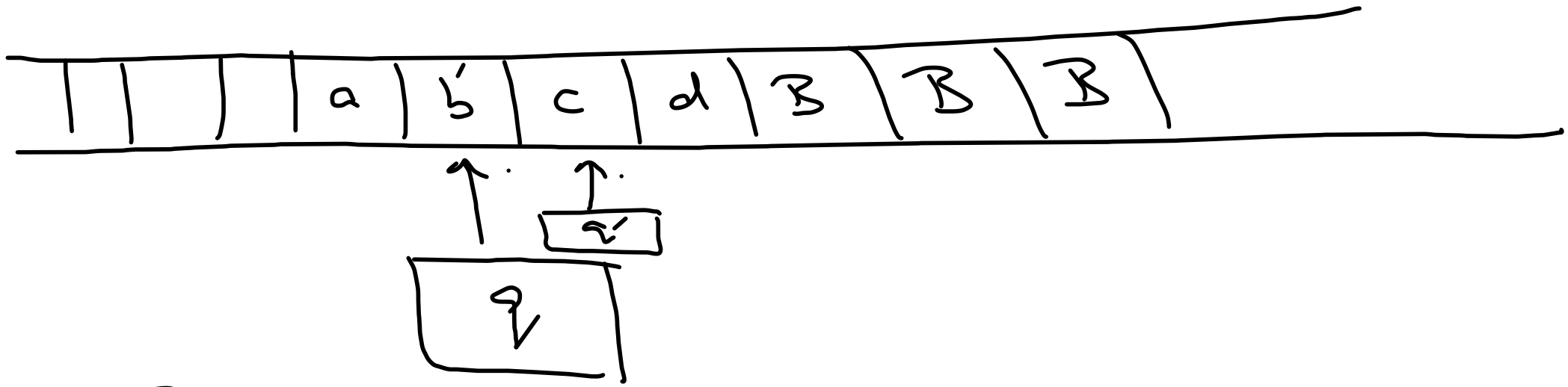
B: "n is composite"

Given $Prob(A \mid B) \leq \frac{1}{2^s}$

Show that $Prob(\neg B \mid A)$ is large.

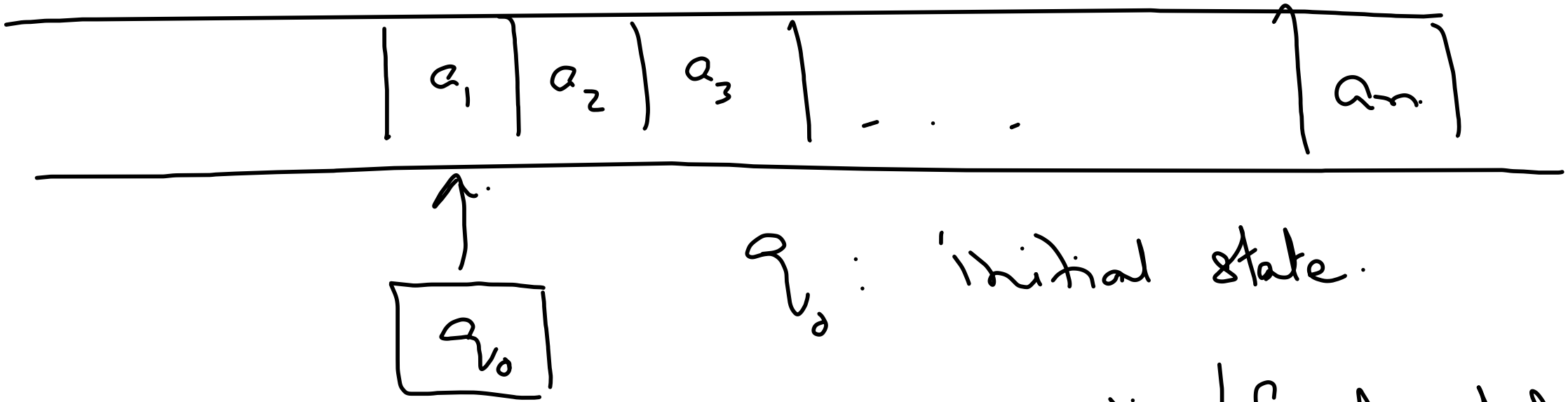
$Prob(B \mid A)$ is small.

NP-complete Problems



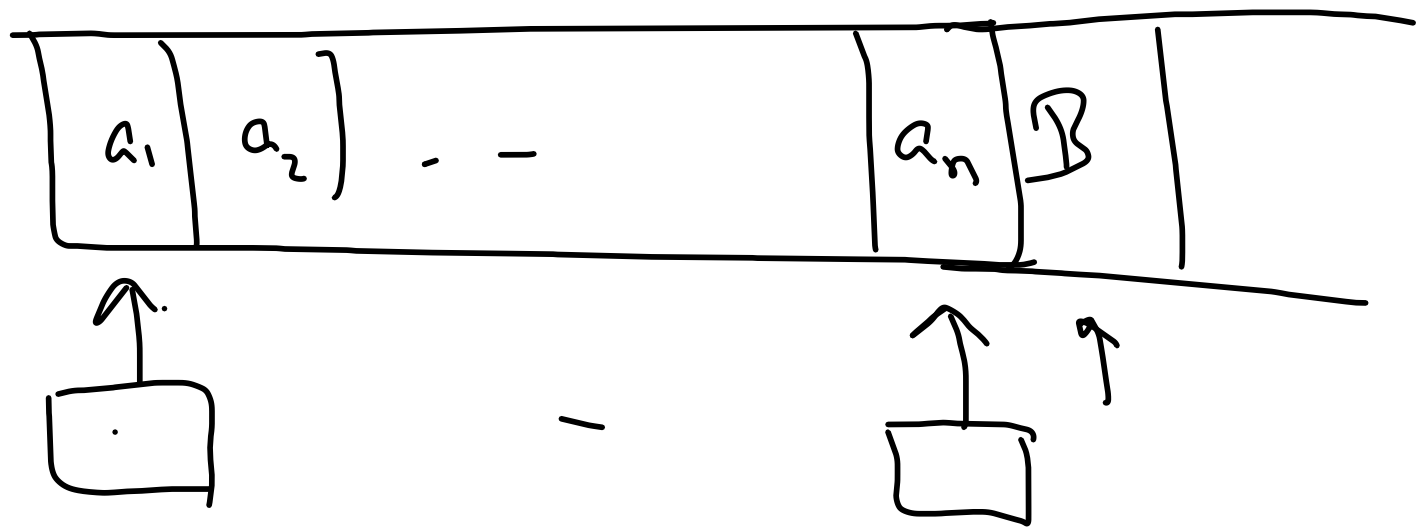
Depending on the state of the finite control and the letter being scanned by the tape-head

$w = a_1 a_2 \cdots a_n$



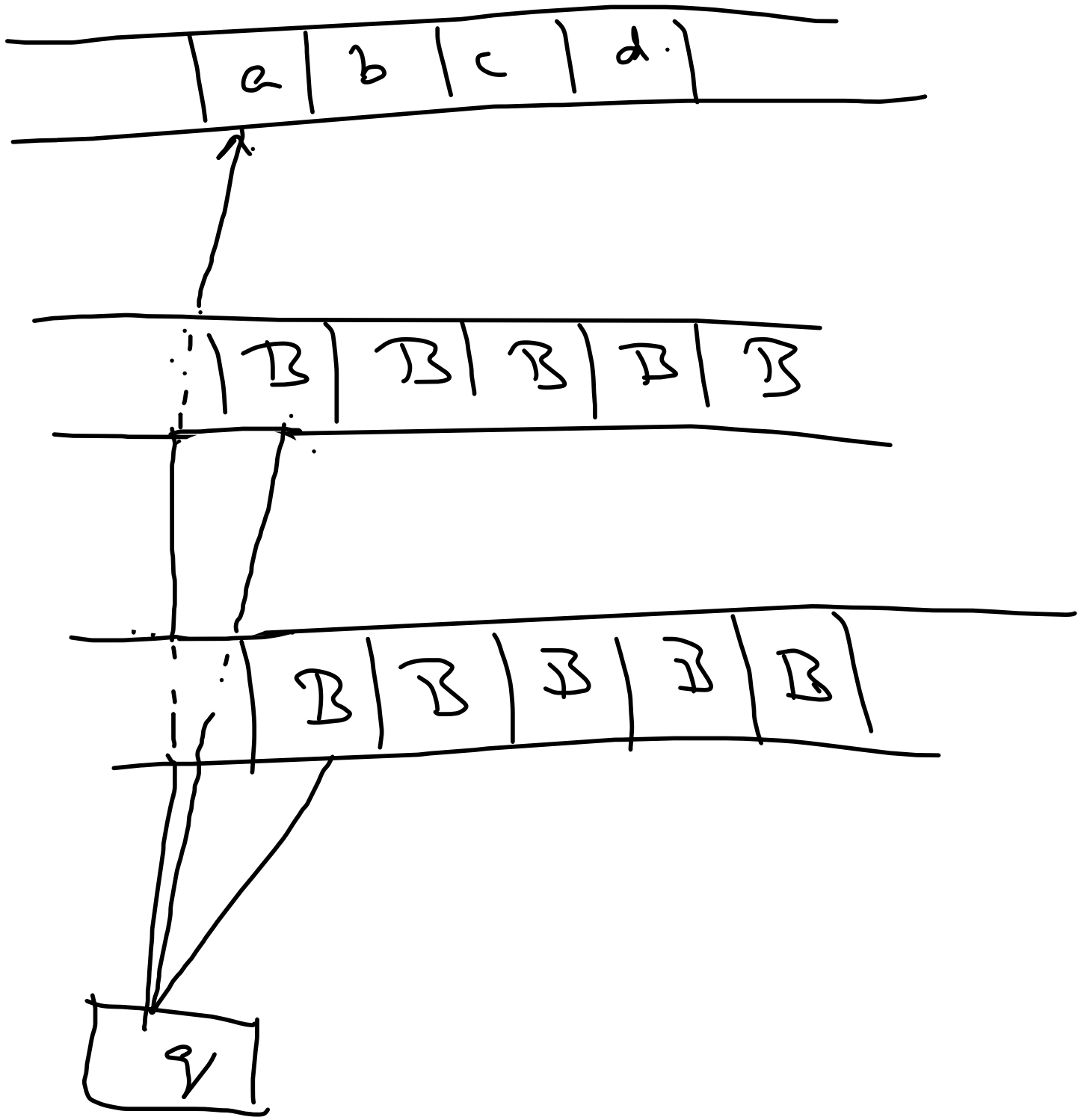
q_0 : initial state.

q_f : accepting | final state.

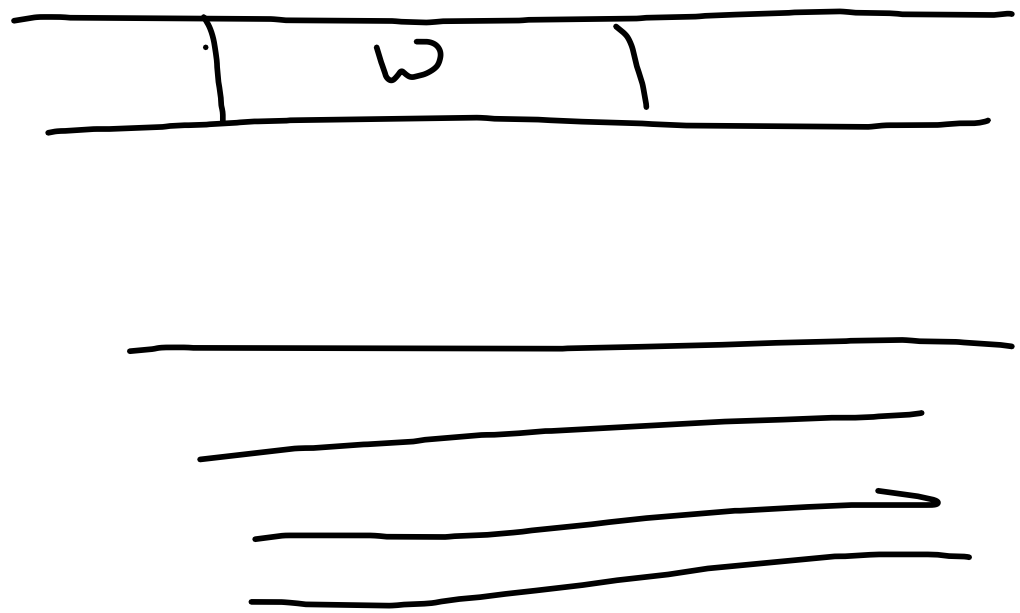


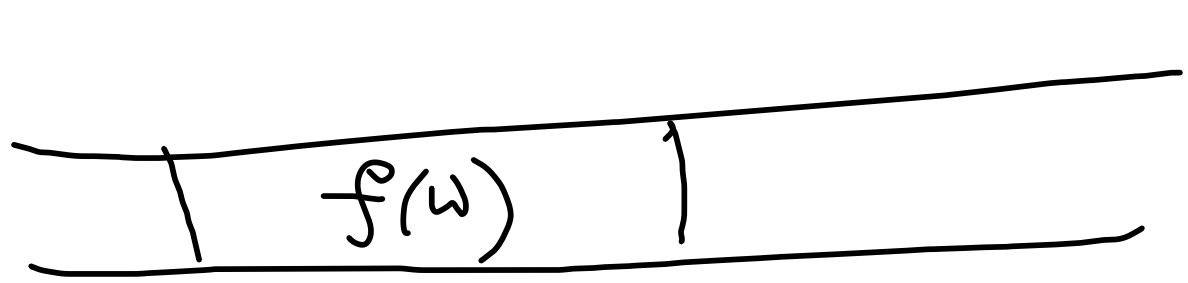
$$\mathcal{L}(M) = \{ w \in \Sigma^* : M \text{ accepts } w \}.$$

r.e. (recursively enumerable)


a
b
c
d
B
B
B
B
B
B
B
B
B
B
q

Defⁿ





Defn A fn $f : \Sigma_1^* \to \Sigma_2^*$ is said to be poly-time computable if $\exists$ a TM M and a poly $p(n)$ s.t. for every input $w \in \Sigma_1^*$ of length n, M outputs $f(w)$ in at most $p(n)$ steps

Defn $L_1, L_2 \subseteq \Sigma^*$.

We say L_1 is poly-time reducible to L_2 & we write $\boxed{L_1 \leq_p L_2}$ if $\exists$ a poly-time computable fn $f : \Sigma^* \longrightarrow \Sigma^*$ s.t.

$$\boxed{x \in L_1 \text{ iff } f(x) \in L_2}$$

Defⁿ $L \subseteq \Sigma^*$ is said to be decidable. recursive if it is accepted by a TM M that halts on every input.