What are probabilistically checkable proofs?

Consider the following problem:

A knows some secret information $a_0 \in \mathbb{F}_2^n$.

B claims that he also knows a_0 and wants to convince A of this fact.

How can B achieve this?

☞ He can give A a vector $a \in \mathbb{F}_2^n$ and ask A to verify that $a_0 \equiv a$.

Note: To be sure that a is indeed identical to a_0 A has to compare each of the n bits.

Can we do better?

What are probabilistically checkable proofs?

Suppose:

A wants to spend as little effort as possible in checking whether $a_0 \equiv a$.

We require the following two conditions:

If B really knows a_0 (*i.e.*, if $a \equiv a_0$), then A has to accept a.

If B does not know a_0 (*i.e.*, if $a \not\equiv a_0$), then A may accept a with probability at most 2^{-10}.

Does this help?

What are probabilistically checkable proofs?

YES!

In this case A has to read only a constant number of bits (independent of n)!

But: B has to submit a in a slightly encoded form.

How does this work?

Key Observation

For $a, a_0 \in \mathbb{F}_2^n$:

$$\mathrm{Prob}_r[r^T a = r^T a_0] = \begin{cases} 1 & , \text{ if } a = a_0 \\ \frac{1}{2} & , \text{ if } a \neq a_0 \end{cases}$$

The Protocol

B gives A a table T which (supposedly) contain for each $r \in \mathbb{F}_2^n$ the scalar product $r^T a_0$.

A chooses a vector $r \in \mathbb{F}_2^n$ uniformly at random and compares $T(r)$ with $r^T a_0$.

A repeats this test 10 times and accepts if and only if all answers were correct.

Claim: This reduces the error probability to 2^{-10}.

Is this correct?

A Counterexample

Suppose: $a_0 = (11011)$ and B has no knowledge of a_0 ;

Assume: B submits a table T such that

$$T(r) = 0 \iff (r_1 = r_{n-1} \text{ and } r_2 = r_n) \text{ or } (r_1 = r_2 \text{ and } r_{n-1} = r_n)x.$$

r_1	r_2	r_3	r_4	r_5	$T(r)$	$r^T a_0$
0	0	$\star$	0	0	0	0
0	0	$\star$	0	1	1	1
0	0	$\star$	1	0	1	1
0	0	$\star$	1	1	0	0
0	1	$\star$	0	0	1	1
0	1	$\star$	0	1	0	0
0	1	$\star$	1	0	1	0
0	1	$\star$	1	1	1	1
1	0	$\star$	0	0	1	1
1	0	$\star$	0	1	1	0
1	0	$\star$	1	0	0	0
1	0	$\star$	1	1	1	1
1	1	$\star$	0	0	0	0
1	1	$\star$	0	1	1	1
1	1	$\star$	1	0	1	1
1	1	$\star$	1	1	0	0

The Protocol — Corrected Version

B gives A a table T which (supposedly) contain for each $r \in \mathbb{F}_2^n$ the scalar product $r^T a_0$.

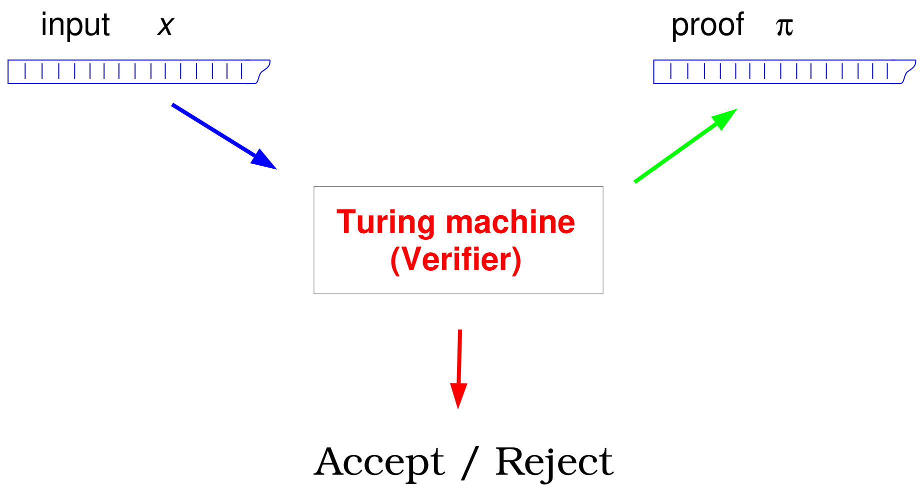
A chooses vector $x, y \in \mathbb{F}_2^n$ uniformly at random and verifies that $T(x+y) = T(x) + T(y)$.

A chooses a vector $r \in \mathbb{F}_2^n$ uniformly at random and compares $T(r)$ with $r^T a_0$.

A repeats these two tests O(1) times and accepts if and only if all tests are ok.

Theorem: This protocol has zero error if B knows a_0 and submits the correct table T, and error probability $\leq 2^{-10}$ otherwise.

Complexity Class $\mathcal{NP}$

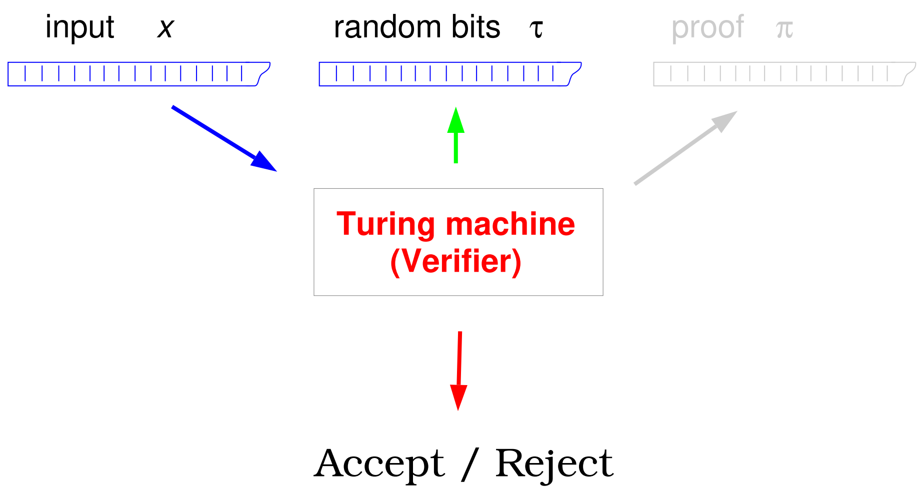


$L \in \mathcal{NP}$ $\quad :\Longleftrightarrow \quad$ there exists a polynomial time Turing machine M such that

$$x \in L \quad \Longrightarrow \quad \exists\ \pi_0 : \quad M(x, \pi_0) = \textsc{Accept}$$

$$x \notin L \quad \Longrightarrow \quad \forall\ \pi : \quad M(x, \pi) = \textsc{Reject}$$

Complexity Class $\mathcal{RP}$

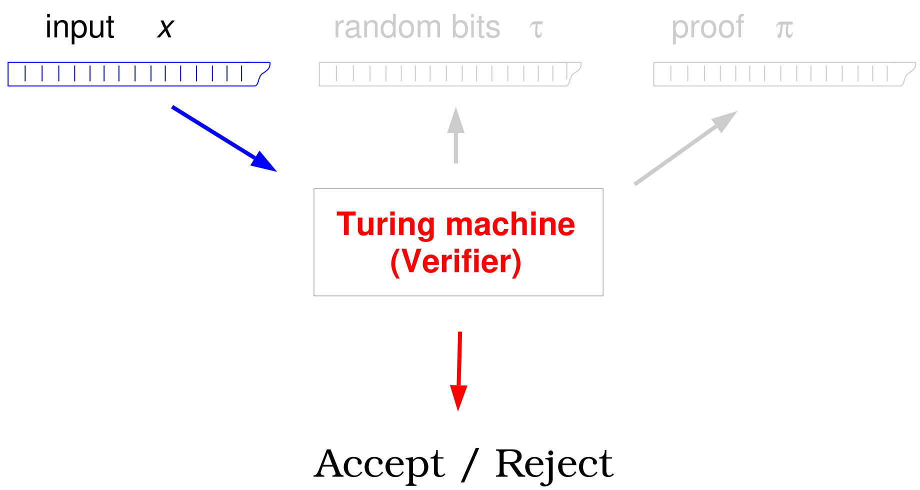


$L \in \mathcal{RP}$ $\quad :\Longleftrightarrow \quad$ there exists a polynomial time Turing machine M such that

$$x \in L \quad \Longrightarrow \quad \text{Prob}_\tau[M(x,\tau) = \text{ACCEPT}] \quad \geq \frac{1}{2}$$

$$x \notin L \quad \Longrightarrow \quad \text{Prob}_\tau[M(x,\tau) = \text{REJECT}] \quad = 1$$

Complexity Class $\mathcal{P}$

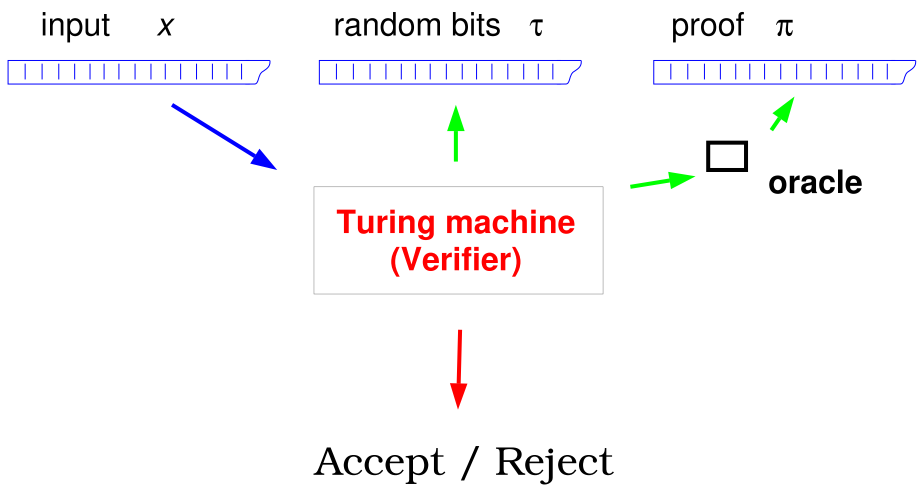


$L \in \mathcal{P}$ $:\Longleftrightarrow$ there exists a polynomial time Turing machine M such that

$$x \in L \implies M(x) = \textsc{Accept}$$

$$x \notin L \implies M(x) = \textsc{Reject}$$

Complexity Class $\mathcal{PCP}(\cdot,\cdot)$



$L \in \mathcal{PCP}(r(n), q(n))$

$:\Longleftrightarrow$ there exists a polynomial time Turing machine M which uses for inputs x of length n at most $\mathcal{O}(r(n))$ many random bits and queries at most $\mathcal{O}(q(n))$ many bits from the proof such that

$$x \in L \implies \exists\ \pi_0 : \quad \text{Prob}_\tau[M(x,\tau,\pi_0) = \text{ACCEPT}] \quad = 1$$

$$x \notin L \implies \forall\ \pi : \quad \text{Prob}_\tau[M(x,\tau,\pi) = \text{REJECT}] \quad \geq \frac{1}{2}$$

Observations

- $\mathcal{PCP}(0, 0) \; = \; \mathcal{P}$
- $\mathcal{PCP}(0, poly(n)) \; = \; \mathcal{NP}$
- $\mathcal{PCP}(poly(n), 0) \; = \;$ co-$\mathcal{RP}$
- $\mathcal{PCP}(poly(n), poly(n)) \; = \; \mathcal{NEXP}$ [BFL91]

Proposition: $\mathcal{PCP}(r(n), q(n)) \; \subseteq \; \text{NTIME}(2^{\mathcal{O}(r(n))} \cdot poly(n))$
for all $q(n) \in poly(n)$.

Corollary: $\mathcal{PCP}(\log n, 1) \; \subseteq \; \mathcal{NP}$

Arora, Lund, Motwani, Sudan, Szegedy '92

$$\mathcal{NP} = \mathcal{PCP}(\log n, 1)$$