An introduction to Probabilistically Checkable Proofs (PCP)

Recall: Definition of NP

Let $L \subseteq \{0,1\}^*$, i.e., L is a language. Then

$L \in NP \iff \exists$ polynomial $p: \mathbb{N} \to \mathbb{N}$ and polynomial-time deterministic Turing machine V s.t. for every $x \in \{0,1\}^*$:

(Completeness) $x \in L \Rightarrow \exists \pi \in \{0,1\}^{p(|x|)} : V(x,\pi) = 1$

(Soundness) $x \notin L \Rightarrow \forall \pi \in \{0,1\}^{p(|x|)} : V(x,\pi) = 0$

Verifier is deterministic and reads every bit of the proof.

What if we relax that?

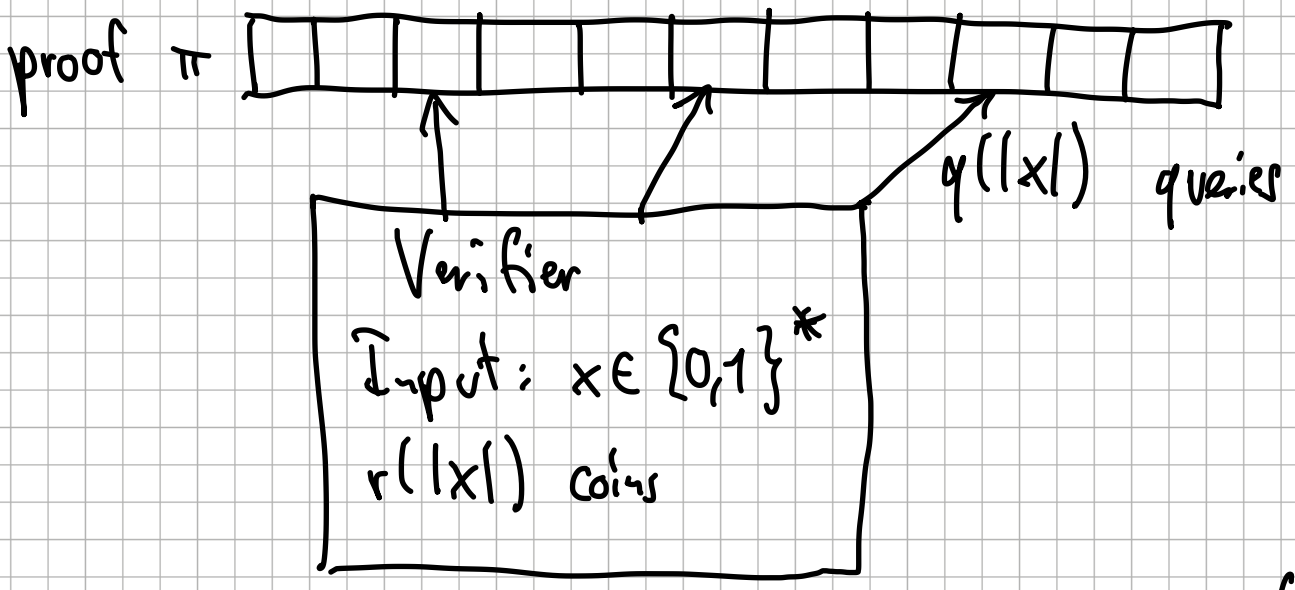
→ probabilistically checkable proofs

Definition [$PCP_{c,s}(r,q)$]

Let $q, r : \mathbb{N} \to \mathbb{N}$ and $0 \le s \le c \le 1$. A language $L \subseteq \{0,1\}^*$ is an element of the complexity class $PCP_{c,s}(r,q)$ $\Leftrightarrow$ $\exists$ a polynomial-time randomized Turing machine V that flips $r(|x|)$ coins, makes $q(|x|)$ queries to some string π and satisfies the following ($\forall x \in \{0,1\}^*$)

(Completeness) $x \in L \Rightarrow \exists \pi \in \{0,1\}^* : \Pr(V(x,\pi)=1) \ge c$

(Soundness) $x \notin L \Rightarrow \forall \pi \in \{0,1\}^* : \Pr(V(x,\pi)=1) \le s$



Remarks:
- maximal relevant size of π: $q(|x|)2^{r(|x|)}$
-

The PCP Theorem

$$NP = PCP_{1,\frac{1}{2}}\left(O(\log(n)), O(1)\right)$$