

Claim 1. *If L has a PCP verifier with randomness $O(1)$ and $O(1)$ queries, then $L \in \mathcal{P}$.*

Proof. Let V be a PCP verifier for L using $\ell = O(1)$ bits of randomness and $Q = O(1)$ queries. Let $P = O(2^\ell) = O(1)$ be an upper-bound on the length of PCP proofs for V .

We construct a polynomial-time algorithm A deciding L . Given x , the algorithm A enumerates over all strings π of length P . For each π , it runs $V^\pi(x, r)$ with all possible choices of random coins $r \in \{0, 1\}^\ell$. Then A accepts x if and only if there was some π such that $V^\pi(x, r)$ accepts with all r 's.

If $x \in L$ then there is π such that $\Pr_r[V^\pi(x, r) = 1] = 1$, in which case A accepts. Otherwise, for every π it holds that $\Pr_r[V^\pi(x, r) = 1] \leq 1/2$, and in particular for every π there is r such that $V^\pi(x, r) = 0$, hence A rejects. Since A enumerates over constantly many strings, and for each string it runs a polynomial-time algorithm (i.e., V), the total runtime of A is polynomial. ■

Claim 2. *If L has a PCP verifier with randomness $O(\log n)$ and $O(1)$ queries, then $L \in \mathcal{NP}$.*

Proof. Let V be a PCP verifier for L using $\ell(n) = O(\log n)$ bits of randomness and $Q = O(1)$ queries. Let $P(n) = O(2^{\ell(n)}) = \text{poly}(n)$ be an upper-bound on the length of PCP proofs for V .

We construct an \mathcal{NP} -verifier \bar{V} for L . Given $x \in \{0, 1\}^n$, the verifier expects a witness w of length $P(n)$. Then \bar{V} simulates $V^w(x, r)$ with all choices of random coins $r \in \{0, 1\}^\ell$, of which there are $2^\ell = \text{poly}(n)$, and accepts iff V accepted with all r 's.

The proof of correctness is very similar to the previous claim, and left as an exercise (please make sure you know how to prove this!). As for running time, since \bar{V} enumerates over $\text{poly}(n)$ choices of r , and for each choice it runs a polytime machine V , the total runtime of \bar{V} is $\text{poly}(n)$. ■

Theorem 3. *For any L and $\varepsilon > 0$, the following two statements are equivalent:*

1. *L has a PCP verifier with randomness $O(\log n)$ and $k = O(1)$ queries*
2. *L is Karp-reducible to $(1, 1/2)$ -approximating k -CSP*

Proof. Let's first prove the interesting direction (1) \Rightarrow (2). Fix L and a PCP verifier V for L with $\ell = O(\log n)$ randomness and $k = O(1)$ queries, and denote by $P(n) = \text{poly}(n)$ the proof length for V .

Given $x \in \{0, 1\}^n$, we construct a k -CSP as follows. The variables of the CSP are denoted $w_1, \dots, w_{P(n)}$. For each choice of $r \in \{0, 1\}^\ell$ we add a k -constraint C_r . Specifically, let $q_1, \dots, q_k \in [P]$ be the locations of queries that V makes when given input x and randomness r ; the k -constraint C_r is over the variables w_{q_1}, \dots, w_{q_k} , and the k -constraint is satisfied if and only if the values of w_{q_1}, \dots, w_{q_k} cause $V^w(x, r)$ to accept.

If $x \in L$ then there is a proof π such that $\Pr_r[V^\pi(x, r) = 1] = 1$ (i.e., V accepts with every choice of randomness r), and by setting $w = \pi$ all constraints C_r will be satisfied. On the other hand, if $x \notin L$ then $\Pr_r[V^\pi(x, r) = 1] \leq 1/2$, meaning that for every possible π , at least half of the choices r cause V to reject; hence, for every w , at least half of the C_r 's are unsatisfied.

For the (2) \Rightarrow (1) direction, assume that L is Karp-reducible to $(1, 1/2)$ approximating a k -CSP. Then, given $x \in \{0, 1\}^n$ we can construct in polynomial time a k -CSP Φ over variables w_1, \dots, w_N and with constraints C_1, \dots, C_m such that

- If $x \in L$ there is w_1, \dots, w_N such that all constraints are satisfied.
- If $x \notin L$ then for every w_1, \dots, w_N , at least half of the constraints are unsatisfied.

We define a PCP verifier V as follows. Given x , it expects a proof of length N , interpreted as w_1, \dots, w_N . It chooses a random $r \in [m]$ and checks if C_r is satisfied, by reading the k bits that C_r depends on (among w_1, \dots, w_N). Note that V runs in polynomial time (because the reduction is polynomial time), uses $\log(m) = \log(\text{poly}(n)) = O(\log n)$ bits of randomness, and reads k bits of the proof.

As for correctness, if $x \in L$ then there is w_1, \dots, w_N that satisfies all constraints C_1, \dots, C_m , hence V accepts for all choices of $r \in [m]$. On the other hand, if $x \notin L$ then for every w_1, \dots, w_N , for at least half of the choices of r it holds that V rejects, hence $\Pr_r[V^w(x, r) = 1] \leq 1/2$. ■