0.1 Probabilistically Checkable Proofs

Before going further we should get acquainted with one more concept from the computational complexity theory, that have an important application in zk-SNARK and provides the theoretical backbone.

A Probabilistically Checkable Proof (PCP) is a type of proof system where the verifier can efficiently check the correctness of a proof by examining only a small, random portion of it, rather than verifying it entirely.

Definition 0.1. A language $\mathcal{L} \subseteq \Sigma^*$ (for some given alphabet Σ) is in the class $\mathsf{PCP}(r, q)$ (**probabilistically checkable proofs**) if for a proof $\pi \in \Sigma^*$, computed by prover in polynomial time $\mathsf{poly}(|x|)$ of the common input x, there exists a probabilistically polynomial time verifier $\mathcal{V}$ such that:

- The verifier receives an input $x \in \Sigma^n$ and access to a proof π, which it can query at any position.
- **Complexity**: The verifier uses at most $r(n)$ random bits to decide which part of the proof to query and the verifier queries at most $q(n)$ bits of the proof.

with following properties:

- **Completeness**: If $x \in \mathcal{L}$, there exist a proof $\pi = \mathcal{P}(x)$ such that $\Pr\{\mathcal{V}(x, \pi) = 1\} = 1$
- **Soundness**: If $x \notin \mathcal{L}$, then for any proof π, $\Pr\{\mathcal{V}(x, \pi) = 1\} = \mathsf{negl}(\lambda)$.

This allows a verification of huge statements with high confidence while using limited computational resources.

Theorem 0.2. PCP theorem (PCP characterization theorem)
Any decision problem in NP has a PCP verifier that uses logarithmic randomness $O(\log n)$ and a constant number of queries $O(1)$, independent of n.

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

0.1.1 PCP application in QAP

Constructing QAP we finished with a single polynomial $P(X)$:

$$P(X) = A(X)B(X) - C(X) = Z_\Omega(X)H(X)$$

We effectively managed to transform all the circuit's constraints, and computations in the short form. It's still allows one to verify that each computational step is preserved by verifying the polynomial evaluation in specific points, instead of recomputing everything.

As it was said early, we perform all the computations in some finite field $\mathbb{F}_p$. The polynomials A, B and C are interpolated polynomials using $|w|$ points, so

$$\deg(A) \leq |w|, \quad \deg(B) \leq |w|, \quad \deg(C) \leq |w|$$

Thus, using properties of polynomials' degrees, we can estimate the degree of polynomial $P(X)$.

$$\deg(P) \leq \max(\deg(A) + \deg(B), \deg(C)) = \max(2|w|, |w|) = 2|w|$$

Now using Schwartz-Zippel Lemma **??**, we can state that if an adversary $\mathcal{A}$ doesn't know a valid witness $\mathbf{w}$ to resolves some circuit $\mathcal{C}$, they still can compute a polynomial $P(X)'$ that satisfies a verifier $\mathcal{V}_{\mathcal{C}}$ with probability less then $\frac{2|w|}{p}$.

$$\Pr[\mathcal{V}_{\mathcal{C}}(P(X)') = \text{accept} \mid P(X)' \xleftarrow{R} A] \leq \frac{2\,|w|}{p}$$

This probability becomes negligible as p grows large, giving us soundness. In the same time, the verifier accepts the $P(X)$ generated using a valid witness with probability 1 giving us the completeness, so, we can categorize QAP as PCP.

We'll modify the form of our proof with the next modifications, but still preserve the PCP properties.