$\mathcal{NP}$ problems and ZKPs

February 20, 2022

1 Graph 3 Colorability

We say that any $\mathcal{NP}$ problems have a Zero-Knowledge Proof System since that some known $\mathcal{NPC}$ problems have Zero-Knowledge Proof System, and by using reduction, we could easily prove that statement.

By introducing the G3C (Graph 3 Colorability), which is a $\mathcal{NPC}$ problem, we give the ZKP of it.

Definition 1. *A G3C is a graph that the vertices are colored by 3 colors and there are no any two vertices that are same color and connected by an edge.*

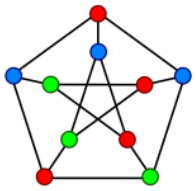

Figure 1: G3C example

Further speaking, not only the G3C problem is $\mathcal{NPC}$ problem, the Graph k-Colorability Problem is also $\mathcal{NPC}$ problem, which consists in finding the k minimum number of colors to paint the vertices of a graph in such a way that any two vertices joined by an edge have always different colors.

Generally, given a graph, there are some algorithm to give a coloring solution of it, which includes Brute-force search, Contraction, Greedy coloring, Heuristic algorithm and so on. For more detail information, please see wikipedia website.

Now we give the ZKP of the G3C problem.

Let G be graphs on n vertices and define $V = \{v_1, v_2, ..., v_n\}$ be the set of vertices, $E = \{e_{i,j} : \exists \textit{edge between } v_i, v_j\}$.

The common input is Graph G, and the prover holds a witness which is a 3-coloring of the graph G. The protocol proceeds follows:

1. Initiate $r = 1$.

2. Round r begins. Prover randomly chooses a permute of the 3-colors to obtain a new coloring, then uses commitment scheme to commit the colors of all vertices by calculating $c_i = COM(v_i, color\ of\ v_i\ in\ round\ r)$, then send all commitments to the Verifier.

3. The Verifier randomly choose an edge $e_{i,j} \in E$, and send it to the Verifier.

4. Prover open c_i and c_j and send them to the Verifier.

5. Verifier checks wether the colors are different, if same, reject. round r ends, goes to round $r + 1$.

6. If the Verifier completes m^2 rounds, then accept.

The ZKP of G3C satisfy the following 3 properties.

- **Completeness**. If the graph is 3 colorable, then any edge the Verifier chooses will be colored differently, and the probability an honest Verifier accept is always 1.

- **Soundness**. If the graph is not 3 colorable, the Verifier will reject in each round with the probability of $\frac{1}{|E|}$. The probability of the Verifier accepts is $(1 - \frac{1}{|E|})^{m^2} \leq negl(n)$

- **Zero Knowledge**. We construct a simulator S to simulate the whole process. It works as follows:

  (a) Setting the Random Tape r of V*.

  (b) Simulate Prover first step. Uniformly and independently select colors for n vertices and compute the commitment c for every vertices.

  (c) Simulate Verifier first step. Place G on V*'s common-input tape, place V*'s Random Tape r (in step (a)), place sequence $\{c_1, c_2, ..., c_n\}$ on V*'s incoming-message tape. After executing a polynomial number of steps of V*, the Simulator could read the outgoing message of V*, $m = (i, j)$.

  (d) Simulate Prover second step. If the color of v_i and v_j are different, then simulator halts with output $(G, r, \{c_1, c_2, ..., c_n\}, v_i,\ color\ of\ v_i,\ v_j,\ color\ of\ v_j)$.

  (e) Failure of Simulation. if the color of v_i and v_j are same, the simulator halts with output $\perp$.

  We also have to prove that the simulator outputs $\perp$ with probability at most $1/2$, and conditioned on not outputting $\perp$, the output of the simulator and the output of the view of Verifier in real interaction are indistinguishable. For detail proof, please go check section 4.4 of Oded Goldreich's *"Foundations of Cryptograph Volume 1"*.

  (In this case, the only information the Verifier receive in each round is the color of v_i and v_j. Considering that the Prover independently select

permutation in each round, thus the color in one round is unrelated to another round. In a higher aspect, we could say that the Verifier gains no knowledge.)