Exercise 5

Zero-Knowledge Proofs

Loïc Baccigalupi

October 18, 2022

5.1 Public-Coin Interactive Proof for Graph Non-Isomorphism

a) Because if $v \in \mathbb{F}_{2^m}$ is uniformly random, then we can see that each element v_i ($v = (v_1, \ldots, v_m)$) is also uniformly random. This implies that the vector $[v] = (v_1, \ldots, v_k)$ is also uniformly random, as it is composed of uniformly random vector elements.

Because of this, we know that y and y' are independent.

This in turn shows that $\forall x \neq x' \in \mathbb{F}_{2^m}$ and $y, y' \in \mathbb{F}_{2^k}$:

$$\begin{aligned}
\mathrm{P}_{h \leftarrow \mathcal{H}}\{h(x) = y \wedge h(x') = y'\} &= \mathrm{P}_{h_{a,b} \leftarrow \mathcal{H}}\{[ax + b] = y \wedge [ax' + b] = y'\} \\
&= \mathrm{P}_{h_{a,b} \leftarrow \mathcal{H}}\{[ax + b] = y\} \mathrm{P}_{h_{a,b} \leftarrow \mathcal{H}}\{[ax' + b] = y'\} \\
&= \frac{1}{2^k} \frac{1}{2^k} \\
&= 2^{-2k}
\end{aligned}$$

b) Let $P = \mathrm{P}_{h,y}\{\exists x \in S : h(x) = y\}$ and $T = \{h(x) : x \in S\} \subseteq \mathbb{F}_{2^k}$ the set of images of h where the inputs are elements of $S \subseteq \mathbb{F}_{2^m}$.

The cardinality $|T|$ is at a maximum if every element of S maps to a distinct element in $\mathbb{F}_{2^k}$, i.e. $|T| = |S|$. This implies that the upper bound of P is the probability of picking a random element of T, i.e.:

$$P \leqslant \frac{|T|}{2^k} = \frac{|S|}{2^k} = |S| 2^{-k}$$

Because we used the maximum cardinality $|T|$, this implies we used the upper bound of p ($= N2^{-k}$). By knowing that $|[\frac{1}{4}; \frac{1}{2})| = \frac{1}{4}$, we can find the lower bound of P:

$$P \leqslant |S| 2^{-k} \left(1 - \frac{1}{4}\right) = 3|S| 2^{-k-2}$$

c) The prover can find with probability at least $3|S|2^{-k-2} = \frac{3}{4}p$ when $|S| = N$ the correct s to send. This means that the protocol is $\frac{3}{4}p$-complete.

If $|S| \leqslant \frac{N}{2}$, the probability of finding the correct x is at most half of what it is when $|S| = N$ ($|S|$ is at most half of N). So the protocol is $\frac{p}{2}$-sound.

d) We can use the GI zero-knowledge proof as seen in class to prove that a graph X is isomorphic to G_0 or G_1, i.e. $X \in S$.

If $G_0 \cong G_1$, $|S| = n!$ and if $G_0 \ncong G_1$, $|S| = 2n!$.

e) If we set $N = 2n!$ and S as seen in the previous sub-question, we want our protocol to accept if $|S| = 2n! = N$ and reject if $|S| \leqslant n! = \frac{N}{2}$ (same conditions as in Goldwasser-Sipser).

Now we have that $S = \{H : H \cong G_0 \text{ or } H \cong G_1\} \subseteq \{\text{"All graphs with } n \text{ vertices"}\}$