ETH Zurich, Department of Computer Science
HS 2023

Dr. Jonathan Bootle
Karen Klein, Varun Maram, Antonio Merino Gallardo

Zero-Knowledge Proofs

Exercise 4

4.1 Necessity of Prover's Randomness in ZK Protocols

Let (P, V) be an interactive proof system *with auxiliary inputs* for a language L. Now suppose (P, V) is (computational) zero-knowledge such that P is *deterministic*. Then show that $L \in \mathbf{BPP}$.[1]

4.2 Zero-Knowledge Protocol for Graph Non-Isomorphism

a) Explain why the GNI protocol given in the 1st lecture is not zero-knowledge.

b) Show that the same protocol is honest-verifier zero-knowledge.

c) Design a statistical zero-knowledge protocol for the GNI problem.

HINT: Use the GI$[k]$ protocol in Task 4.3 as a *sub-protocol*. You can rely on the fact that GI$[k]$ is knowledge sound with knowledge error 2^{-k} as proven in Task 4.3.

4.3 (Zero-Knowledge) Proof of Knowledge for Graph Isomorphism (*)

Let $\mathrm{GI} = (P_{\mathrm{GI}}, V_{\mathrm{GI}})$ be the zero-knowledge protocol for graph isomorphism seen in the 2nd lecture. Now let $\mathrm{GI}[k] = (P_{\mathrm{GI}[k]}, V_{\mathrm{GI}[k]})$ be the *k-sequential repetition* of the GI protocol such that the verifier $V_{\mathrm{GI}[k]}$ accepts if and only if the verifier V_{GI} in every single execution of the basic GI protocol accepts. Prove that GI$[k]$ is knowledge sound with knowledge error 2^{-k}.

References

[1] Roughly speaking, **BPP** is essentially a *randomized* version of class **P**, and still contains "easy" problems. We say that $L \in \mathbf{BPP}$ if there exists a *randomized* algorithm M and a polynomial q such that,

- if $x \in L$, then $\Pr[M(x) = 1] \geq 3/4$,
- if $x \notin L$, then $\Pr[M(x) = 1] \leq 1/2$,
- for all x, M terminates in at-most $q(|x|)$ steps on input x.

Also see `https://en.wikipedia.org/wiki/BPP_(complexity)`, `https://complexityzoo.net/Complexity_Zoo:B#bpp`.