[name]: Efficient zero-knowledge proof with optimal prover computation

October 31, 2018

1 Preliminary

In this section, we will introduce some useful results and definitions.

1.1 Interactive Proof

Traditional proof involves two static objects: a prover $\mathcal{P}$ and a verifier $\mathcal{V}$. The prover $\mathcal{P}$ takes a statement x as input and generate a string π as a proof, then the verifier $\mathcal{V}$ checks if the statement x and proof π are correct. A interactive proof is a stronger notion of proof, it allows a prover $\mathcal{P}$ to convince a verifier $\mathcal{V}$ of the validity of some statement. The interactive proof runs in several rounds, allows the verifier to ask questions in each round based on prover's answers of previous rounds. We phrase this in term of $\mathcal{P}$ trying to convince $\mathcal{V}$ that $f(x) = 1$. The proof system is interesting iff the running time of $\mathcal{V}$ is less than the time of directly computing the function f.

We formalize the "interactive proof" in the following:

Definition 1. Let f be a boolean function. A pair of interactive machines $\langle \mathcal{P}, \mathcal{V} \rangle$ is an interactive proof for f with soundness ϵ if the following holds:

- **Completeness.** For every x such that $f(x) = 1$ it holds that $\Pr[\langle \mathcal{P}, \mathcal{V} \rangle(x) = \textit{accept}] = 1$.
- **ϵ-Soundness.** For any x with $f(x) \neq 1$ and any $\mathcal{P}^*$ it holds that $\Pr[\langle \mathcal{P}^*, \mathcal{V} \rangle = \textit{accept}] \leq \epsilon$

1.2 Sum Check Protocol

The sum check problem is a fundamental problem that serves as a building block for varies applications. Informally the problem requires us to sum on a binary hypercube $(x_0, x_1, ..., x_l)$ for a given function $g(x_0, x_1, ..., x_l)$. Directly compute the function requires exponential computation, Lund et al. [1]

References

[1] C. Lund, L. Fortnow, H. Karloff, and N. Nisan, *Algebraic methods for interactive proof systems*, J. ACM, 39 (1992), pp. 859–868.