Delegating Computation: Interactive Proofs for Muggles

Authors: Shafi Goldwasser, Yael Tauman Kalai, Guy N. Rothblum
Presenter: Kristýna Mašková

21.11.2024

Theorem 1 (Main Result) *Let L be a language that can be computed by a family of $O(\log(S(n)))$-space uniform boolean circuits of size $S(n)$ and depth $d(n)$. L has an interactive proof where:*

1. *The prover runs in time poly$(S(n))$. The verifier runs in time $n \cdot$poly$(d(n), \log S(n))$ and space $O(\log(S(n)))$. Moreover, if the verifier is given oracle access to the low-degree extension of its input, then its running time is only poly$(d(n), \log S(n))$.*
2. *The protocol has perfect completeness and soundness $1/2$.*
3. *The protocol is public-coin, with communication complexity $d(n)\cdot$polylog$(S(n))$.*

Proposition 1 *There exists a Turing machine that takes as input an extension field $\mathbb{H}$ of $\mathbb{GF}[2]$, an extension field $\mathbb{F}$ of $\mathbb{H}$, and an integer m. The machine runs in time poly$(|\mathbb{H}|, m)$ and space $O(\log(|\mathbb{H}|) + \log(m))$. It outputs the unique $2m$-variate polynomial $\tilde{\beta} : \mathbb{F}^m \times \mathbb{F}^m \to \mathbb{F}$ of degree $|\mathbb{H}| - 1$ in each variable (represented as an arithmetic circuit of degree $|\mathbb{H}| - 1$ in each variable), such that for every $(w_0, w_1, \ldots, w_{k-1}) \in \mathbb{F}^k$ with $k \leq |\mathbb{H}|^m$, and for every $z \in \mathbb{F}^m$,*

$$\widetilde{W}(z) = \sum_{p \in \mathbb{H}^m} \tilde{\beta}(z, p) \cdot W(p),$$

where $W : \mathbb{H}^m \to \mathbb{F}$ is the function corresponding to $(w_0, w_1, \ldots, w_{k-1})$, and $\widetilde{W} : \mathbb{F}^m \to \mathbb{F}$ is its low-degree extension (i.e., the unique extension of $W : \mathbb{H}^m \to \mathbb{F}$ of degree at most $|\mathbb{H}| - 1$ in each variable).

Moreover, $\tilde{\beta}$ can be evaluated in time poly$(|\mathbb{H}|, m)$ and space $O(\log(|\mathbb{H}|) + \log(m))$. Namely, there exists a Turing machine with the above time and space bounds, that takes as input parameters $\mathbb{H}, \mathbb{F}, m$, and a pair $(z, p) \in \mathbb{F}^m \times \mathbb{F}^m$, and outputs $\tilde{\beta}(z, p)$.

Claim 1 *There exists a Turing machine that takes as input an extension field $\mathbb{H}$ of $\mathbb{GF}[2]$, an extension field $\mathbb{F}$ of $\mathbb{H}$, an integer m, a sequence $w = (w_0, w_1, \ldots, w_{k-1}) \in \mathbb{F}^k$ such that $k \leq |\mathbb{H}|^m$, and a coordinate $z \in \mathbb{F}^m$. It outputs the value $\widetilde{W}(z)$,* *where $\widetilde{W}$ is the unique low-degree extension of w (with respect to $\mathbb{H}, \mathbb{F}, m$). The machine's running time is $|\mathbb{H}|^m \cdot poly(|\mathbb{H}|, m)$ and its space usage is $O(m \cdot \log(|\mathbb{H}|))$.*

Lemma 1 (Schwartz-Zippel Lemma) *Let $\mathbb{F}$ be a field and $f(x_1, x_2, \ldots, x_n)$ a nonzero polynomial of degree d. If $r_1, r_2, \ldots, r_n$ are chosen independently and uniformly at random from $\mathbb{F}$, then*

$$\Pr[f(r_1, r_2, \ldots, r_n) = 0] \leq \frac{d}{|S|}.$$