COSC 544 Probabilistic Proof Systems 10/26/17

A First Linear PCP (Of Size $|\mathbb{F}|^{O(S^2)}$)

Lecturer: Justin Thaler

1 A Simple Linear PCP for Non-Deterministic Circuit Evaluation

Let $\{\mathcal{C}, x, y\}$ be an instance of non-deterministic circuit evaluation. For this lecture, we refer to a setting $W \in \mathbb{F}^S$ of values to each gate in $\mathcal{C}$ as a transcript for $\mathcal{C}$.

The linear PCP of this section is from IKO [IKO07], and is based on the observation that W is a correct transcript iff W satisfies the following $\ell = S + |y| - |w|$ constraints: there are no constraints for any witness elements, there is one constraint for every other non-output gate of $\mathcal{C}$, and there are two constraints for each output gate of $\mathcal{C}$.

Specifically, the constraints are the following.

- For each input gate $\mathbf{a}$, there is a constraint enforcing that $W_{\mathbf{a}} - x_{\mathbf{a}} = 0$. This effectively insists that the transcript W actually correspond to the execution of $\mathcal{C}$ on input x, and not some other input.
- For each output gate a there is a constraint enforcing that $W_{\mathbf{a}} - y_{\mathbf{a}} = 0$. This effectively insists that the transcript W actually correspond to an execution of $\mathcal{C}$ that produces outputs y, and not some other set of outputs.
- If gate a is an addition gate with in-neighbors $\text{in}_1(\mathbf{a})$ and $\text{in}_2(\mathbf{a})$, there is a constraint enforcing that $W_{\mathbf{a}} - \left(W_{\text{in}_1(\mathbf{a})} + W_{\text{in}_2(\mathbf{a})}\right) = 0$.
- If gate a is a multiplication, there is a constraint enforcing that $W_{\mathbf{a}} - W_{\text{in}_1(\mathbf{a})} \cdot W_{\text{in}_2(\mathbf{a})} = 0$.

Together, the last two types of constraints insist that the transcript actually respects $\mathcal{C}$ (i.e., any addition (respectively, multiplication) gate actually computes the addition (respectively, product) of its two inputs. Note that the constraint for gate a of $\mathcal{C}$ is always of the form $Q_{\mathbf{a}}(W) = 0$ for some polynomial $Q_{\mathbf{a}}$ of degree at most 2 in the entries of W.

For a transcript W for $\{\mathcal{C}, x, y\}$, let $W \otimes W$ denote the length-S^2 vector whose (i, j)th entry is $W_i \cdot W_j$. Let $(W, W \otimes W)$ denote the vector of length $\mathbb{F}^{S^2+S}$ obtained by concatenating W with $W \otimes W$. Consider a PCP proof π containing all evaluations of the linear function $f_{(W,W\otimes W)} \colon \mathbb{F}^{S^2+S} \to \mathbb{F}$ defined as $f_{(W,W\otimes W)}(\cdot) := \langle \cdot, (W, W \otimes W)\rangle$. π is typically called the *Hadamard encoding* of $(W, W \otimes W)$. Notice that π has length $|\mathbb{F}|^{S^2+S}$, which is enormous. However, $\mathcal{P}$ will never need to explicitly materialize all of π.

$\mathcal{V}$ needs to check three things. First, that π is a linear function. Second, assuming that π is a linear function, $\mathcal{V}$ needs to check that π is of the form $f_{(W,W\otimes W)}$ for some transcript W. Third, that W satisfies all S constraints described above.

First Check: Linearity Testing. Linearity testing is a considerably simpler task than the more general low-degree testing problems considered in the MIP of Lecture 14. (note: linearity testing is equivalent to testing that an m-variate function equals polynomial of total degree 1 (with no constant term), while the low-degree testing problem considered in Lecture 14 tested whether an m-variate function is multilinear, which means its total degree can be as large as m).

Specifically, to perform linearity testing, the verifier picks two random points $\mathbf{q}^{(1)}, \mathbf{q}^{(2)} \in \mathbb{F}^{S+S^2}$ and checks that $\pi(\mathbf{q}^{(1)} + \mathbf{q}^{(2)}) = \pi(\mathbf{q}^{(1)}) + \pi(\mathbf{q}^{(2)})$, which requires three queries to π. If π is linear then the test always passes. Moreover, it is known that if the test passes with probability $1-\delta$, then there is some linear function f_d such that π is δ-close to f_d [BLR93], at least over fields of characteristic 2.[1]

Second Check. Assuming π is linear, π can be written as $f_\mathbf{d}$ for some vector $\mathbf{d} \in \mathbb{F}^{S^2+S}$. To check that $\mathbf{d}$ is of the form $(W, W \otimes W)$ for some transcript W, $\mathcal{V}$ does the following.

- $\mathcal{V}$ picks $\mathbf{q}^{(3)}, \mathbf{q}^{(4)} \in \mathbb{F}^s$ at random.
- Let $(\mathbf{q}^{(3)}, \mathbf{0})$ denote the vector in $\mathbb{F}^{S^2+S}$ whose first S entries equal $\mathbf{q}^{(3)}$ and whose last S^2 entries are 0. Similarly, let $(\mathbf{0}, \mathbf{q}^{(3)} \otimes \mathbf{q}^{(4)})$ denote the vector whose first S entries equal 0, and whose last S^2 entries equal $\mathbf{q}^{(3)} \otimes \mathbf{q}^{(4)}$. $\mathcal{V}$ checks that $\pi(\mathbf{q}^{(3)}, \mathbf{0}) \cdot \pi(\mathbf{q}^{(4)}, \mathbf{0}) = \pi(\mathbf{0}, \mathbf{q}^{(3)} \otimes \mathbf{q}^{(4)})$. This requires three queries to π.

Clearly the check will pass if π is of the claimed form. If π is not of the claimed form, the test will fail with high probability over the choice of $\mathbf{q}^{(3)}$ and $\mathbf{q}^{(4)}$. This holds because $\pi(\mathbf{q}^{(3)}, \mathbf{0}) \cdot \pi(\mathbf{q}^{(4)}, \mathbf{0}) = f_\mathbf{d}(\mathbf{q}^{(3)}, \mathbf{0}) \cdot f_\mathbf{d}(\mathbf{q}^{(4)}, \mathbf{0})$ is a quadratic polynomial in the entries of $\mathbf{q}^{(3)}$ and $\mathbf{q}^{(4)}$, as is $f_\mathbf{d}(\mathbf{0}, \mathbf{q}^{(3)} \otimes \mathbf{q}^{(4)})$, and the Schwartz-Zippel lemma guarantees that any two distinct low-degree polynomials can agree on only a small fraction of points.

Third Check. Once $\mathcal{V}$ is convinced that $\pi = f_\mathbf{d}$ for some $\mathbf{d}$ of the form $(W, W \otimes W)$, $\mathcal{V}$ is ready to check that W satisfies all ℓ constraints described above. This is the core of the PCP.

In order to check that $Q_i(W) = 0$ for all constraints i, it suffices for $\mathcal{V}$ to pick random values $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}$, and check that $\sum_{i=1}^{\ell} \alpha_i Q_i(W) = 0$. Indeed, this equality is always satisfied if $Q_i(W) = 0$ for all i; otherwise, $\sum_{i=1}^{\ell} \alpha_i Q_i(W)$ is a non-zero multilinear polynomial in the variables $(\alpha_1, \ldots, \alpha_\ell)$, and the Schwartz-Zippel lemma guarantees that this polynomial is non-zero at almost all points $(\alpha_1, \ldots, \alpha_\ell) \in \mathbb{F}^\ell$.

Notice that $\sum_{i=1}^{\ell} \alpha_i Q_i(W)$ is itself a degree-2 polynomial in the entries of W, which is to say that it is a linear combination of the entries of $(W, W \otimes W)$. Hence it can be evaluated with one additional query to π.

Soundness Analysis. A formal proof of the soundness of the linear PCP just described is a bit more involved than indicated above, but not terribly so. Roughly it proceeds as follows. If the prover passes the linearity test with probability $1-\delta$, then π is δ-close to a linear function $f_\mathbf{d}$. Hence, as long as the k queries in the second and third checks are distributed uniformly in $\mathbb{F}^{S^2+S}$, then with probability $1 - k \cdot \delta$, the verifier will never encounter a point where π and $f_\mathbf{d}$ differ, and we can treat π as $f_\mathbf{d}$ for the remainder of the analysis. However, the queries in the second and third checks are not uniformly distributed in $\mathbb{F}^{S^2+S}$ as described. Nonetheless, they can be made uniformly distributed by replacing each query $\mathbf{q}$ with two random queries $\mathbf{q}'$ and $\mathbf{q}''$ subject to the constraint that $\mathbf{q}' + \mathbf{q}'' = \mathbf{q}$, for then by linearity of $f_\mathbf{d}$, $f_\mathbf{d}(\mathbf{q})$ can be deduced from $f_\mathbf{d}(\mathbf{q}') + f_\mathbf{d}(\mathbf{q}'')$. With this change, the soundness analysis of the second and third steps are as indicated above.

[1] See [AB09, Theorem 19.9] for a short proof of this statement based on Discrete Fourier analysis. Over fields of characteristic other than 2, the known soundness guarantees of the linearity test are weaker. See [SBV+13, Proof of Lemma A.2] and [BCH+96, Theorem 1.1].

$\mathcal{V} \to \mathcal{P}$ Communication	$\mathcal{P} \to \mathcal{V}$ Communication	Queries	$\mathcal{V}$ time	$\mathcal{P}$ time
$O(S^2)$ field elements	$O(1)$ field elements	$O(1)$	$O(S^2)$	$O(S^2)$

Table 1: Costs of the argument system from Section 1 when run on a non-deterministic circuit $\mathcal{C}$ of size S. Note that the verifier's cost and the communication cost can be amortized when simultaneously outsourcing $\mathcal{C}$'s execution on a large *batch* of inputs. The stated bound on $\mathcal{P}$'s time assumes $\mathcal{P}$ knows a witness w for $\mathcal{C}$.

Protocol Costs. The costs of the argument system obtained by combining the above linear PCP with the commitment protocol are summarized in Table 1. $\mathcal{V}$'s time and $\mathcal{P}$'s time are both $\Theta(S^2)$, but if $\mathcal{V}$ is simultaneously verifying $\mathcal{C}$'s execution over a large *batch* of inputs, then the $\Theta(S^2)$ cost for $\mathcal{V}$ can be amortized over the entire batch. Total communication from $\mathcal{V}$ to $\mathcal{P}$ is $\Theta(S^2)$ as well (this cost can also be amortized), but the communication in the reverse direction is just a constant number of field elements per input.

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, New York, NY, USA, 1st edition, 2009.

[BCH+96] Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos A. Kiwi, and Madhu Sudan. Linearity testing in characteristic two. *IEEE Transactions on Information Theory*, 42(6):1781–1795, 1996.

[BLR93] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. Comput. Syst. Sci.*, 47(3):549–595, 1993.

[IKO07] Yuval Ishai, Eyal Kushilevitz, and Rafail Ostrovsky. Efficient arguments without short pcps. In *22nd Annual IEEE Conference on Computational Complexity (CCC 2007), 13-16 June 2007, San Diego, California, USA*, pages 278–291. IEEE Computer Society, 2007.

[SBV+13] Srinath T. V. Setty, Benjamin Braun, Victor Vu, Andrew J. Blumberg, Bryan Parno, and Michael Walfish. Resolving the conflict between generality and plausibility in verified computation. In Zdenek Hanzálek, Hermann Härtig, Miguel Castro, and M. Frans Kaashoek, editors, *EuroSys*, pages 71–84. ACM, 2013.