Non-commutative circuits and the sum-of-squares problem

Pavel Hrubeš*   Avi Wigderson*   Amir Yehudayoff*

Abstract

We initiate a direction for proving lower bounds on the size of non-commutative arithmetic circuits. This direction is based on a connection between lower bounds on the size of non-commutative arithmetic circuits and a problem about commutative degree four polynomials, the classical sum-of-squares problem: find the smallest $n$ such that

\begin{equation}
(x_1^2 + x_2^2 + \cdots + x_k^2) \cdot (y_1^2 + y_2^2 + \cdots + y_k^2) = f_1^2 + f_2^2 + \cdots + f_n^2,
\end{equation}

where each $f_i = f_i(X,Y)$ is bilinear in $X = \{x_1, \ldots, x_k\}$ and $Y = \{y_1, \ldots, y_k\}$. Over the complex numbers, we show that a sufficiently strong super-linear lower bound on $n$ in (1), namely, $n \geq k^{1+\varepsilon}$ with $\varepsilon > 0$, implies an exponential lower bound on the size of arithmetic circuits computing the non-commutative permanent.

More generally, we consider such sum-of-squares identities for any biquadratic polynomial $h(X,Y)$, namely

\begin{equation}
h(X,Y) = f_1^2 + f_2^2 + \cdots + f_n^2.
\end{equation}

Again, proving $n \geq k^{1+\varepsilon}$ in (2) for any explicit $h$ over the complex numbers gives an exponential lower bound for the non-commutative permanent. Our proofs rely on several new structure theorems for non-commutative circuits, as well as a non-commutative analog of Valiant’s completeness of the permanent.

*School of Mathematics Institute for Advanced Study, Princeton, NJ. Emails: pahrubes@gmail.com, avi@ias.edu and amir.yehudayoff@gmail.com. Research supported by NSF Grant DMS-0835373.
We proceed to prove such super-linear bounds in some restricted cases. We prove that $n \geq \Omega(k^{6/5})$ in (1), if $f_1, \ldots, f_n$ are required to have integer coefficients. Over the real numbers, we construct an explicit biquadratic polynomial $h$ such that $n$ in (2) must be at least $\Omega(k^2)$. Unfortunately, these results do not imply circuit lower bounds.

We also present other structural results about non-commutative arithmetic circuits. We show that any non-commutative circuit computing an ordered non-commutative polynomial can be efficiently transformed to a syntactically multilinear circuit computing that polynomial. The permanent, for example, is ordered. Hence, lower bounds on the size of syntactically multilinear circuits computing the permanent imply unrestricted non-commutative lower bounds. We also prove an exponential lower bound on the size of non-commutative syntactically multilinear circuit computing an explicit polynomial. This polynomial is, however, not ordered and an unrestricted circuit lower bound does not follow.