Contribution ID: **17** Type: **not specified**

Nondeterministic Refutations for Nearest Boolean Vector

Tuesday, July 11, 2023 10:30 AM (20 minutes)

Andrej Bogdanov and Alon Rosen

Abstract: Most n-dimensional subspaces $\mathcal{A}$ of $\mathbb{R}^m$ are $\Omega(\sqrt{m})$-far from the Boolean cube $\{-1,1\}^m$ when $n < cm$ for some constant $c > 0$. How hard is it to certify that the Nearest Boolean Vector (NBV) is at least $\gamma\sqrt{m}$ far from a given random $\mathcal{A}$?

Certifying NBV instances is relevant to the computational complexity of approximating the Sherrington-Kirkpatrick Hamiltonian, i.e. maximizing $x^T Ax$ over the Boolean cube for a matrix A sampled from the Gaussian Orthogonal Ensemble. The connection was discovered by Mohanty, Raghavendra, and Xu (STOC 2020). Improving on their work, Ghosh, Jeronimo, Jones, Potechin, and Rajendran (FOCS 2020) showed that certification is not possible in the sum-of-squares framework when $m \ll n^{1.5}$, even with distance $\gamma = 0$.

We present a non-deterministic interactive certification algorithm for NBV when $m \gg n \log n$ and $\gamma \ll 1/mn^{1.5}$. The algorithm is obtained by adapting a public-key encryption scheme of Ajtai and Dwork.

Presenter: BOGDANOV, Andrej

Session Classification: Track A-3