Erfan Khaniki:

Nisan-Wigderson generators in proof complexity: new lower bounds

A map $g : \{0,1\}^n \to \{0,1\}^m$ ($m > n$) is a hard proof complexity generator for a proof system P iff for every string $b \in \{0,1\}^m \setminus \mathsf{Rng}(g)$, formula $\tau_b(g)$ naturally expressing $b \notin \mathsf{Rng}(g)$ requires superpolynomial size P-proofs. One of the well-studied maps in the theory of proof complexity generators is Nisan–Wigderson generator. Razborov [Raz15] conjectured that if A is a suitable matrix and f is a $\mathsf{NP} \cap \mathsf{CoNP}$ function hard-on-average for $\mathsf{P/poly}$, then $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for Extended Frege. In this paper, we prove a form of Razborov's conjecture for AC^0-Frege. We show that for any symmetric $\mathsf{NP} \cap \mathsf{CoNP}$ function f that is exponentially hard for depth two AC^0 circuits, $\mathsf{NW}_{f,A}$ is a hard proof complexity generator for AC^0-Frege in a natural setting. As direct applications of this theorem, we show that:

1. For any f with the specified properties, $\tau_b(\mathsf{NW}_{f,A})$ based on a random b and a random matrix A with probability $1 - o(1)$ is a tautology and requires superpolynomial (or even exponential) AC^0-Frege proofs.
2. Certain formalizations of the principle $f_n \notin (\mathsf{NP} \cap \mathsf{CoNP})/\mathsf{poly}$ requires superpolynomial AC^0-Frege proofs.

These applications relate to two questions that were asked by Krajíček [Kra19].