Pseudorandom Generators in Proof Complexity

Def. A generator $G_n : \{0,1\}^n \to \{0,1\}^m$ is *hard* in P if, for any $\vec{b} \in \{0,1\}^m$, no proof $\Pi \in P$ exists showing $\vec{b} \notin \mathrm{Im}(G_n)$ efficiently.

Prop. The Tseitin generator is hard in resolution.

Def. $J_i(A) := \{j \in [n] : a_{ij} = 1\}$ and $X_i(A) := \{x_j : j \in J_i(A)\}$ describe the 1-columns of row i.

Def.

$$\begin{cases} g_1(\vec{x}) = 1 \\ \vdots \\ g_m(\vec{x}) = 1 \end{cases} \qquad \mathrm{Vars}(g_i) \subseteq X_i(A) \tag{1}$$

is *Equation 1*. Refuting it shows $\langle 1, \ldots, 1 \rangle \notin \mathrm{Im}(G_n)$.

Def. Fix $i \in [m]$. Let f be s.t. $\mathrm{Vars}(f) \subseteq X_i(A)$. Then y_f is the *extension variable* of f.

Def. $\mathrm{Vars}(A) := \{y_f : \exists i \in [m] : \mathrm{Vars}(f) \subseteq X_i(A)\}$

Def. $C = y_{f_1}^{\varepsilon_1} \vee \cdots \vee y_{f_k}^{\varepsilon_k} \implies \|C\| := f_1^{\varepsilon_1} \vee \cdots \vee f_k^{\varepsilon_k}$

Def. Fix A. $\tau(A, G_n)$ denotes the collection of clauses $C = y_{f_1}^{\varepsilon_1} \vee \cdots \vee y_{f_k}^{\varepsilon_k}$ for which

$$\mathrm{Vars}(f_i) \subseteq X_i(A) \quad i = 1, \ldots, k \qquad \text{and} \qquad g_i \vDash \|C\|$$

We call $\tau(A, G_n)$ the *functional encoding* of Equation 1.

Prop. $\tau(A, G_n)$ is satisfiable $\iff$ Equation 1 has a solution $\vec{x}$.

Def. For $I \subseteq [m]$, $\partial_A(I)$ (called the *boundary* of I) denote all columns which, when restricted to I, contain one "1." A is called an (r, s, c)*-expander* if $|J_i(A)| \leq s$ and, for all choices I as above, $(|I| \leq r \implies |\partial_A(I)| \geq c|I|$.

Def. A function g_i is called ℓ*-robust* if every ρ such that $g_i(\rho) \in \{0,1\}$ satisfies $|\rho| \geq \ell$.

Def. For a clause C in $\mathrm{Vars}(A)$, $\mu(C)$ is the size of a minimal $I \subseteq [m]$ such that:

(a) $\forall y_f^{\varepsilon} \in C\ \exists i \in I : \mathrm{Vars}(f) \subseteq X_i(A)$

(b) $\{\, g_i \mid i \in I\} \vDash \|C\|$

Claim 1. For a clause C with $\frac{r}{2} < \mu(C) \leq r$, $w(C) > \frac{r(c+\ell-s)}{2\ell}$.

Claim 2. Any resolution refutation Π of τ contains a clause C with $\frac{r}{2} < \mu(C) \leq r$.

Main Theorem. Let $A \in M_{m \times n}(\{0,1\})$ be an (r, s, c)-expander, and let g_i be ℓ-robust for $i = 1, \ldots, m$. Let $c + \ell \geq s + 1$. Then

$$w_{\mathrm{Res}}(\tau(A, G_n)) > \frac{r(c + \ell - s)}{2\ell}$$