Pseudorandom generators hard for propositional proof systems

Markus Latte

April 3 and 4, 2009
JASS09
Санкт Петербург

Pseudorandom Generators in Complexity Theory

Informally, a pseudorandom generator is a (computable) function

$$G_n : \{0,1\}^n \to \{0,1\}^m \qquad (n < m)$$

which stretches a short random string $\mathbf{x}$ to a long random string $G_n(\mathbf{x})$ such that a deterministic polytime algorithm f cannot distinguish them, i. e. the difference between

$$\mathop{\mathbf{Pr}}_{\mathbf{x}\in\{0,1\}^n}[f(G_n(\mathbf{x})) = 1] \qquad \text{and}$$

$$\mathop{\mathbf{Pr}}_{\mathbf{y}\in\{0,1\}^m}[f(\mathbf{y}) = 1]$$

is small.

Pseudorandom Generators in Complexity Theory

Informally, a pseudorandom generator is a (computable) function

$$G_n : \{0,1\}^n \to \{0,1\}^m \qquad (n < m)$$

which stretches a short random string $\mathbf{x}$ to a long random string $G_n(\mathbf{x})$ such that a deterministic polytime algorithm f cannot distinguish them, i. e. the difference between

$$\mathop{\mathbf{Pr}}_{\mathbf{x}\in\{0,1\}^n}[f(G_n(\mathbf{x}))=1] \qquad \text{and}$$

$$\mathop{\mathbf{Pr}}_{\mathbf{y}\in\{0,1\}^m}[f(\mathbf{y})=1]$$

is small.
Hence, a random generator for size m can be replaced by a random generator for size n together with G_n without affecting f essentially.

Pseudorandom Generators in Complexity Theory

Informally, a pseudorandom generator is a (computable) function

$$G_n : \{0,1\}^n \to \{0,1\}^m \qquad (n < m)$$

which stretches a short random string $\mathbf{x}$ to a long random string $G_n(\mathbf{x})$ such that a deterministic polytime algorithm f cannot distinguish them, i. e. the difference between

$$\mathop{\mathbf{Pr}}_{\mathbf{x}\in\{0,1\}^n}[f(G_n(\mathbf{x})) = 1] \qquad \text{and}$$

$$\mathop{\mathbf{Pr}}_{\mathbf{y}\in\{0,1\}^m}[f(\mathbf{y}) = 1]$$

is small.

Hence, a random generator for size m can be replaced by a random generator for size n together with G_n without affecting f essentially.

Pseudorandom Generators in Proof Complexity

Definition

A generator is a family $(G_n)_{n \in \mathbb{N}}$ such that $G_n : \{0,1\}^n \to \{0,1\}^m$ for some $m > n$.

Definition

A generator $(G_n : \{0,1\}^n \to \{0,1\}^m)_{n \in \mathbb{N}}$ is hard for a propositional proof system P iff
for all $n \in \mathbb{N}$ and for any string $b \in \{0,1\}^m \setminus \mathrm{Image}(G_n)$
there is no efficient P-proof of the statement $\ulcorner G_n(x_1, \ldots, x_n) \neq b \urcorner$.

($x_1, \ldots, x_n$ are propositional variables)

Purpose

To establish a lower bound, it suffices to . . .

- . . . find a generator G_n.
- . . . find an encoding of $\ulcorner G_n(x_1, \ldots, x_n) \neq b \urcorner$.

Table of contents

Nisan-Wigderson Generator

Let $A = (a_{i,j})$ be matrix of dimension $m \times n$ over $\{0, 1\}$.
For any row number $i \in [m]$ let

$$J_i(A) := \{j \in [n] \mid a_{i,j} = 1\} \text{ and}$$
$$X_i(A) := \{x_j \mid j \in J_i(A)\}.$$

Nisan-Wigderson Generator

Let $A = (a_{i,j})$ be matrix of dimension $m \times n$ over $\{0, 1\}$.
For any row number $i \in [m]$ let

$$J_i(A) := \{j \in [n] \mid a_{i,j} = 1\} \text{ and}$$
$$X_i(A) := \{x_j \mid j \in J_i(A)\}.$$

Let $g_1(x_1, \ldots, x_n)$, $\ldots$, $g_m(x_1, \ldots, x_n)$ be boolean functions such that $\mathrm{Vars}(g_i) \subseteq X_i(A)$ for all $i \in [m]$.

Nisan-Wigderson Generator

Let $A = (a_{i,j})$ be matrix of dimension $m \times n$ over $\{0, 1\}$.
For any row number $i \in [m]$ let

$$J_i(A) := \{j \in [n] \mid a_{i,j} = 1\} \text{ and}$$
$$X_i(A) := \{x_j \mid j \in J_i(A)\}.$$

Let $g_1(x_1, \ldots, x_n)$, ..., $g_m(x_1, \ldots, x_n)$ be boolean functions such that $\mathrm{Vars}(g_i) \subseteq X_i(A)$ for all $i \in [m]$.

We are interested in the system of boolean equations:

$$g_1(x_1, \ldots, x_n) = 1$$
$$\vdots$$
$$g_m(x_1, \ldots, x_n) = 1$$

Divide and Conquer

Using Nisan-Wigderson generators, the construction of a hard generator can be decomposed into four aspects:

- combinatorial properties of matrix A,
- hardness conditions for the base functions $\vec{g}$,
- encoding of the equation system $\vec{g}(\vec{x}) = \vec{1}$, and
- a lower bound.

Combinatorial Properties of Matrix A

For a set of rows $I \subseteq [m]$, its boundary is the set

$$\partial_A(I) := \{j \in [n] \mid \exists! i \in I . a_{i,j} = 1\}.$$

Remark: $\partial_A(I)$ defines a function $\partial_A(I) \to I$.

A is an (r, s, c)-expander iff

- for all $i \in [m]$: $|J_i(A)| \leq s$, and
- for all $I \subseteq [m]$: $|I| \leq r$ implies $|\partial_A(I)| \geq c\,|I|$.

Encoding of A and $\vec{g}$

There are many possible encodings. All share one common property.

Informal Equation on Encodings

Complexity of a proof for $\ulcorner \vec{g}(\vec{x}) \neq \vec{1} \urcorner =$
Complexity of the functions $\vec{g}(\vec{x})$ –
Complexity of the encoding $\ulcorner \cdot \urcorner$

Functional Encoding of A and $\vec{g}$

For every Boolean function f satisfying $\mathsf{Vars}(f) \subseteq X_i(A)$ for some $i \in [m]$, an extension variable y_f is presumed, living in $\mathsf{Vars}(A)$.

Functional Encoding of A and $\vec{g}$

For every Boolean function f satisfying $\mathrm{Vars}(f) \subseteq X_i(A)$ for some $i \in [m]$, an extension variable y_f is presumed, living in $\mathrm{Vars}(A)$.

The functional encoding $\tau(A, \vec{g})$ is the CNF over the variables $\mathrm{Vars}(A)$ consisting of clauses

$$y_{f_1}^{\varepsilon_1} \vee \ldots \vee y_{f_w}^{\varepsilon_w}$$

for which a row $i \in [m]$ exists such that

- $\mathrm{Vars}(f_1) \cup \ldots \cup \mathrm{Vars}(f_w) \subseteq X_i(A)$, and
- $g_i \models f_1^{\varepsilon_1} \vee \ldots \vee f_w^{\varepsilon_w}$.

Lemma
The system $\vec{g}(\vec{x}) = \vec{1}$ is satisfiable iff $\tau(A, \vec{g})$ is satisfiable.

Examples of Clauses Generated by One Row

- y_{g_i}

Since $f(x, \vec{x}) \equiv \Big(\neg x \wedge f(0, \vec{x})\Big) \vee \Big(x \wedge f(1, \vec{x})\Big)$ for any boolean function f (Shannon-expansion):

- $y_{\neg f(x,\vec{x})} \vee y_{x \wedge f(0,\vec{x})} \vee y_{x \wedge f(1,\vec{x})}$
- $y_{\neg(\neg x \wedge f(0,\vec{x}))} \vee y_{f(x,\vec{x})}$
- $y_{\neg(x \wedge f(1,\vec{x}))} \vee y_{f(x,\vec{x})}$

Size of Functional Encoding

Lemma

If $\tau(A, \vec{g})$ is unsatisfiable then it has an unsatisfiable sub-CNF of size $\mathcal{O}(2^s m)$ provided that $|J_i(A)| \leq s$ for all $i \in [m]$ for some s.

Width Lower Bound for Resolution

Definition

A boolean function f is ℓ-robust if every restriction ρ holds: if $f|_\rho$ is constant then $|\rho| \geq \ell$.

Width Lower Bound for Resolution

Definition

A boolean function f is ℓ-robust if every restriction ρ holds: if $f|_\rho$ is constant then $|\rho| \geq \ell$.

Theorem

Let A be an (r, s, c)-expander matrix of size $m \times n$ and let $g_1, \ldots, g_m$ be ℓ-robust functions such that $\mathrm{Vars}(g_i) \subseteq X_i(A)$. Then every resolution refutation of $\tau(A, \vec{g})$ must have width at least

$$\frac{r(c + \ell - s)}{2\ell}$$

provided that a certain restriction holds on c, ℓ and s.

Later on the theorem is used with $c = \frac{3}{4}s$ and $\ell = \frac{5}{8}s$, say. Thus the width lower bound is $\approx r$.

Proof of the Width Lower Bound for Resolution

The proof follows the method developed by Ben-Sasson and Wigderson:

Define a measure μ on clauses such that

- $\mu(C) \leq \mu(C_0) + \mu(C_1)$ for any resolution step

$$\frac{C_0 \quad C_1}{C},$$

- $\mu(C) = 1$ for any axiom C, and
- $\mu(\bot) > r$.

Proof of the Width Lower Bound for Resolution

The proof follows the method developed by Ben-Sasson and Wigderson:

Define a measure μ on clauses such that

- $\mu(C) \leq \mu(C_0) + \mu(C_1)$ for any resolution step

$$\frac{C_0 \quad C_1}{C},$$

- $\mu(C) = 1$ for any axiom C, and
- $\mu(\bot) > r$.

Hence there is a clause C with $r/2 < \mu(C) \leq r$.

Proof of the Width Lower Bound for Resolution

The proof follows the method developed by Ben-Sasson and Wigderson:

Define a measure μ on clauses such that

- $\mu(C) \leq \mu(C_0) + \mu(C_1)$ for any resolution step

$$\frac{C_0 \quad C_1}{C},$$

- $\mu(C) = 1$ for any axiom C, and
- $\mu(\bot) > r$.

Hence there is a clause C with $r/2 < \mu(C) \leq r$.

Finally, it suffices that the clause is wide.

Proof of the Width Lower Bound for Resolution

Definition

The measure $\mu(C)$ for a clause C is the *size* of a minimal $I \subseteq [m]$ such that

- $\forall y_f^{\varepsilon} \in C \; \exists i \in I.\ \mathrm{Vars}(f) \subseteq X_i(A)$, and ($\mu$-cover)
- $\{g_i \mid i \in I\} \models \|C\|$. ($\mu$-sem)

Proof of the Width Lower Bound for Resolution

Definition

The measure $\mu(C)$ for a clause C is the *size* of a minimal $I \subseteq [m]$ such that

- $\forall y_f^\varepsilon \in C \; \exists i \in I.\, \mathrm{Vars}(f) \subseteq X_i(A)$, and ($\mu$-cover)
- $\{g_i \mid i \in I\} \models \|C\|$. ($\mu$-sem)

Lemma

The measure μ exhibits the first two demanded properties.

Proof of the Width Lower Bound for Resolution

Lemma

- *If* $r/2 < \mu(C) \leq r$ *then the width of* C *is at least* $\frac{r(c+\ell-s)}{2\ell}$.
- $\mu(\perp) > r$ *provided that* $c + \ell \geq s + 1$.

Claim: for all $i_1 \in I_1$: $|J_{i_1} \cap \partial_A(I)| \leq s - \ell$

Proof sketch:

- $\{g_i \mid i \in I \setminus \{i_1\}\} \not\models \|C\|$.
- α witnessing assignment.
- Define a partial restriction ρ by

$$\rho(x_j) := \begin{cases} \alpha(x_j) & \text{if } j \notin J_{i_1} \cap \partial_A(I) \\ \text{undefined} & \text{otherwise} \end{cases}$$

- ρ is total for $\text{Vars}(g_i)$ for $i \neq i_1$.
- ρ is total on $\text{Vars}(\|C\|)$ since $i_1 \notin I_0$
- $g_i|_\rho = 1$ for $i \neq i_1$, and $\|C\|\,|_\rho = 0$
- By (μ-sem): $g_{i_1}|_\rho = 0$.
- Let ρ_1 be ρ restricted to the domain of g_{i_1}, i.e. to $J_{i_1}(A)$.
- Since ρ undef. on $J_{i_1} \cap \partial_A(I)$: domain of ρ_1 is $J_{i_1} \setminus \partial_A(I)$.
- As g_i is ℓ-robust: $|J_{i_1} \setminus \partial_A(I)| \geq \ell$

Proof (Auxiliary estimations).

- Since A is an (r, s, c)-expander:

$$\begin{aligned} c\,|I| &\leq |\partial_A(I)| \\ &\leq s\,|I_0| \;\;+\;\; (s-\ell)\,|I_1| \\ &= (s-\ell)\,|I| \;\;+\;\; \ell\,|I_0| \\ &\leq (s-\ell)\,|I| \;\;+\;\; \ell \cdot \mathrm{width}(C) \end{aligned}$$

- Using $|I| > r/2$:

$$\mathrm{width}(C) \geq \frac{(c+\ell-s)\,|I|}{\ell} > \frac{(c+\ell-s)r}{2\ell}$$

□

From Width Lower Bound to Size Lower Bound

Theorem

Let τ be an unsatisfiable CNF in n variable and clauses the width of which is at most w. Then every refutation of τ of size S has a clause of width $w + \mathcal{O}(\sqrt{n \log S})$.

Proof.

See "Short proofs are narrow – resolution made simple" by Ben-Sasson and Wigderson. □

Size Lower Bound for Resolution

Corollary

Let $\epsilon > 0$ be an arbitrary constant,
let A be a $(r, s, \epsilon s)$-expander of size $m \times n$, and
let $g_1, \ldots, g_m$ be $(1 - \epsilon/2)s$-robust functions such that $\mathrm{Vars}(g_i) \subseteq X_i(A)$.

Then every resolution refutation of $\tau(A, \vec{g})$ has size at least

$$exp\left(\Omega\left(\frac{r^2}{m\, 2^{2^s}}\right)\right)/2^s.$$

Addendum to the proof: Size Lower Bound for Resolution

Example for $y_{f_1} \vee y_{f_2} \vee y_{f_3} \vee y_{f_4}$

$$y_{f_1} \vee y_{f_2 \vee f_3 \vee f_4}$$

$$\overline{y}_{f_2 \vee f_3 \vee f_4} \vee f_2 \vee y_{f_3 \vee f_4} \qquad f_2 \vee f_3 \vee f_4 \longrightarrow f_2 \vee (f_3 \vee f_4)$$

$$\overline{y}_{f_3 \vee f_4} \vee y_{f_3} \vee y_{f_4}$$ similar

$$\overline{}$$

$$y_{f_1} \vee y_{f_2} \vee y_{f_3} \vee y_{f_4}$$

Existence of Expanders

Theorem

For any parameters s and n there exists an $(r, s, \frac{3}{4}s)$-expander of size $n^2 \times n$ where

$$r = \frac{\epsilon n}{s} \quad n^{-\frac{1}{s\epsilon}}$$

for some constant ϵ.

Addendum to the proof: Existence of Expanders

- To show:

$$\mathbf{Pr}\left[A \text{ is not an } (r, s, \tfrac{3}{4}s)\text{-expander}\right] \leq \sum_{\ell=1}^{r} \binom{n^2}{\ell} p_\ell$$

$$\leq \sum_{\ell=1}^{r} n^{2\ell} p_\ell$$

  where p_ℓ is the probability that any given ℓ rows violate the second expansion property.
- To estimate p_ℓ, fix a set I of rows such that $\ell = |I| \leq r$.
- each column $j \in \bigcup_{i \in I} J_i(A) \setminus \partial_A(I)$ "belongs" to at least two rows.
- Since $\partial_A(I) \subseteq \bigcup_{i \in I} J_i(A)$:

$$\left|\bigcup_{i \in I} J_i(A)\right| \leq |\partial_A(I)| + \frac{1}{2}\left(\sum_{i \in I} |J_i(A)| - |\partial_A(I)|\right).$$

Addendum to the proof: Existence of Expanders (Cont.)

- So, the violation of the the second expansion property, i.e. $|\partial_A(I)| < \frac{3}{4}s\ell$, implies $\left|\bigcup_{i\in I} J_i(A)\right| \leq \frac{7}{8}s\ell$.
- $p_\ell \leq \mathbf{Pr}\left[\left|\bigcup_{i\in I} J_i(A)\right| \leq \frac{7}{8}s\ell\right]$.
- See picture on the black board.
- Thus:

$$\mathbf{Pr}\left[\left|\bigcup_{i\in I} J_i(A)\right| \leq 7/8s\ell\right] \leq \frac{\binom{s\ell}{s\ell/8}\cdot n^{7/8s\ell}\cdot (s\ell)^{s\ell/8}}{n^{s\ell}}$$

$$\leq \binom{s\ell}{s\ell/8}\left(\frac{s\ell}{n}\right)^{s\ell/8}$$

$$\leq \left(\frac{2^8\cdot s\ell}{n}\right)^{s\ell/8}$$

Addendum to the proof: Existence of Expanders (Cont.)^2

- Putting all together:

$$\mathbf{Pr}\left[A \text{ is not an } (r,s,c)\text{-expander}\right] \leq \sum_{\ell=1}^{r} n^{2\ell}\left(\frac{2^8 \cdot s\ell}{n}\right)^{s\ell/8} \leq \sum_{\ell=1}^{r} n^{2\ell}\left(\frac{2^8 \cdot s r}{n}\right)^{s\ell/8}$$

- This geometric progression is bounded by $\frac{1}{2}$ if

$$n^2\left(\frac{2^8 \cdot s r}{n}\right)^{s/8} < \frac{1}{2}$$

- This inequality is satisfied for

$$r = \frac{\epsilon}{s} n^{-\frac{1}{s\epsilon}}$$

for $\epsilon = 2^{-16}$.

Size Lower Bounds for Resolution

Definition

Let A be a matrix over $\{0, 1\}$ of dimension $m \times n$. A sequence of functions $g_1, \ldots, g_m$ is good for A iff for each $i \in [m]$ the following holds.

- g_i is $\frac{5}{16} \log \log n$-robust and
- $\mathrm{Vars}(g_i) \subseteq X_i(A)$.

Size Lower Bounds for Resolution

Definition

Let A be a matrix over $\{0, 1\}$ of dimension $m \times n$. A sequence of functions $g_1, \ldots, g_m$ is good for A iff for each $i \in [m]$ the following holds.

- g_i is $\frac{5}{16} \log \log n$-robust and
- $\mathrm{Vars}(g_i) \subseteq X_i(A)$.

Corollary (First version)

There exists a family of $m \times n$ matrices, $A^{(m,n)}$, such that for any sequence of functions $\vec{g}$ good for $A^{(m,n)}$ and for any resolution refutation π of $\tau(A^{(m,n)}, \vec{g})$, the size of π is at least

$$exp \left(\frac{n^{2-\mathcal{O}(1/\log \log n)}}{m} \right) / \sqrt{\log(n)}.$$

Proof.

- With loss of generality, $m \leq n^2$.
- Apply the expander construction with $s = \frac{1}{2} \log \log n$ to get an $(r, s, \frac{3}{4}s)$-expander.
- Cross out all rows but m rows arbitrarily. The resulting matrix is still an $(r, s, \frac{3}{4}s)$-expander.
- Recall size lower bounds for $\tau(A, \vec{g})$ resolution refutations:

$$exp\left(\Omega\left(\frac{r^2}{m \cdot 2^{2^s}}\right)\right) / 2^s$$

...

Proof (cont.)

Using $2^{2^s} = 2^{\sqrt{\log n}} \leq n^{1/\log\log n}$ and $1/s \geq n^{-1/s}$ the exponent gets:

$$\begin{aligned}
\frac{r^2}{m \cdot 2^{2^s}} &\geq \frac{r^2}{m \cdot n^{1/\log\log n}} \\
&= \frac{\epsilon^2 n^2 n^{-\frac{2}{s\epsilon}}}{s^2 \; m \; n^{1/\log\log n}} && \text{(expand } r\text{)} \\
&= \frac{\epsilon^2 n^2 n^{-(\frac{4}{\epsilon}+1)/\log\log n}}{s^2 \; m} && \text{(expand } s\text{)} \\
&\geq \frac{\epsilon^2 n^2 n^{-(\frac{4}{\epsilon}+5)/\log\log n}}{m} && \text{(sec. inequal.)} \\
&= \epsilon^2 \frac{n^{2-\mathcal{O}(1/\log\log n)}}{m} && \square
\end{aligned}$$

Corollary (First version—just a reminder)

There exists a family of $m \times n$ matrices, $A^{(m,n)}$, such that for any sequence of functions $\vec{g}$ good for $A^{(m,n)}$ and for any resolution refutation of $\tau(A^{(m,n)}, \vec{g})$ has a size at least

$$exp\left(\frac{n^{2-\mathcal{O}(1/\log\log n)}}{m}\right) / \sqrt{\log(n)}.$$

Corollary (First version—just a reminder)

There exists a family of $m \times n$ *matrices,* $A^{(m,n)}$*, such that for any sequence of functions* $\vec{g}$ *good for* $A^{(m,n)}$ *and for any resolution refutation of* $\tau(A^{(m,n)}, \vec{g})$ *has a size at least*

$$exp\left(\frac{n^{2-\mathcal{O}(1/\log\log n)}}{m}\right) / \sqrt{\log(n)}.$$

Corollary (Second version)

There exists a family of $m \times n$ *matrices,* $A^{(m,n)}$*, such that for any sequence of functions* $\vec{g}$ *good for* $A^{(m,n)}$*:*

- $\tau(A^{(m,n)}, \vec{g} \oplus \vec{b})$ *is unsatisfiable for some* $\vec{b} \in \{0,1\}^m$ *if* $m > n$*, and*
- *for any* $\vec{b} \in \{0,1\}^m$*, any resolution refutation of* $\tau(A^{(m,n)}, \vec{g} \oplus \vec{b})$ *has a size at least*

$$exp\left(\frac{n^{2-\mathcal{O}(1/\log\log n)}}{m}\right) / \sqrt{\log(n)}.$$

Proof.

- For any $\vec{b} \in \{0,1\}^m$ the following is true.
  $$\begin{aligned} & \tau(A^{(m,n)}, \vec{g} \oplus \vec{b}) \text{ unsatisfiable} \\ \iff & \vec{g}(\vec{x}) \oplus \vec{b} = 1 \text{ is unsatisfiable wrt. } \vec{x} \\ \iff & \vec{g}(\vec{x}) = \neg\vec{b} \text{ is unsatisfiable wrt. } \vec{x} \\ \iff & \vec{g}(\vec{x}) \neq \neg\vec{b} \text{ for all } \vec{x} \in \{0,1\}^n \\ \iff & \neg\vec{b} \notin \text{Image}(\vec{g}) \end{aligned}$$
  Indeed, $\vec{g} : \{0,1\}^n \to \{0,1\}^m$ is not surjective, since $m > n$.
- Note that the robustness is invariant under negation. □

Lemma

Let $0 < \epsilon < 1$*. For any sufficiently large* k*, any random function over* k *variables is* ϵk*-robust which a probability* $\geq \frac{1}{2}$*.*

Lemma

Let $0 < \epsilon < 1$. For any sufficiently large k, any random function over k variables is ϵk-robust which a probability $\geq \frac{1}{2}$.

Proof.

A function f is not ϵk-robust iff there exists a restriction ρ such that $|\rho| < \epsilon k$ and $f|_\rho$ is constant. In particular, there exists a restriction ρ such that $|\rho| = \epsilon k$ and $f|_\rho$ is constant. Thus its truth table contains a "block" of $|\rho|$ columns and $2^{k-|\rho|}$ rows such that the result values are constant. ...

Proof (cont.).

$$\mathbf{Pr}\left[\text{f is not } \epsilon k\text{-robust}\right] \leq \frac{\binom{k}{\epsilon k} 2^{\epsilon k} \quad 2^{2^k - 2^{k-\epsilon k}+1}}{2^{2^k}}$$
$$= \underbrace{\binom{k}{\epsilon k}}_{\leq 2^k} 2^{\epsilon k - 2^{(1-\epsilon)k}+1}$$
$$\leq 2^{(1+\epsilon)k - 2^{(1-\epsilon)k}+1}$$
$$\overset{!}{<} 2^{-1}$$

For the last inequality, $(1+\epsilon)k + 2 < 2^{(1-\epsilon)k}$ suffices. For sufficiently large ks, this is true. □

Definition

Let A be a matrix over $\{0,1\}$ of dimension $m \times n$.
The characteristic function, $\chi_i^{\oplus}(A)$, of the row $i \in [m]$ is $\vec{x} \mapsto \oplus X_i(A)$.

Definition

For any $m \times n$ matrix A and $b \in \{0,1\}^m$:
$\tau_\chi(A, \vec{b}) := \tau(A, \overrightarrow{\chi^{\oplus}(A)} \oplus \vec{b})$

Corollary (Third version)

There exists a family of $m \times n$ matrices, $A^{(m,n)}$, such that:

- $\tau_\chi(A^{(m,n)}, \vec{b})$ *is unsatisfiable for some* $\vec{b} \in \{0,1\}^m$ *if* $m > n$, *and*
- *for any* $\vec{b} \in \{0,1\}^m$, *any resolution refutation of* $\tau_\chi(A^{(m,n)}, \vec{b})$ *has a size at least*

$$exp\left(\frac{n^{2-\mathcal{O}(1/\log\log n)}}{m}\right)/\sqrt{\log(n)}.$$

Proof (as patch).

Its remains to show that the functions $\chi_i^{\oplus}(A)$ are good for A. During the construction of the expander, the 1s in each rows are chosen randomly. The cancellation of its rows to get A is at random. Hence any $\chi_i^{\oplus}(A)$ is a random function on at most $1/2 \log\log n$ variables. With high probability, these are $5/8 \cdot 1/2 \log\log n$ robust, therefore also good for A. □

Remark: This is a superpolynominal lower bound.

Conclusion — Open Problems

- Improve the I/O-ration of the constructed pseudorandom generators to quadratic.
- Improve the size lower bound for functional encodings, in particular get rid of the 2^{s^s} denominator.

Conclusion — Road Not Taken

- Other encodings are possible such as the circuit encoding and the linear encoding.
- The method of pseudorandom generators admits degree and size lower bounds for the Polynomial Calculus and the Polynomial Calculus with Resolution.

Conclusion – Lesson Learned

- The technique of pseudorandom generator can separate the task of proving lower bounds into —more or less— independent subtasks.
- Other approaches like Tseitin tautologies fit into this framework.
- Concepts used in complexity theory might be also used in proof complexity.