Electronic Colloquium on Computational Complexity, Report No. 46 (2010)

Nisan-Wigderson generators in proof systems with forms of interpolation

Ján Pich[1]
Faculty of Mathematics and Physics
Charles University in Prague

March, 2010

We prove that the Nisan-Wigderson generators based on computationally hard functions and suitable matrices are hard for propositional proof systems that admit feasible interpolation.

Introduction

Proof complexity generators refer to candidate hard tautologies for strong proof systems like Frege proof system or Extended Frege. They were independently introduced by Krajíček [4] and by Alekhnovich, Ben-Sasson, Razborov, and Wigderson [1].

Roughly speaking, the tautologies encode the fact that $b \notin Rng(g)$ for an element b outside of the range of a map (the actual generator) $g : \{0,1\}^n \mapsto \{0,1\}^m$, where $m > n$, defined by a circuit of size $m^{O(1)}$.

If $g : \{0,1\}^{t(n)^{O(1)}} \mapsto \{0,1\}^{2^n}$ sends codes of $t(n)$-size circuits with n inputs to the truth tables of functions they compute, then the tautologies $f \notin Rng(g)$ say that f has no $t(n)$-size circuits. Denote such a formula by $\neg Circuit_{t(n)}(f)$. The hardness of such tautologies can be interpreted as the hardness of proving circuit lower bounds. This captures an element of a self-reference in the P vs NP problem.

As Razborov pointed out in [8], to prove the hardness of $\neg Circuit_{t(n)}(f)$ in a proof system, it is sufficient to show that there exists a generator $g : \{0,1\}^{t_0(n)} \mapsto \{0,1\}^{2^n}$ which is (i) constructive: for every $x \in \{0,1\}^{t_0(n)}$, there is a $t(n)$-size circuit computing y-th bit of $g(x)$ from $y \in \{0,1\}^n$, and (ii) hard: it is hard to prove $f \notin Rng(g)$ in the given proof system. Condition (i) means that for each $x \in \{0,1\}^{t_0(n)}$, the function given by the truth table $g(x)$ is computable by $t(n)$-size circuits. Therefore, since by (ii) it is hard to prove that f differs from all $g(x)$, it is also hard to prove that it is not computable by a $t(n)$-size circuit.

A prominent example of a constructive generator in the above sense is the Nisan-Wigderson generator (based on functions computable by $t(n)$-size circuits), cf. [6]. Razborov [8] conjectured that the Nisan-Wigderson generator

[1] Partially supported by a grant from The John Templeton Foundation

ISSN 1433-8092

with the original parameters as in [6] based on any poly-time function that is hard on average for $NC^1/poly$ is hard for the Frege proof system. We prove a weak version of the conjecture, namely that it holds for proof systems that admit certain form of interpolation.

Background and definitions

Symbol $\mathbb{P}$ always refers to probability with respect to the uniform distribution. For a natural number n, $[n] := \{1, ..., n\}$. We write x for a sequence of variables $x_1, ..., x_n$ where n is a number determined by the context (analogously for $y, z..$). If $S \subseteq [n]$, then $x|S$ denotes all variables x_i's such that $i \in S$. For an assigment a to x, $a|S$ is a restricted to $x|S$. When we write a formula $A(x, y) \vee B(x, z)$ we understand that $x = x_1, ..., x_n$ are the only common variables of A and B and that $y = y_1, ..., y_m, z = z_1, ..., z_l$ are some of (not necessarily all) additional variables in the respective formulas.

Definition 1. *A proof complexity generator $g : \{0, 1\}^* \mapsto \{0, 1\}^*$ is a function computed by $m^{O(1)}$-size circuits $\{C_n\}$ representing restrictions of g, $g_n : \{0, 1\}^n \mapsto \{0, 1\}^m$ for some injective function $m = m(n) > n$.*

For a proof complexity generator g and any string $b \in \{0, 1\}^m$ define the τ-formula $\tau(C_n)_b$ as $b \not\equiv C_n(x)$. The variables of $\tau(C_n)_b$ are $x_1, ..., x_n$ for inputs of C_n, and $y_1, ..., y_{m^{O(1)}}$ for gates of C_n.

$\tau(C_n)_b$ is a tautology iff $b \notin Rng(C_n)$. We shall denote the formulas simply $\tau(g)_b$ because circuits C_n are though as canonically determined by g. We also often speak about proof complexity generators while we mean the τ formulas they define.

Definition 2. *A generator g is a hard proof complexity generator for a propositional proof system P iff there is no polynomial size P-proof of any $\tau(g)_b$ (for m tending to infinity).*

A promising class of proof complexity generators is inspired by the Nisan-Wigderson generators (shortly NW-generators), cf. [6].

Definition 3. *Let $n < m$ and A be an $m \times n$ 0-1 matrix with l ones per row. $J_i(A) := \{j \in [n] | A_{ij} = 1\}$. Let $f : \{0, 1\}^l \mapsto \{0, 1\}$ be a Boolean function. Define function $NW_{A,f} : \{0, 1\}^n \mapsto \{0, 1\}^m$ as follows: The i-th bit of the output is computed by f from the bits $x|J_i(A)$.*

We speak about these functions as about NW-generators but in computational complexity the term NW-generator usually refers to the construction where f is a suitably hard function and A is in addition a (d, l) combinatorial design. The design property means that $J_i(A) \cap J_k(A)$ has size $\leq d$ for any two different rows i, j.

Assuming that the NW-generators are based on the combinatorial designs with the same parameteres as in the seminal paper [6], Razborov proposed,

Conjecture 1 (Razborov [8]). *Any NW-generator based on any poly-time function that is hard on average for $NC^1/poly$, is hard for the Frege proof system.*

Conjecture 2 (Razborov [8]). *Any NW-generator based on any function in $NP \cap coNP$ that is hard on average for P/poly, is hard for Extended Frege.*

The parameters are actually not specified more precisely in [8]. We prove

- (in Proposition 4:) Any NW-generator based on a combinatorial design as the one constructed in the proof of Lemma 2.5 in [6], and on any poly-time function hard for $NC^1/poly$ (not necessarily hard on average), is hard for any proof system with the formula interpolation.
- (in Proposition 2:) Any NW-generator based on any function such that for any $m^{O(1)}$-size circuit C, $|\mathbb{P}[C(x) = f(x)] - \frac{1}{2}| < \frac{1}{2m}$, (and on a matrix that is not necessarily a combinatorial design), is hard for any proof system with the constructive interpolation.

Definition 4. *A proof system P admits*

EIP - effective interpolation iff there is a polynomial $p(x)$ such that for any disjunction $A(x,y) \vee B(x,z)$ with P-proof of size m there is a $p(m)$-size circuit $C(x)$ that for each assigment a to x finds out a tautology from the set $\{A(a,y), B(a,z)\}$.

CIP - constructive interpolation iff there is a polynomial $p(x)$ such that for any disjunction $A(x,y) \vee B(x,z)$ with P-proof of size m there is a $p(m)$-size circuit $C(x)$ that for each assigment a to x finds out an $O(m)$-size proof for a tautology in $\{A(a,y), B(a,z)\}$.

FIP - formula interpolation iff P admits EIP but the circuit $C(x)$ is in fact a formula.

These interpolations are not believed to hold in strong proof systems. Krajíček [3] however proved that resolution admits EIP and one of his proofs gives also CIP. Pudlák [7] later gave a different proof of CIP with better bound on proofs: the constructed proof is of size $\leq m$. It is also not hard to see that tree-like resolution admits FIP.

Results of the paper

The idea behind using feasible interpolation for the lengths-of-proofs lower bounds is to find a pair of disjoint NP sets that is not possible to separate by a set in P/poly: The tautologies expressing the disjointness of the pair cannot have short proofs in any proof system with EIP.

We now observe that this idea can be captured via the τ-formulas.

Denote $[f(x) \neq 0 \vee f(x) \neq 1]$ the tautology $\tau(NW_{A,f})_{(0,1)}$ where A is a $2 \times n$ 0-1 matrix full of ones and $f \in NP \cap coNP$ (so the tautologies say that for any x, $f(x) \neq 0$ or $f(x) \neq 1$).

Conditions $f(x) = 0$ and $f(x) = 1$ define two NP sets and the formula $[f(x) \neq 0 \vee f(x) \neq 1]$ asserts their disjointness.

Proposition 1. $[f(x) \neq 0 \vee f(x) \neq 1]$ *based on a function* $f \in NP \cap coNP$ *which does not have* $n^{O(1)}$*-size circuits is hard for any proof system* P *with EIP.*

Proof: For the sake of contradiction assume that there is a proof system P with EIP and $n^{O(1)}$-size P-proof of the given tautology. By EIP there is an $n^{O(1)}$-size circuit that can decide for every assigment a to x whether $f(a) \neq 0$ or $f(a) \neq 1$, hence it determines the value of $f(a)$, contradicting complexity of f. ■

Note that we need the assumption $f \in NP \cap coNP$ to express the tautology $\tau(NW_{A,f})_{(0,1)}$ as an $n^{O(1)}$-size formula. Analogously, the assumption $f \in NTime(m^{O(1)}) \cap coNTime(m^{O(1)})$ for $m \geq n^{O(1)}$ allows to express $\tau(NW_{A,f})_{(b_1,\ldots,b_m)}$ based on an $m \times n$ matrix A as $m^{O(1)}$-size formula

$$\bigvee_{i \leq m} \neg\alpha_{b_i}(x|J_i(A), v^i)$$

using $NTime(m^{O(1)})$-definitions of $f(x|J_i(A)) = \epsilon$, for $\epsilon = 0, 1$:

$$f(x|J_i(A)) = \epsilon \ \text{ iff } \ \exists v \ (|v| \leq m^{O(1)}) \ \alpha_\epsilon(x|J_i(A), v)$$

where α_ϵ is a polynomial time relation. The tuples of variables v^i in the disjunction are disjoint.

We use this in the following weak version of Conjecture 2.

Proposition 2. *Any NW-generator based on*

1. *any $m \times n$ 0-1 matrix A with l ones per row (not necessarily a combinatorial design)*
2. *any function $f : \{0,1\}^l \mapsto \{0,1\}$ in $NTime(m^{O(1)}) \cap coNTime(m^{O(1)})$ such that for any $m^{O(1)}$-size circuit C, $|\mathbb{P}_{x\in\{0,1\}^l}[C(x) = f(x)] - \frac{1}{2}| < \frac{1}{2m}$*

is hard for any proof system P with CIP.

Proof: Assume that there is a proof system P with CIP and $s = m^{O(1)}$-size P-proof of some $\tau(NW_{A,f})_{(b_1,\dots,b_m)}$. We will describe an $m^{O(1)}$-size circuit C such that $|\mathbb{P}_{x\in\{0,1\}^l}[C(x) = f(x)] - \frac{1}{2}| \geq \frac{1}{2m}$.

Our f is in $NTime(m^{O(1)}) \cap coNTime(m^{O(1)})$. As we noted, this means that $\tau(NW_{A,f})_{(b_1,\dots,b_m)}$ can be expressed as

$$\bigvee_{i\leq m} \neg\alpha_{b_i}(x|J_i(A), v^i)$$

CIP implies that there is an $m^{O(1)}$-size circuit which for any assigment a to the variables x outputs proof of one of the disjunctions

$$\bigvee_{i=1}^{k} \neg\alpha_{b_i}(a|J_i(A), v^i), \quad \bigvee_{i=k+1}^{m} \neg\alpha_{b_i}(a|J_i(A), v^i)$$

where $k = \lfloor \frac{m}{2} \rfloor$. The new proof has the size at most $O(s)$. Therefore, we can iterate the usage of CIP $\log m$ times and get the true value of some $f(a|J_i(A))$. The resulting circuit C' consisting of all circuits given by CIP remains $m^{O(1)}$-size and for any input a it outputs the true value of some $f(a|J_i(A))$.

Fix an $i \in [m]$ such that C' outputs the value of $f(a|J_i(A))$ for at least $\frac{2^n}{m}$ $a's \in \{0,1\}^n$. Now, let C be an $m^{O(1)}$-size circuit which uses C' to check whether given input leads to the fixed value of $f(a|J_i(A))$. If it does, then it outputs the value of $f(a|J_i(A))$, otherwise it outputs always zero or always one, whichever is better on the remaining inputs. Therefore,

$$\mathbb{P}_{x\in\{0,1\}^n}[C(x) = f(x|J_i(A))] \geq \frac{1 - 1/m}{2} + \frac{1}{m} = \frac{1}{2} + \frac{1}{2m}$$

Since $f(x|J_i(A))$ does not depend on all bits of $x = x_1, ..., x_n$ we can rewrite $\mathbb{P}_{x\in\{0,1\}^n}[C(x) = f(x|J_i(A))]$ as the average over all possible choices of values of bits from $[n] \setminus J_i(A)$ of the same expression where only $x|J_i(A)$

are choosen at random. It follows that for some particular choice of these additional values the circuit C preserves the advantage.

■

We can weaken the assumption of CIP to EIP but this will require an additional property of the matrices A in the NW-generators.

Definition 5. *Let A be an $m \times n$ 0-1 matrix with l ones per row. $J_i(A) = \{j \in [n] | A_{i,j} = 1\}$. A is l-uniform iff there is a partition of $[n]$ into l sets such that there is exactly one element of each $J_i(A)$ in each set of the partition.*

Note that $m \times n$ $(\log m, l)$ design matrices with $l = \sqrt{n}$ ones per row constructed in the proof of Lemma 2.5 in [6] are $\sqrt{n}$-uniform.

Proposition 3. *Any NW-generator based on*

1. *any $m \times n$ l-uniform matrix A with l ones per row*
2. *any function $f : \{0,1\}^l \mapsto \{0,1\}$ in $NTime(m^{O(1)}) \cap coNTime(m^{O(1)})$ such that f does not have $m^{O(1)}$-size circuits*

is hard for any proof system P with EIP.

Proof: Assume that there is a proof system P with EIP and $m^{O(1)}$-size proof of some $\tau(NW_{A,f})_b$. This $\tau(NW_{A,f})_b$ can be expressed in a form

$$\bigvee_i \neg\alpha_0(x|J_i(A), v^i) \vee \bigvee_j \neg\alpha_1(x|J_j(A), v^j)$$

where $\neg\alpha_0(x|J_i(A), v^i)$ encodes $f(x|J_i(A)) \neq 0$ and $\neg\alpha_1(x|J_j(A), v^j)$ encodes $f(x|J_j(A)) \neq 1$.

By EIP, there exists an $m^{O(1)}$-size circuit C that for every assigment a to x finds out which of $\bigvee_i \neg\alpha_0(a|J_i(A), v^i)$, $\bigvee_j \neg\alpha_1(a|J_j(A), v^j)$ is true.

Denote now by S a partition of $[n]$ certifying that A is l-uniform. An $m^{O(1)}$-size circuit computing f proceed as follows.

It extends input $a \in \{0,1\}^l$ to $\overline{a} \in \{0,1\}^n$ where $\overline{a}_i$ for $i \in K$, K a block of S, has the same value as a_j where $j \in K \cap J_1(A)$ (which is uniquely determined). Then it uses the circuit C to find out which of $\bigvee_i \neg\alpha_0(\overline{a}|J_i(A), v^i)$, $\bigvee_j \neg\alpha_1(\overline{a}|J_j(A), v^j)$ is true. If it is the former one, then it outputs 1, otherwise 0.

This circuit finds the true value of $f(a)$ because the uniformity of A implies that if $\bigvee_i \neg\alpha_0(\overline{a}|J_i(A), v^i)$ then all $\neg\alpha_0(\overline{a}|J_i(A), v^i)$'s hold, resp. if $\bigvee_j \neg\alpha_1(\overline{a}|J_j(A), v^j)$ then all $\neg\alpha_1(\overline{a}|J_j(A), v^j)$'s hold.

■

To derive a weak version of Conjecture 1 we need to consider the strong form FIP of the interpolation property.

Proposition 4. *Any NW-generator based on any $m \times n$ l-uniform matrix A with l ones per row, and on any poly-time function which is not in $NC^1/poly$, is hard for any pps P with FIP.*

Proof: If we replace EIP by FIP in proof of Proposition 3, we obtain a poly-size formula computing f. Using a well known technique, the formula can be equivally rewritten as poly-size formula with logarithmic depth. ■

It is easy to construct an $m \times n$ l-uniform matrix for $m = 2^{n^\delta}$, where $\delta < 1$ (in the proof of Lemma 2.5 in [6], Nisan and Wigderson constructed $2^{n^\delta} \times n$ $\sqrt{n}$-uniform matrices that are also $(n^\delta, \sqrt{n})$ designs). Our Propositions hold for such large m too. Moreover, NW-generators based on poly-time functions are constructive. Therefore, according to the discussion from the introduction, Proposition 4 implies that if there exists a poly-time function hard for $NC^1/poly$, then it is hard to prove any superpolynomial circuit lower bound in proof systems with FIP, this applies e.g. to tree-like resolution.

Let us note in the end that if $NP = coNP$, then there is a function $f \in NTime(2^{O(l)}) \cap coNTime(2^{O(l)})$ such that $(*)$: for any $2^{\Omega(l)}$-size circuit C, $|\mathbb{P}[C(x) = f(x)] - 1/2| < 1/2^{\Omega(l)}$ (see Theorem 3.1 in [5]).

If we set $m = 2^l$ (and e.g. $l = \sqrt{n}$) in Proposition 4, then its assumptions require a function such that $|\mathbb{P}[C(x) = f(x)] - 1/2| < 1/2^{O(l)}$ for any $2^{O(l)}$-size circuit C. Of course, such function does not exist. If we could slightly weaken this assumption to ask for a function such that $(*)$, then $NP = coNP$ would imply that there is no polynomially bounded proof system with CIP, hence (unconditionally) $P \neq NP$.

Acknowledgement

I would like to thank Jan Krajíček for helpful discussions and suggestions.

References

[1] M.Alekhnovich, E.Ben-Sasson, A.A.Razborov, and A.Wigderson, Pseudorandom generators in propositional proof complexity, SIAM Journal on Computing, 34(1):67-88, 2004. In Proc. 41st IEEE Symposium on FOCS: 43-53, 2000.

[2] J.Krajíček, Bounded arithmetic, propositional logic and complexity theory, Cambridge University Press, 1995.

[3] J.Krajíček, Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, Journal of Symbolic Logic, 62(2):457-486, 1997.

[4] J.Krajíček, On the weak pigeonhole principle, Fundamenta Mathematicae, 170(1-3):123-140, 2001.

[5] J.Krajíček, Diagonalization in proof complexity, Fundamenta Mathematicae, 182:181-192, 2004.

[6] N.Nisan and A.Wigderson, Hardness vs. randomness, Journal of Computer and System Sciences, 49(2):149-167, 1994.

[7] P.Pudlák, Lower bounds for resolution and cutting planes proofs and monotone computations, Journal of Symbolic Logic, 62(3):981-998, 1997.

[8] A.A.Razborov, Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution, preprint, 2003.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de