Early View publication on www.interscience.wiley.com
(issue and page numbers not yet assigned;
citable using Digital Object Identifier – **DOI**)

Math. Log. Quart., 1 – 5 (2007) / **DOI** 10.1002/theDOIsuffix

# Nisan-Wigderson generators in proof systems with forms of interpolation

**Ján Pich***

Charles University in Prague, Faculty of Mathematics and Physics

Received XXXX, revised XXXX, accepted XXXX
Published online XXXX

**Key words** Nisan-Wigderson generator, proof complexity, feasible interpolation
**MSC (2000)** 00-xx

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.

## 1 Introduction

Proof complexity generators are used to define candidate hard tautologies for strong proof systems like Frege proof system or Extended Frege. They were independently introduced by Krajíček [3] 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 generator $g : \{0,1\}^n \longmapsto \{0,1\}^m$, where $m > n$, defined by a circuit of size $m^{O(1)}$.

If $g : \{0,1\}^{t(n)^{O(1)}} \longmapsto \{0,1\}^{2^n}$ 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 self-reference in the P vs NP problem.

As Razborov pointed out in [7], to prove the hardness of $\neg Circuit_{t(n)}(f)$ in a proof system, it is sufficient to show that there exists a generator $g : \{0,1\}^{t_0(n)} \longmapsto \{0,1\}^{2^n}$ with arbitrary $t_0(n) \leq 2^{O(n)}$ and such that $g$ is

1. 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 $y \in \{0,1\}^n$
2. hard: it is hard to prove $f \notin Rng(g)$ in the given proof system

Condition 1. 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 2. 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. [5]. Razborov [7] conjectured that the Nisan-Wigderson generator with the original parameters as in [5] 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.

## 2 Background and definitions

Symbol $\mathbf{P}$ 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

[*] Partially supported by a grant from The John Templeton Foundation E-mail: janpich@yahoo.com

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

For a proof complexity generator $g$ and any string $b \in \{0,1\}^m$ define the $\tau$-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 $g$.

**Definition 2.2** 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. [5].

**Definition 2.3** 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 $f : \{0,1\}^l \longmapsto \{0,1\}$ be a Boolean function. Define function $NW_{A,f} : \{0,1\}^n \longmapsto \{0,1\}^m$ 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 [5], Razborov proposed,

**Conjecture 2.4** *(Razborov [7]) 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 2.5** *(Razborov [7]) 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 [7]. We prove

- (in Proposition 3.5:) Any NW-generator based on a combinatorial design as the one constructed in the proof of Lemma 2.5 in [5], and on any poly-time function in $n$ hard for formulas of poly-size in $m$, is hard for any proof system with the formula interpolation.
- (in Proposition 3.2:) Any NW-generator based on any function such that for any $m^{O(1)}$-size circuit $C$, $|\mathbf{P}[C(x) = f(x)] - \frac{1}{2}| < \frac{1}{2m}$, (and on a matrix that is not necessarily a combinatorial design), is hard for any proof system with the constructive interpolation.

**Definition 2.6** A proof system P admits

- effective interpolation (EIP) 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 $x$ outputs a tautology from the set $\{A(a,y), B(a,z)\}$.
- constructive interpolation (CIP) iff there is a family of polynomial size circuits $\{C_n\}_{n=1}^{\infty}$ such that for any disjunction $A(x,y) \vee B(x,z)$ with P-proof $\pi$ of size $m$ there is a circuit $C(x,\pi) \in \{C_n\}_{n=1}^{\infty}$ that for each assigment $a$ to $x$ outputs an $O(m)$-size proof for a tautology in $\{A(a,y), B(a,z)\}$. Note that the input of the circuit $C$ contains $\pi$, so it has polynomial size in the length of $\pi$.
- formula interpolation (FIP) 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 [2] however proved that resolution admits EIP and one of his proofs gives also CIP. Pudlák [6] 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.

## 3 Results of the paper

The idea behind using feasible interpolation for proving lower bounds on the lengths of proofs 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 $\tau$-formulas.

Denote $[f(x) \neq 0 \vee f(x) \neq 1]$ the tautology $\tau(NW_{A,f})_{(0,1)}$ where $A$ is a $2 \times n$ matrix with all entries being 1 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 3.1** *$[f(x) \neq 0 \vee f(x) \neq 1]$ 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 $\tau(NW_{A,f})_{(b_1,\dots,b_m)}$ 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 $\alpha_\epsilon$ 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 2.5.

**Proposition 3.2** *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 $f : \{0,1\}^l \longmapsto \{0,1\}$ in $NTime(m^{O(1)}) \cap coNTime(m^{O(1)})$ such that for any $m^{O(1)}$-size circuit C, $|\mathbf{P}_{x \in \{0,1\}^l}[C(x) = f(x)] - \frac{1}{2}| < \frac{1}{2m}$*

*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 $|\mathbf{P}_{x \in \{0,1\}^l}[C(x) = f(x)] - \frac{1}{2}| \geq \frac{1}{2m}$.

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,

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

Since $f(x|J_i(A))$ does not depend on all bits of $x = x_1, ..., x_n$ we can rewrite $\mathbf{P}_{x\in\{0,1\}^n}[C(x) = f(x|J_i(A))]$ 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 3.3** 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 [5] are $\sqrt{n}$-uniform.

**Proposition 3.4** *Any NW-generator based on*

1. *any $m \times n$ $l$-uniform matrix $A$ with $l$ ones per row*
2. *any function $f : \{0,1\}^l \longmapsto \{0,1\}$ 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. Define a linear order on $S$ by the smallest elements of its blocks: $K < L$ for $K, L \in S$ iff $minK < minL$. 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 $i \in K_j$, $K_j$ the $j$-th smallest block of $S$, has the same value as $a_j$. 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 2.4 we need to consider the strong form FIP of the interpolation property.

**Proposition 3.5** *Any NW-generator based on any $m \times n$ $l$-uniform matrix $A$ with $l$ ones per row, and on any poly-time function in $l$ which does not have poly-size formulas in $m$, is hard for any pps P with FIP.*

Proof. If we replace EIP by FIP in proof of Proposition 3.4, we obtain a poly-size formula computing $f$. □

Let us mention a few direct applications of previous propositions.

Recall that resolution satisfies CIP (see [6]) and therefore tautologies $\tau(NW_{A,f})_b$ where $b \notin Rng(NW_{A,f})$ based on any matrix $A$ and on any function $f$ satisfying assumptions of Proposition 3.2 are hard for resolution, according to Proposition 3.2.

Further, Proposition 3.5 implies certain conditional hardness of proving superpolynomial circuit lower bounds. Firstly, note that 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 [5], 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, the resulting NW-generators based on poly-time functions are constructive in the sense that for any $x \in \{0,1\}^{n^{1/\delta}}$ the function represented by the truth table $NW(x)$ is computable by poly-size circuits in $n$. Therefore, according to the discussion from the introduction, Proposition 3.5 implies that if there exists a poly-time function hard for subexponential size formulas, then it is hard to prove any superpolynomial circuit lower bound (i.e. formulas $\neg Circuit_{t(n)}(f)$ for any superpolynomial function $t(n)$ and for any function $f$) in proof systems with FIP. This applies e.g. to tree-like resolution because a straightforward modification of the second proof of Theorem 6.1 in [2] (which proves that resolution admits EIP) actually shows that tree-like resolution proofs yield interpolants that are in fact formulas, i.e. tree-like resolution admits FIP.

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 $C$, $|\mathbf{P}[C(x) = f(x)] - 1/2| < 1/2^{\Omega(l)}$ (see Theorem 3.1 in [4]).

If we set $m = 2^l$ (and e.g. $l = \sqrt{n}$) in Proposition 3.5, then its assumptions require a function such that $|\mathbf{P}[C(x) = f(x)] - 1/2| < 1/2^{O(l)}$ 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) $P \neq NP$.

**Acknowledgements** I would like to thank Jan Krajíček for helpful discussions and suggestions. I also want to thank an anonymous referee who helped improve the presentation of the paper.

## 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).

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

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

[4] J. Krajíček, Diagonalization in proof complexity, Fundamenta Mathematicae, **182**, 181-192 (2004).

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

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

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