Electronic Colloquium on Computational Complexity, Report No. 76 (2021)

Pseudorandom Generators, Resolution and Heavy Width

Dmitry Sokolov

St. Petersburg State University
St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences

June 4, 2021

Abstract

Following the paper of Alekhnovich, Ben-Sasson, Razborov, Wigderson [Ale+04] we call a pseudorandom generator $\mathcal{F}: \{0,1\}^n \to \{0,1\}^m$ hard for for a propositional proof system P if P cannot efficiently prove the (properly encoded) statement $b \notin \mathrm{Im}(\mathcal{F})$ for any string $b \in \{0,1\}^m$.

In [Ale+04] authors suggested the "functional encoding" of considered statement for Nisan–Wigderson generator that allows the introduction of "local" extension variables. These extension variables may potentially significantly increase the power of the proof system. In [Ale+04] authors gave a lower bound $\exp\left[\frac{n^2}{m\Omega\left(2^{2^\Delta}\right)}\right]$ on the length of Resolution proofs where Δ is the degree of the dependency graph of the generator. This lower bound meets the barrier for the restriction technique.

In this paper, we introduce a "heavy width" measure for Resolution that allows showing a lower bound $\exp\left[\frac{n^2}{m2^{\mathcal{O}(\varepsilon\Delta)}}\right]$ on the length of Resolution proofs of the considered statement for the Nisan–Wigderson generator. This gives an exponential lower bound up to $\Delta := \log^{2-\delta} n$ (the bigger degree the more extension variables we can use). It is a solution to an open problem from [Ale+04].

1 Introduction

Pseudorandom generators [Yao82] is one the most important notions in modern computer science. A pseudorandom generator can be considered as a function $\mathcal{F}: \{0,1\}^n \to \{0,1\}^m$ such that for all small circuits $C \in \mathfrak{C}$:

$$\left|\Pr_{x\in\{0,1\}^n}[C(\mathcal{F}(x))] - \Pr_{y\in\{0,1\}^m}[C(y)]\right| \xrightarrow[n\to 0]{} 0,$$

where $\mathfrak{C}$ is some circuit class, and x, y are taken from the uniform distribution.

The condition on a pseudorandom generator can be rephrased in the following more informal way: "For a class of circuits $\mathfrak{C}$ it is hard to distinguish points inside and outside of the image of $\mathcal{F}$". This fact was used by Alekhnovich, Ben-Sasson, Razborov, and Wigderson [Ale+04] who suggested a natural way of viewing pseudorandom generators from the proof complexity perspective. Following [Ale+04] we call a pseudorandom generator $\mathcal{F}: \{0,1\}^n \to \{0,1\}^m$ hard for for a propositional proof system P if P cannot efficiently prove the (properly encoded as a CNF formula) statement $b \notin \mathrm{Im}(\mathcal{F})$ for any string $b \in \{0,1\}^m$. Similar constructions were also proposed by Krajíček [Kra01].

The problem of proving lower and upper bounds on the considered formulas is natural and at the same time there are lots of motivations from different areas of computer science. We discuss some of them and also refer the reader to [Ale+04; BP98; Raz15] for the detailed survey.

ISSN 1433-8092

Candidate Hard Examples for Strong Proof Systems. Despite the success of proving lower bounds on weak proof systems like Resolution, Polynomial Calculus, etc. we are still far away from lower bounds on strong proof systems like Frege or Extended Frege. Moreover, at this moment, we have few candidates for hard examples for these systems. In [Raz15] Razborov introduced explicit conjectures that formulas obtained from Nisan–Wigderson pseudorandom generators are hard for Frege and Extended Frege.

These Razborov's conjectures are based on the deep connection between pseudorandom generators and so-called Circuit formulas. That provides another important motivation in circuit complexity.

Circuit Lower Bound. In [Raz95] Razborov introduced the principle $\mathsf{Circuit}_t(f_n)$ expressing that the circuit size of the Boolean function f_n in n variables, given as its truth-table, is lower bounded by $t = t(n)$. Razborov stated that to show that a proof system P does not have efficient proofs of the formula $\mathsf{Circuit}_t(f_n)$, it suffices to design a sufficiently constructive pseudorandom generator hard for P and such that the number of output bits, as a function of the number of input bits, is as large as possible. In other words, the pseudorandom generators in proof complexity capture the arguments that are required to prove the circuit lower bounds (see also [Ale+04; Raz96]).

In this paper, we focus on the Nisan–Wigderson generators that were mention above. This partial case already illustrates all considered applications and shows the limits of the current techniques for proving lower bounds in proof complexity that we discuss next section.

1.1 Nisan–Wigderson Generators

The Nisan–Wigderson pseudorandom generator [NW94] may be described by a family of functions $\{f_1, \dots, f_m\}$ and a bipartite dependency graph $G := (L, R, E)$ where $|L| = m$, $|R| = n$ and each vertex in L has degree Δ. We identify the right part of this graph with a set of boolean variables $x_1, \dots, x_n$ and the left part with the output bits. We define a function $\mathcal{F}_{G,f}\colon \{0,1\}^n \to \{0,1\}^m$ such the j-th bit of output is defined by $f_j(x_{i_1}, x_{i_1}, \dots, x_{i_\Delta})$ where x_{i_k} are neighbours of the vertex $v_j \in L$.

Pick some $b \in \{0,1\}^n \setminus \mathrm{Im}(\mathcal{F}_{G,f})$. We produce the unsatisfiable CNF formula $\mathsf{PRG}_{G,F,b}$ that states $b \in \mathrm{Im}(\mathcal{F})$ in the most natural way i.e. we encode the constraints $f_j(x) = b_j$ independently. If the function f_j is simple enough (or Δ is small enough) then we can encode it in CNF directly in terms of $x_{i_1}, x_{i_2}, x_{i_\Delta}$. But if $\Delta \gg \log n$ this encoding will be superpolynomial even in the case of parity function. To solve this problem, in [Ale+04] the authors suggested to use "local" extension variables, so-called "functional encoding". In other words we can introduce any variable y_g which value corresponds to some function g that depends on some set of variables X_g and $X_g \subseteq \mathrm{N}(v)$ where $v \in L$ and $\mathrm{N}(v)$ is a set of neighbours of v.

Another important motivation for the considered functional encoding is that it naturally characterizes the spectrum of proof systems between Resolution and Extended Frege. To see this we remind a classical Theorem that Resolution with all extension variables is equivalent to Extended Frege [CR79; Kra95]. So if we omit the locality constraint $X_g \subseteq \mathrm{N}(v)$ and allow all possible extension variables then any lower bound on the size of Resolution proofs can be transformed into lower bounds on the Extended Frege. Note that the bigger Δ the more extension variables we allow to use, and the behaviour of Resolution is closer to the behaviour of Extended Frege. So the question about proving the lower bounds for a bigger degree of the dependency graph is extremely important.

Technical Aspects of Proving Lower Bounds. The most popular technique for proving lower bounds in proof complexity is a restriction. The main idea of this technique that we can hit the small proof by some restriction and obtain a well-structured proof. For example, this trick was used to reduce the question about the size of the resolution proof to a question about the width of proof. It can be used explicitly [Ale+04] or implicitly [CEI96; IPS99; BW01].

The "quality" of the restriction trick depends on the number of variables in our formula. Hence the lower bounds on the functional encoding of Nisan–Wigderson generator are an important barrier. The lower bound presented in [Ale+04] shows the limits of the classical restriction approach.

Prior Results. Despite the importance of the problem, only a few lower bounds are known. Alekhnovich, Ben-Sasson, Razborov, and Wigderson [Ale+04] showed a lower bound $\exp\left[\frac{n^2}{m\Omega(2^{2^\Delta})}\right]$ on the length of Resolution proofs on the functional encoding of the Nisan–Wigderson generator. Since this proof used the "pure restriction technique" it also works for the Polynomial Calculus, which was also done in the same paper. This is the only lower bound that deals with the full functional encoding. They formulated the list of open problems that included:

- to prove a lower bound that works for $m \gg n^2$;
- to get rid of 2^{2^Δ} scaling factor in the lower bound.

In [Kra06] Krajíček showed a simplified proof of the lower bound from [Ale+04], but it works only for a certain choice of the small number of local extension variables. This lower bound is given via reduction from the Pigeonhole Principle and hence it works for the bigger class of proof systems. For another choice of local extension variables Razborov [Raz15] showed a superpolynomial lower bound up to $m = \mathcal{O}\left(n^{\log n}\right)$. This lower bound works for the Resolution and k-DNF Resolution, and it is obtained via the so-called "Small Restriction Switching Lemma" [SBI04; Raz15].

If we switch back from the Nisan–Wigderson generator to the general case then we must point out that in [Raz15] Razborov showed a lower bound for subexponential parameter m. This lower bound is based on two ideas: a lower bound on the Nisan–Wigderson generator, composition Theorem [Kra04; Raz15]. The generator used in this lower bound is a composition of several Nisan–Wigderson generators.

1.2 Our Results

Theorem 1.1 [Informal]

Let $G := (L, R, E)$ be an $(r, \Delta, (1-\varepsilon)\Delta)$-expander, where $|L| = m, |R| = n$. If f_i is a family of *good* functions then for any $b \notin \mathrm{Im}(\mathcal{F}_{G,f})$ any resolution proof of $\mathrm{PRG}_{G,f,b}$ requires size $\exp\left[2^{-\mathcal{O}(\varepsilon\Delta)} \cdot \frac{r^2}{m}\right]$.

For the random graphs this Theorem gives us the following result.

Theorem 1.2 [Informal]

Let n be large enough integer number, $\delta > 0$, $m := n^{2-\delta}$, $\Delta := \log^{2-\delta} n$ and $G \sim \mathcal{G}(m, n, \Delta)$. If f_i is a family of *good* functions then whp for any $b \notin \mathrm{Im}(\mathcal{F}_{G,f})$ any resolution proof of $\mathrm{PRG}_{G,f,b}$ requires size $\exp\left[n^{\Omega(\delta)}\right]$.

1.3 Our Technique

We start with the approach that gives a lower bound $\exp\left[\frac{n^2}{m\Omega(2^{2^\Delta})}\right]$ on the size of resolution proofs of $\mathrm{PRG}_{G,f}$. This strategy has the same flavor as a strategy from [Ale+04] but has some differences in details.

Let $\pi := (D_1, \dots, D_\ell)$ be a Resolution proof of $\mathrm{PRG}_{G,f}$ and H is a set of clauses of width at least w_0. For the sake of contradiction assume that π has small size and apply the following algorithm.

1. If π is small then H is small.
2. Pick the most frequent literal y in H. Note that it is contained in at least $w_0/2^{2^{\Delta}+1}$ fraction of clauses.
3. Set y to 0 in π. This operation kills all clauses that contain y.
4. After this assignment $\pi \restriction (x = 0)$ is still a proof of a restricted formula.
5. We apply a "closure" trick [AR03; Ale+04] to make sure that the remaining formula does not contain a "local contradiction" (see also an iterative version of this trick in [Sok20]).
6. Repeat while we have clauses of large width.

If H is small we kill all clauses of large width in a few iterations. To achieve a contradiction it remains to show that if there is no "local contradiction" then any resolution proof requires width at least w_0 for the right choice of w_0.

This strategy is **semantic**, i.e. we do not care about the exact form of clauses in the proof; we need only two properties:

- clauses of large width can be killed with large probability by a "random assignment";
- clauses of small width are not so easy to satisfy (we need this property for the width lower bound).

The bottleneck of the considered strategy is the fraction of clauses that contain some specific literal. So if we want to improve the lower bound, we need to expand this bottleneck. First of all, we will count a number of output bits that are "touched" by a clause rather than the number of input variables. To do it we define a "canonical form" of a clause that helps to split all variables into m baskets. Unfortunately, our canonical form of a clause is a **syntactic** representation of i.e. it heavily depends on the exact representation of a clause and not only the function defined by it.

On the one hand, the syntactic measure has already provided problems in the analysis. On the other hand, it is still not enough for our lower bound. To expand the bottleneck even more we introduce the new measure "heavy width". Informally speaking if we have clause D then we want to count only those output bits of the generator the value of which heavily correlated to a value of the clause D.

Let define the full strategy. Let $\pi := (D_1, \dots, D_\ell)$ be a Resolution proof of $\mathrm{PRG}_{G,f}$ and H is a set of clauses of heavy width at least w_0 (in other words there are at least w_0 output bits of the generator that values are correlated with the value of a clause). For the sake of contradiction assume that π has a small size and apply the following algorithm.

1. If π is small then of H is small.
2. Pick an output bit v of the generator uniformly at random.
3. Set all neighbors of v in order to satisfy constraints to this output bit. In our case this operation kills $\frac{2^{-\varepsilon\Delta}}{m}$ fraction of clauses in H
4. After this assignment the restricted proof is still a proof of a restricted formula.
5. We apply a "closure" trick to make sure that the remaining formula does not contain "local contradiction".
6. Repeat while we have clauses of large width.

If H is small we kill all clauses of large width in a few iterations. To achieve a contradiction it remains to show that if there is no “local contradiction” then any resolution proof requires a large “heavy width”.

To show the lower bound on the heavy width we equip a game approach (that is similar to [Pud00; AD08]) with a new invariant. This is the place where the problem with the syntactic definition of a canonical form arises. To avoid this problem we again will use the expansion properties of our dependency graph.

2 Preliminaries

Let x be a propositional variable, i.e., a variable that ranges over the set $\{0,1\}$. A literal of x is either x (denoted sometimes as x^1) or $\neg x$ (denoted sometimes as x^0).

Definition 2.1

Let $f\colon \{0,1\}^n \to \{0,1\}$. We say that f is (δ,k)-**balanced** for some $0<\delta\le\frac{1}{2}$ and $k\ge 0$ iff for any $b\in\{0,1\}$ and any partial assignment ρ of size at most k the size of $(f|_\rho)^{-1}(b)$ is at least $\frac{\delta}{2^{n-|\rho|}}$.

Some examples:

- $\mathsf{Parity}(x_1,\dots,x_n)$ is $\left(\frac{1}{2},n-1\right)$-balanced;
- $\mathsf{IP} := \sum\limits_{i=1}^{n/2} x_i y_i \bmod 2$ is $\left(\frac{1}{4},\frac{n}{2}-1\right)$-balanced;
- random function is $\left(\frac{1}{4},\frac{n}{5}\right)$-balanced (see Lemma A.4 for the calculations).

2.1 Expanders and Closure

We use the following notation: $\mathrm{N}_G(S)$ is the set of neighbours of the set of vertices S in the graph G, $\partial_G(S)$ is the set of unique neighbours of the set of vertices S in the graph G. We omit the index G if the graph is evident from the context.

A bipartite graph $G:=(L,R,E)$ is an (r,Δ,c)-**expander** if all vertices $u\in L$ have degree at most Δ and for all sets $S\subseteq L$, $|S|\le r$, it holds that $|\mathrm{N}(S)|\ge c\cdot|S|$. Similarly, $G:=(L,R,E)$ is an (r,Δ,c)-**boundary expander** if all vertices $u\in L$ have degree at most Δ and for all sets $S\subseteq L$, $|S|\le r$, it holds that $|\partial S|\ge c\cdot|S|$. In this context, a simple but useful observation is that

$$|\mathrm{N}(S)|\le|\partial S|+\frac{\Delta|S|-|\partial S|}{2}=\frac{\Delta|S|+|\partial S|}{2},$$

since all non-unique neighbours have at least two incident edges. This implies that if a graph G is an $(r,\Delta,(1-\varepsilon)\Delta)$-expander then it is also an $(r,\Delta,(1-2\varepsilon)\Delta)$-boundary expander.

The next proposition is well known in the literature. In this form it was used in [GMT09].

Proposition 2.2

If $G := (L, R, E)$ is an (r, Δ, c)-boundary expander then for any set $S \subseteq L$ of size $k \leq r$ there is an enumeration $v_1, v_2, \ldots, v_k \in S$ and a sequence $R_1, \ldots, R_k \subseteq \mathrm{N}(S)$ such that:

- $R_i = \mathrm{N}(v_i) \setminus \left(\bigcup_{j=1}^{i-1} \mathrm{N}(v_j) \right)$;
- $|R_i| \geq c$.

In particular, there is a matching on the set S.

Proof. We create this sequence in reversed order. Since $|S| \leq r$ it holds that $|\partial S| \geq c|S|$ and there is a vertex $v_k \in S$ such that $|\partial S \cap \mathrm{N}(v_k)| \geq c$. Let $R_k := |\partial S \cap \mathrm{N}(v_k)|$, and repeat the process on $S \setminus \{v_k\}$. □

Let $G := (L, R, E)$ denote a bipartite graph. Consider a **closure** operation that seems to have originated in [AR03; Ale+04].

Definition 2.3

For vertex sets $S \subseteq L, U \subseteq R$ we say that the set S is (U, r, ν)-**contained** if $|S| \leq r$ and $|\partial S \setminus U| < \nu|S|$. For any set $J \subseteq R$ let $S := \mathrm{Cl}^{r,\nu}(J)$ denote an arbitrary but fixed set of maximal size such that S is (J, r, ν)-contained.

Lemma 2.4

Suppose that G is an (r, Δ, c)-boundary expander and that $J \subseteq R$ has size $|J| \leq \Delta r$. Then $|\mathrm{Cl}^{r,\nu}(J)| < \frac{|J|}{c-\nu}$.

Proof. By definition we have that $|\partial \mathrm{Cl}^{r,\nu}(J) \setminus J| < \nu|\mathrm{Cl}^{r,\nu}(J)|$. Since $|\mathrm{Cl}^{r,\nu}(J)| \leq r$ by definition, the expansion property of the graph guarantees that $c|\mathrm{Cl}^{r,\nu}(J)| - |J| \leq |\partial \mathrm{Cl}^{r,\nu}(J) \setminus J|$. The conclusion follows. □

Suppose $J \subseteq R$ is not too large. Then Lemma 2.4 shows that the closure of J is not much larger. Thus, after removing the closure and its neighbourhood from the graph, we are still left with a decent expander. The following lemma makes this intuition precise.

Lemma 2.5

Let $J \subseteq R$ be such that $|J| \leq \Delta r$ and $|\mathrm{Cl}^{r,\nu}(J)| \leq \frac{r}{2}$ and let $G' := G \setminus (\mathrm{Cl}^{r,\nu}(J) \cup J \cup \mathrm{N}(\mathrm{Cl}^{r,\nu}(J)))$. Then any set S of vertices from the left side of G', with size $|S| \leq \frac{r}{2}$, satisfies that $|\partial_{G'} S| \geq \nu|S|$.

Proof. Suppose the set $S \subseteq L(G')$ violates the boundary expansion guarantee. Observe that $\mathrm{Cl}^{r,\nu}(J)$ and S are both sets of size at most $\frac{r}{2}$. Furthermore, the set $(\mathrm{Cl}^{r,\nu}(J) \cup S)$ is (J, r, ν)-contained in the graph G. As $\mathrm{Cl}^{r,\nu}(J)$ is a (J, r, ν)-contained set of maximal cardinality, this leads to a contradiction. □

2.2 Existence

For $n, m, \Delta \in \mathbb{N}$, we denote by $\mathcal{G}(m, n, \Delta)$ the distribution over bipartite graphs with disjoint vertex sets $L := \{v_1, \dots, v_m\}$ and $R := \{u_1, \dots, u_n\}$ where the neighbourhood of a vertex $v \in L$ is chosen by sampling a subset of size Δ uniformly at random from R.

The next claim follows from the standard calculation.

Lemma 2.6 [de Rezende et al. [Rez+20]]

Let n, m and Δ be large enough integers such that $m > n \geq \Delta$. Let $\xi, \chi \in \mathbb{R}^+$ be such that $\xi < 1/2$, $\xi \ln \chi \geq 2$ and $\xi \Delta \ln \chi \geq 4 \ln m$. Then for $r = n/(\Delta \cdot \chi)$ and $c = (1 - 2\xi)\Delta$ it holds asymptotically almost surely for a randomly sampled graph $G \sim \mathcal{G}(m, n, \Delta)$ that G is an (r, Δ, c)-boundary expander.

3 Nisan–Wigderson PRG and Its Encoding

Let $G := (L, R, E)$ be a bipartite graph such that $L := \{v_1, v_2, \dots, v_m\}$, $R := \{u_1, u_2, \dots, u_n\}$ and each vertex in L has degree Δ. We identify the right part of this graph with a set of boolean variables $\{x_1, x_2, \dots, x_n\}$ and the left part with a set of output bits. Based on this identity we introduce a pseudorandom generator $\mathcal{F}_{G,f} \colon \{0,1\}^n \to \{0,1\}^m$ that is defined by the graph G and a family of the **base** functions $f_1, f_2, \dots, f_m \colon \{0,1\}^\Delta \to \{0,1\}$ in the natural way: the j-th bit of output is defined by $f_j(u_{i_1}, u_{i_2}, \dots, u_{i_\Delta})$ where $u_{i_k} \in \mathrm{N}(v_j)$ is a set of neighbours of the vertex $v_j \in L$. We also use a notation $\mathrm{Vars}_j := \mathrm{N}(v_j)$.

We want to encode the question about inversion of the function $\mathcal{F}_G$ as a propositional formula. Following the [Ale+04] and [Ale+02] we allow to use "local" extension variables and say that a boolean function g is **local** iff there is some $i \in [m]$ such that g depends only on Vars_i.

3.1 Functional Encoding

Definition 3.1

Let $\mathcal{F}_{G,f} \colon \{0,1\}^n \to \{0,1\}^m$ be a pseudorandom generator based on the graph G and base functions $f_1, f_2, \dots, f_m \colon \{0,1\}^\Delta \to \{0,1\}$. Let $b \in \{0,1\}^m$ be an arbitrary point, and $\mathfrak{G}$ be a collection of local functions.

We write a CNF formula $\mathrm{PRG}_{G,f,b}$ on variables $x_1, \dots, x_n$ and variables y_g for all $g \in \mathfrak{G}$ consists of the following constraints written in CNF:

original: $y_{f_i} = b_i$;

extension: $g(x) = 1 \leftrightarrow y_g = 1$.

We omit indices of $\mathrm{PRG}_{G,f,b}$ if it is clear from the context. Following [Ale+04] we say that it is **functional encoding**.

The following observation is a straightforward corollary from the definition.

Remark 3.2 [Aleckhovich et al. [Ale+04]]

Formula $\mathrm{PRG}_{G,f,b}$ is unsatisfiable iff $b \notin \mathrm{Im}(\mathcal{F}_G)$.

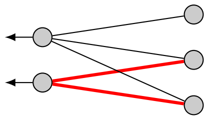

Figure 1: Dependency graph

3.1.1 Assignments, Restrictions and Clauses

Note that a variable y_{x_i} equivalent to x_i so wlog we assume that we use only y variables. Moreover if we have some assignment ρ to x variables (we call it x-**assignment**) it can define an assignment on y variables in the natural way. We denote this assignment by ρ^y and it defined by the following relation: $y_g|_{\rho^y} := y_{g|_\rho}$. We say that these assignment are **normal** and note that these assignments never violate extension axioms. In this paper we consider only normal assignments.

Consider a clause $D := (y_{g_1}^{c_1} \vee y_{g_2}^{c_2} \vee \ldots \vee y_{g_\ell}^{c_\ell})$ in y variables. Note, that under normal assignments:

- $y_g^0 \equiv y_{1-g}$;
- $y_g \vee y_{g'} \equiv y_{g \vee g'}$

and we can rewrite a clause D in the equivalent form under normal assignments $D \equiv (y_{h_1} \vee y_{h_2} \vee \ldots \vee y_{h_m})$ where

$$h_i := \bigvee_{j:\mathrm{Vars}(g_j)\in \mathrm{Vars}_i} (1 \oplus c_j \oplus g_j).$$

We say that it is a **canonical form**. It is convenient to think about a clause D as a negation of a system:

$$\begin{cases} h_1(x) = 0 \\ h_2(x) = 0 \\ \quad\vdots \\ h_m(x) = 0 \end{cases}$$

Remark 3.3

The definition of canonical form is "syntactic", or in other words it heavily depends on variables that appear in the clause D and not only on the boolean function that is defined by it.

To illustrate the remark above let consider an example: the graph is defined of fig. 1,

$$\ell(x) := x_1 \oplus x_2 \oplus x_3, \ell'(x) := x_1 \oplus x_2, \ell''(x) := x_3, D := y_\ell \vee y_{\ell'} \text{ and } D' := y_\ell \vee y_{\ell''}.$$

The canonical form of D is defined by the following functions:

$$h_1(x) := (x_1 \oplus x_2 \oplus x_3) \vee (x_1 \oplus x_2), \;\; h_2(x) := 1$$

But under normal assignments D is equivalent to D' for which the canonical form is defined by:

$$h_1(x) := (x_1 \oplus x_2 \oplus x_3) \vee x_3, \;\; h_2(x) := x_3$$

The observation 3.3 is a source of problems for the proof of the main Theorem, since we should always pay an attention to the exact form of the clauses.

4 Lower Bound

In this section we prove the main Theorem.

Theorem 4.1 [Formalization of Theorem 1.1]

Let $G := (L, R, E)$ be an $(r, \Delta, (1-\varepsilon)\Delta)$-expander, where $|L| = m, |R| = n$. If f_i is a family of $\left(\frac{1}{4}, 3\varepsilon\Delta\right)$-balanced functions then for any $b \notin \mathrm{Im}(\mathcal{F}_{G,f})$ any resolution proof of $\mathrm{PRG}_{G,f,b}$ has size $\exp\left[\Omega\left(\frac{\varepsilon^5 r^2}{2^{6\varepsilon\Delta} m}\right)\right]$.

We defer the proof of this Theorem to section 4.4. Let start with a plan of our proof.

- We introduce an analog of width measure on clauses with two important differences:
  - we want to count number of output bits that are touched by a clause rather than number of input variables;
  - we want to count only those outputs that we cannot erase from a clause "for free".

  Let call this measure "heavy width".

- We hit our proof by a random restriction. We will do it step by step and at each step we choose some output bit and assign it in order to satisfy it. This assignment equivalent to erasure some vertices from the right part of the graph. So after each step some output bit will not satisfy the expansion property of the graph. We say that these output bits are in danger and choose some assignment to satisfy them.

- We repeat this process while we do not kill all clauses of big heavy width. At this step it is important that we deal with heavy width rather than usual width.

- We prove a lower bound on the heavy width. For the sake of contradiction we assume that there is a proof of small heavy width. We trace a path in this resolution proof from the final clause to some axiom and maintain a partial assignment that:
  - do not satisfy the current clause (not that this clause may have a large classical width, hence our assignments will not set this clause to a constant);
  - do not violate any axiom.

  In the leaf these properties will give a contradiction.

We apply this Theorem for good enough graphs.

Theorem 4.2 [Formalization of Theorem 1.2]

Let n be large enough integer number, $\delta > 0$, $m := n^{2-\delta}$, $\Delta := \log^{2-\delta} n$ and $G \sim \mathcal{G}(m, n, \Delta)$. If f_i is a family of $\left(\frac{1}{4}, 3\varepsilon\Delta\right)$-balanced functions then whp for any $b \notin \mathrm{Im}(\mathcal{F}_{G,f})$ any resolution proof of $\mathrm{PRG}_{G,f,b}$ has size $\exp\left[n^{\Omega(\delta)}\right]$.

Proof. Fix $\chi := n^{\delta/10}$ and $\xi := \frac{100}{\delta \log n}$.

We use Lemma 2.6 and show that our graph G whp is an $\left(\frac{n^{1-\delta}}{\mathrm{polylog}(n)}, \log^{2-\delta} n, (1 - \frac{200}{\delta \log n})\Delta\right)$-expander. Indeed:

- $\xi < \frac{1}{2}$;

- $\xi \ln \chi = \frac{100}{\delta \log n} \frac{\delta}{10} \ln n > 2$;
- $\xi \ln \chi \Delta \geq 4 \ln m$.

Hence by Theorem 4.1 size of any resolution proof of $\mathsf{PRG}_{G,f,b}$ has size at least $\exp\left[\Omega\left(\frac{n^{2-\delta/5}}{\mathsf{polylog}(n) 2^{\Omega(\log^{1-\delta} n)} m}\right)\right] \geq \exp\left[\Omega\left(\frac{n^{2-\delta/5}}{n^{2-\delta/2}}\right)\right] = \exp\left[n^{\Omega(\delta)}\right]$. $\square$

Remark 4.3

Note that if f_i is a balanced function then $f_i(x) \oplus b_i$ is also a balanced function. Hence to simplify the notation wlog we assume that $b = 0^n$ and we omit an index b in the rest of the section. All the results holds for any $b \notin \mathrm{Im}(\mathcal{F}_{G,f})$.

4.1 The "Heavy Width"

In classical restriction technique the notion of width of a clause C is used to estimate the probability that random restriction will satisfy a clause. We give the next definition in order to save this property even if can deal with extension variables.

Definition 4.4

Fix a formula $\mathsf{PRG}_{G,f}$. Let C be a clause with canonical form: $\bigvee_{i=1}^{m} (h_i(\mathrm{N}(i)) = 1)$. We say that i-th output bit is η-**heavy** in C wrt $\mathsf{PRG}_{G,f}$ iff $\Pr_{z \leftarrow f_i^{-1}(0)} [h_i(z) = 1] \geq \eta$. And the η-**heavy width** or $\mathrm{hw}^{\eta}_{\mathsf{PRG}_{G,f}}$ of a clause C is the number of η-heavy output bits in C.

This definition of width depends on the formula.

To justify this notion we may think about "information" about i-th output bit in the clause C. We pick a point $z \in \{0,1\}^{\Delta}$ that satisfy the constraint $f_i(z) = 0$ uniformly at random. If the probability that we satisfy C by this assignment is small than C "almost avoid" y variables that belongs to i-th output bit. In this case we pretend that the clause C is independent of i-th output bit, otherwise the value of C is heavily correlated with the value of f_i.

Remark 4.5

The standard width measure can be considered as an η-heavy width measure. But in the different part of the proofs of classical resolution lower bounds we assume different parameters η.

- for the reduction from size to width: η is an absolute positive constant (usually $\frac{1}{2}$);
- for the width lower bound: $0 < \eta < \frac{1}{2^n}$.

And it works since without extension variables for local functions we can state that: if an output bit is η-heavy for some $\eta > 0$ then it also η'-heavy for some $\eta' \approx \frac{1}{2}$.

We define heavy width by using only canonical form of the clause, that may give us potential problems due to the Remark 3.3.

4.2 Size to heavy width reduction

In this section we present a random restriction argument that helps to reduce the question about size of proof to a question about η-heavy width of the proof for carefully chosen parameter η. Fix some $\mathsf{PRG}_{G,f}$.

Let define the key object that we use in our main Theorem.

Definition 4.6

Let $G := (L, R, E)$ be an $(r, \Delta, (1-\varepsilon)\Delta)$-expander. We say that an x-assignment ρ of $\mathrm{PRG}_{G,f}$ is **self-reduction** iff there is a set $L_\rho \subseteq L$ such that:

- $|L_\rho| \leq \varepsilon^2 \frac{r}{16}$;
- ρ assigns all and only variables from $\mathrm{N}(L_\rho)$, moreover ρ satisfy constraints from the set L_ρ;
- $G \setminus (L_\rho \cup \mathrm{N}(L_\rho))$ is an $(r, \Delta, (1-2\varepsilon)\Delta)$-expander.

The **size** of self-reduction is the size of the set L_ρ.

The next observation is trivial, but at the same it gives an opportunity to deal with heavy width measure since it is defined only for the PRG formulas.

Remark 4.7

If ρ is a self-reduction of $\mathrm{PRG}_{G,f}$ then $\mathrm{PRG}_{G,f}|_{\rho^y}$ is equivalent to $\mathrm{PRG}_{G',f'}$ under normal assignments where:

- $G' := G \setminus (L_\rho \cup \mathrm{N}(L_\rho))$;
- $f' := \{f'_1, \dots, f'_m\}$ and $f'_i := f_i|_\rho$.

We use the following algorithm to generate self-reductions.

Algorithm 1 r, ε are parameters.

$O_1 := \emptyset$ ▷ Set of **active** output bits
$G_1 := G$ ▷ $G_i = (L_i, R_i, E_i)$
$i := 1$
$\rho_1 := \emptyset$
For all $j \in [m]$: $p^1_j := f_j$
while $i \leq \varepsilon^3 \frac{r}{32}$ **do**
    Pick a vertex $v^i \in L_i$ uniformly at random
    Pick an x-assignment $\sigma_i \leftarrow (p^i_{v^i})^{-1}(0)$ uniformly at random
    $O_{i+1} := O_i \cup \{v^i\}$
    $G'_{i+1} := G_i \setminus (\{v^i\} \cap N_{G_i}(v^i))$
    $B_i := \max\{B \subseteq L'_{i+1} \mid |B| \leq r, |\partial_{G'_{i+1}}(B)| \leq (1-2\varepsilon)|B|\}$
    Pick an x-assignment ν_i on $\mathrm{N}_{G'_{i+1}}(B_i)$ that satisfy all constraints from the set B_i
    $G_{i+1} := G'_{i+1} \setminus (B_i \cup \mathrm{N}_{G'_{i+1}}(B_i))$
    $\rho_{i+1} := \rho_i \cup \sigma_i \cup \nu_i$
    For all $j \in [m]$: $p^{i+1}_j := f_j|_{\rho_{i+1}}$
    $i := i + 1$
return ρ_i

Following the Remark 4.7 note that $(\mathrm{PRG}_{G,f})|_{\rho^y_i}$ is equivalent to PRG_{G_i,p^i}.

Lemma 4.8

Let $G := (L, R, E)$ be an $(r, \Delta, (1-\varepsilon)\Delta)$-expander graph such that $|L| = m$, $|R| = n$ and $\frac{10}{\varepsilon} \leq r$. If $f := \{f_1, \dots, f_m\}$ is a collection of $\left(\frac{1}{4}, 3\varepsilon\Delta\right)$-balanced functions then Algorithm 4.2 generates a self-reduction of $\varphi := \mathsf{PRG}_{G,f}$.

Before the proof we present an intuition about parameters. We are given a family of expander graphs that fixes some ε (that we want to be as small as possible) and Δ. We choose a family of balanced functions with proper parameters. Parameter ε determines $\gamma := 2^{-\varepsilon\Delta}$, on the one hand it is just abbreviation, on the other hand it corresponds to the scaling factor 2^{ρ} from the definition of balanced function. In the classical Resolution lower bounds γ is some constant (that is implicit and hidden inside the proof).

Proof. Let $\ell := \varepsilon^3 \frac{r}{32}$ be the number of iterations of our algorithm.

By induction we show the following properties:

- G_i is an $(r, \Delta, (1-2\varepsilon)\Delta)$-expander;
- $|C_i| \leq \varepsilon^2 \frac{r}{32}$,

where $C_i := \bigcup\limits_{j=1}^{i} B_j$. For proof see Proposition A.3 in appendix A.

We have to show that on each iteration we can find some x-assignment ν_i that satisfy the requirements. Since $|C_i| \leq \varepsilon^2 \frac{r}{32}$ that imply, in particular, that $|B_i| \leq \varepsilon^2 \frac{r}{32}$.

Fix some iteration i. Since G_i is an $(r, \Delta, (1-2\varepsilon)\Delta)$-expander then by Lemma A.2 graph G'_{i+1} is an $(r, \Delta, (1-3\varepsilon)\Delta)$-expander. Hence by Proposition 2.2 there is an enumeration $u^1, u^2, \dots, u^{|B_i|} \in B_i$ and a sequence $R_1, \dots, R_k \subseteq \mathrm{N}_{G'_{i+1}}(S)$ such that:

- $R_e = \mathrm{N}_{G'_{i+1}}(u^e) \setminus \left(\bigcup\limits_{j=1}^{e-1} \mathrm{N}_{G'_{i+1}}(u^j)\right)$;
- $|R_e| \geq (1-3\varepsilon)\Delta$.

We define the x-assignment ν_i step by step starting from u^1. Consider an auxiliary x-assignment $\kappa := \rho_i \cup \sigma_i$. Since f_{u^1} is a $\left(\frac{1}{4}, 3\varepsilon\Delta\right)$-balanced function and κ assign at most $|\mathrm{N}_G(u^1)| - |\mathrm{N}_{G'_{i+1}}(u^1)| < 3\varepsilon\Delta$ its variables then $f_{u^1}|_{\kappa}$ is not a constant and we define an x-assignment $\nu_i^{u^1}$ to R_1 variables to satisfy the constraint $f_{u^1}(x) = 0$. We continue this process for vertices u^j and $\kappa := \rho_i \cup \sigma_i \cup \bigcup\limits_{\ell=1}^{j-1} \nu_i^{u^\ell}$. The x-assignment $\nu_i := \bigcup\limits_{\ell} \nu_i^{u^\ell}$ satisfy all constraints from the set B_i as desired.

At this moment we proved that we can realise all steps of our algorithm. The x-assignment ρ_ℓ assigns only variables from $\mathrm{N}(O_\ell \cup C_\ell)$, hence $L_\rho := O_\ell \cup C_\ell$. The first property of self-reduction is satisfied: $|L_\rho| \leq \ell + \varepsilon^2 \frac{r}{32} \leq \varepsilon^2 \frac{r}{16}$. The second follow from the construction. The third property was proved above. Moreover all intermediate x-assignments ρ_i are also satisfy these properties. $\square$

Theorem 4.9

Let $G := (L, R, E)$ be an $(r, \Delta, (1-\varepsilon)\Delta)$-expander graph such that $|L| = m$, $|R| = n$ and $\frac{10}{\varepsilon} \leq r$. Fix $\gamma := 2^{-\varepsilon\Delta}$. Let $f := \{f_1, \dots, f_m\}$ be a collection of $\left(\frac{1}{4}, 3\varepsilon\Delta\right)$-balanced functions, and $\pi := D_1, \dots, D_s$ be a resolution proof of $\varphi := \mathsf{PRG}_{G,f}$.

If $s < \exp\left(\frac{\varepsilon^3 r}{32} \cdot \frac{1}{3}\gamma^6 \frac{w}{m}\right)$ for some $w \in \mathbb{N}$ then there is a self-reduction ρ such that $\mathrm{hw}^{\gamma^3}_{\varphi|_{\rho^y}}$ of $\pi|_{\rho^y}$ is at most w.

Proof. We show that under the current assumptions Algorithm 4.2 whp give such an x-assignment. Let $\ell := \varepsilon^3 \frac{r}{32}$ be the number of iterations of our algorithm. By Lemma 4.8 it generates self-reduction ρ. We have to check that whp $\pi|_\rho$ transforms into proof of small heavy width. We do it for each clause in the proof separately.

One of the important difference of heavy width and a classical width that after application of a partial assignment it may increase since we also apply an assignment to the functions f_i and change our formula. To avoid this problem we analyse $\mathrm{hw}_\varphi^{\frac{\gamma^6}{3}}$ rather than $\mathrm{hw}_\varphi^{\gamma^3}$ of the clauses and show that for any $D \in \pi$:

- $\mathrm{hw}_{\varphi|_{\rho_i^y}}^{\frac{\gamma^6}{3}}(D|_{\pi|_{\rho_i}})$ is small for any $i \le \ell$ than this clause cannot "grow" to much in the end;
- if $\mathrm{hw}_{\varphi|_{\rho_i^y}}^{\frac{\gamma^6}{3}}(D|_{\pi|_{\rho_i}})$ is big enough for some $i \le \ell$ it will be killed with good enough probability on $i+1$-th iteration.

Let start with the first part of the proof. Fix some $i \le \ell$ and pick some alive output bit $v \in L \setminus L_\rho$. We remind a notation $p_v^i := f_v|_{\rho_i}$. Output bit v is alive and graph G_ℓ is an $(r, \Delta, (1-3\varepsilon)\Delta)$-expander, hence x-assignments ρ_i and ρ_ℓ can assign at most $3\varepsilon\Delta$ variables from $\mathrm{N}(v)$. Thus for all $i \le \ell$:

$$\begin{aligned}
\Pr_{z \leftarrow (p_v^\ell)^{-1}(0)}[h_v(z) = 1] &\le \frac{|h_v^{-1}(1) \cap (p_v^\ell)^{-1}(0)|}{|(p_v^\ell)^{-1}(0)|} \\
&\le \frac{|h_v^{-1}(1) \cap (p_v^i)^{-1}(0)|}{|(p_v^\ell)^{-1}(0)|} && (\rho_i \subseteq \rho_\ell) \\
&= \frac{|h_v^{-1}(1) \cap (p_v^i)^{-1}(0)|}{|(p_v^i)^{-1}(0)|} \cdot \frac{|(p_v^i)^{-1}(0)|}{|(p_v^\ell)^{-1}(0)|} \\
&\le \frac{|h_v^{-1}(1) \cap (p_v^i)^{-1}(0)|}{|(p_v^i)^{-1}(0)|} \cdot \frac{|f_v^{-1}(0)|}{|(p_v^\ell)^{-1}(0)|} && (p_v^i = f_v|_{\rho_i}) \\
&\le \frac{|h_v^{-1}(1) \cap (p_v^i)^{-1}(0)|}{|(p_v^i)^{-1}(0)|} \cdot \frac{\frac{3}{4}2^\Delta}{\frac{1}{4}2^{\Delta - 3\varepsilon\Delta}} && (f \text{ is balanced}) \\
&\le \Pr_{z \leftarrow (p_v^i)^{-1}(0)}[h_v(z) = 1] \cdot 3 \cdot 2^{3\varepsilon\Delta}
\end{aligned}$$

Hence for all $D \in \pi$ and all $v \in L$ if v is γ^3-heavy in $D|_{\rho_\ell}$ wrt $\varphi|_{\rho^y}$ then v is $\frac{\gamma^6}{3}$-heavy in $D|_{\rho_i^y}$ wrt $\varphi|_{\rho_i^y}$ for all $i \le \ell$. And $\mathrm{hw}_{\varphi|_{\rho_i^y}}^{\gamma^3}(D|_{\rho_\ell^y}) \ge w$ imply that $\mathrm{hw}_{\varphi|_{\rho_i^y}}^{\frac{\gamma^6}{3}}(D|_{\rho_i^y}) \ge w$ for all $i \in \ell$.

Consider a clause D in $\pi|_{\rho_{i-1}^y}$. It is killed by ρ_i^y with probability at least:

$$\begin{aligned}
\Pr_{v^i, \sigma_i}[D|_{\sigma_i} = 1] \le \Pr_{v_i, \sigma_i}[h_{v^i}|_{\sigma_i^y} = 1] \\
&= \Pr_{v^i, \sigma_i}\left[v^i \text{ is } \frac{\gamma^6}{3}\text{-heavy output bit}\right] \cdot \Pr_{v^i, \sigma_i}\left[(h_{v^i}|_{\sigma_i^y} = 0) \mid v^i \text{ is } \frac{\gamma^6}{3}\text{-heavy output bit}\right] \\
&\le \frac{|\{v^i \in [m] \mid v^i \text{ is } \frac{\gamma^6}{3}\text{-heavy output bit in } \mathrm{PRG}_{G,f,b}|_{\rho_{i-1}}\}|}{m} \cdot \frac{\gamma^6}{3}.
\end{aligned}$$

For any clause $D \in \pi$ there are two ways.

- At some moment $i \le \ell$ the $\mathrm{hw}_{\varphi|_{\rho_i^y}}^{\frac{\gamma^6}{3}}(D|_{\rho_i^y}) \le w$. In this case D is not interesting for us anymore, since as we proved above $\mathrm{hw}_{\varphi|_{\rho^y}}^{\gamma^3}(D|_{\rho^y}) \le w$.

- If $\mathrm{hw}^{\frac{\gamma^6}{3}}_{\varphi|_{\rho_i^y}}(D|_{\rho_i^y}) \geq w$ then the probability that the clause $D|_{\rho_i}$ is survived on $i+1$-th iteration is at most:
$$\Pr[D|_{\rho_i} \text{ is survived on } i+1\text{-th iteration}] \leq 1 - \frac{w}{m}\frac{\gamma^6}{3}.$$
And hence:
$$\begin{aligned} \Pr[D \text{ is survived after } \ell \text{ iterations}] &\leq \\ \prod_i \Pr[D|_{\rho_i} \text{ is survived on } i+1\text{-th iteration}] &\leq \\ \left(1 - \frac{w}{m}\frac{\gamma^6}{3}\right)^{\ell}. & \qquad \text{since } \mathrm{hw}^{\frac{\gamma^6}{3}}_{\varphi|_{\rho_i^y}}(D|_{\rho_i^y}) \geq w \end{aligned}$$

To conclude the proof note that

$$\Pr[\mathrm{hw}^{\gamma^3}_{\varphi|_{\rho_\ell^y}}(D|_{\rho_\ell^y}) > w] \leq \left(1 - \frac{w}{m}\frac{\gamma^6}{3}\right)^{\ell} = \left(1 - \frac{w}{m}\frac{\gamma^6}{3}\right)^{\varepsilon^3 \frac{r}{32}} < \left(1 - \frac{w}{m}\frac{\gamma^6}{3}\right)^{\frac{1}{\frac{w}{m}\frac{\gamma^6}{3}} \log s} < \frac{1}{s}.$$

By the union bound over all $D \in \pi$ we conclude that:

$$\Pr[\exists D \in \pi, \mathrm{hw}^{\gamma^3}_{\varphi|_{\rho_\ell^y}}(D|_{\rho_\ell^y}) > w] < 1.$$

Or in other words there is an x-assignment ρ that satisfy all required properties. $\square$

4.3 Heavy width lower bound

For the sake of contradiction assume that we have a proof $\pi := (D_1, \dots, D_s)$ of small heavy width. Starting from D_s we trace the path p in the dag of π to the initial clause. During this process we maintain a partial x-assignment σ such that in the clause $D \in p$ for any small set S of initial clauses the x-assignment σ can be extended for an x-assignment $\kappa \supseteq \rho$ such that S is satisfied by κ, but D does not. That give us a contradiction in a leaf where D should be one the initial clauses.

In this section we assume that $G := (L, R, E)$ be an $(r, \Delta, (1-\varepsilon)\Delta)$-expander and $\mathrm{PRG}_{G,f}$ is based on this graph an some functions f_i and some point $b \notin \mathcal{F}_{G,f}$. All clauses deal with variables of $\mathrm{PRG}_{G,f}$. We also fix an abbreviation $\gamma := 2^{-\varepsilon\Delta}$.

Let start with auxiliary objects and lemmas.

Definition 4.10

Let ρ be a self-reduction of $\mathrm{PRG}_{G,f}$. Let C be a clause, I_η be a set of η-heavy output bits wrt $\mathrm{PRG}_{G,f}|_{\rho^y}$. We say that an output bit v is (η,ν)-**dangerous** for a clause C iff $v \in \mathrm{Cl}^{r,\nu}(\mathrm{N}_G(I_\eta \cup L_\rho))$. Denote this set by $\mathcal{D}^{\eta,\nu}_{C,\rho}$.

Note that this definition make sense only if graph G is an expander. Also note that $I_\eta \cup L_\rho \subseteq \mathrm{Cl}^{r,\nu}(\mathrm{N}_G(I_\eta \cup L_\rho))$. For fixed parameters η and ν and a clause C we also say that an x-assignment $\sigma \supseteq \rho$ is (η,ν)-**locally consistent** iff:

- $\sigma^{-1}(\{0,1\}) = \mathrm{N}(\mathcal{D}^{\eta,\nu}_{C,\rho})$;
- $C|_{\sigma^y} \not\equiv 1$;
- σ satisfy all constraints that correspond to $\mathcal{D}^{\eta,\nu}_C$.

The following Lemma is the heart of the proof. It says that locally consistent assignments cannot *violate* any constraint from our formula.

Lemma 4.11

Let $f := \{f_1, \dots, f_m\}$ be a collection of $\left(\frac{1}{4}, 3\varepsilon\Delta\right)$-balanced functions, $\gamma < \frac{1}{8}$ and ρ be a self-reduction of $\mathrm{PRG}_{G,f}$. If C is a clause such that $\mathrm{hw}^{\gamma^3}_{\mathrm{PRG}_{G,f}|_\rho}(C) \leq \varepsilon\frac{r}{8}$ and σ is a $(\gamma^3, (1-2\varepsilon\Delta))$-locally consistent assignment then for any $J \subseteq L$ such that $|J| \leq \varepsilon\frac{r}{4}$, where is an extension $\kappa \supseteq \sigma$ such that:

- $\kappa^{-1}(\{0,1\}) \supseteq \mathrm{N}(\mathcal{D}^{\gamma^3,(1-2\varepsilon)\Delta}_{C,\rho}) \cup \mathrm{N}(J)$;
- $C|_{\kappa^y} \not\equiv 1$;
- $\forall v \in J, f_v(x)|_\kappa = 0$.

Proof. Let $\mathcal{D} := \mathcal{D}^{\gamma^3,(1-2\varepsilon)\Delta}_{C,\rho}$ and the canonical form of C is the following: $\bigvee_i (h_i(x) = 1)$. Let $I := \mathrm{Cl}^{r,(1-2\varepsilon)\Delta}(\mathrm{N}_G(J) \cup \mathrm{N}_G(\mathcal{D})) \setminus \mathcal{D}$. By Lemma 2.4 $|I| \leq \frac{3}{8}r$. By the definition of closure $I \supseteq J \setminus \mathcal{D}$.

By Lemma 2.5 graph $G' := G \setminus (\mathcal{D} \cup \mathrm{N}_G(\mathcal{D}))$ is an $(\frac{r}{2}, \Delta, (1-2\varepsilon)\Delta)$-expander. By Proposition 2.2 there is an enumeration $v^1, v^2, \dots, v^{|I|} \in I$ and a sequence $R_1, \dots, R_{|I|} \subseteq \mathrm{N}_{G'}(S)$ such that:

- $R_i = \mathrm{N}_{G'}(v^i) \setminus \left(\bigcup_{j=1}^{i-1} \mathrm{N}_{G'}(v^j)\right)$;
- $|R_i| \geq (1-2\varepsilon)\Delta$.

We define a family of x-assignments ν_i and $\kappa_i := \bigcup_{j=1}^{i} \nu_i \cup \sigma$ step by step, starting from ν_1 in the following way:

- $\nu_i^{(-1)}(\{0,1\}) = R_i$;
- $f_{v^i}(x)|_{\kappa_i} = 0$;
- $C|_{\kappa_i^y} \not\equiv 1$.

We have to show the existence of such ν_i. Note that $|R_i| \geq (1-2\varepsilon)\Delta$ hence κ_{i-1} can assign at most $2\varepsilon\Delta$ variables in $\mathrm{N}_G(v^i)$. Since f_{v^i} is a balanced function:

$$|(f_{v^i}|_{\kappa_{i-1}})^{-1}(0)| \geq \frac{1}{4}\gamma^2 2^\Delta \geq \frac{1}{4}\gamma^2 |f_{v^i}^{-1}(0)|.$$

Output bit v^i is not γ^3-heavy hence there are at most $\gamma^3|f_{v^i}^{-1}(0)|$ different x-assignments to R_i that satisfy h_{v^i}, assuming that $\gamma < \frac{1}{8}$ we can find an assignment that maps h_{v^i} to 0 and satisfy the constraint $f_{v^i}(x) = 0$. We define $\kappa := \kappa_{|I|}$.

It remains to check that κ^y does not satisfy C, that does not immediately follow from the construction due to Remark 3.3. To show this fact we use an expansion of underlying graph. For the sake of contradiction assume that κ^y maps some variable $y_g \in C$ to 1. Consider two cases.

1. Let $\mathrm{Vars}(g) \subseteq \mathrm{N}_G(v)$ for some $v \notin \mathcal{D} \cup I$. By definition $\mathcal{D} \cup I = \mathrm{Cl}^{r,(1-2\varepsilon)\Delta}(\mathrm{N}_G(J) \cup \mathrm{N}_G(\mathcal{D}))$, hence by Lemma 2.5 graph $G \setminus (\mathcal{D} \cup I \cup \mathrm{N}_G(I \cup \mathcal{D}))$ is an $(\frac{r}{2}, \Delta, (1-2\varepsilon)\Delta)$-expander and κ

assigns at most $2\varepsilon\Delta$ variables in $\mathrm{N}_G(v)$. Thus:

$$\begin{aligned}
\Pr_{z \leftarrow f_v^{-1}(0)}[h_v(z) = 1] &\geq \Pr_{z \leftarrow f_v^{-1}(0)}[z \text{ cons. with } \kappa] \\
&\geq \Pr_{z \leftarrow \{0,1\}^\Delta}[z \text{ cons. with } \kappa \wedge f_v(z) = 0] \\
&\geq \Pr_{z \leftarrow \{0,1\}^\Delta}[z \text{ cons. with } \kappa] \cdot \Pr_{z \leftarrow \{0,1\}^\Delta}[f_v(z) = 0 \mid z \text{ cons. with } \kappa] \\
&\geq \gamma^2 \Pr_{z \leftarrow \{0,1\}^\Delta}[f_v(z) = 0 \mid z \text{ cons. with } \kappa] \\
&\geq \gamma^2 \Pr_{z \leftarrow \{0,1\}^\Delta}[f_v(z)|_\kappa = 0] \\
&\geq \frac{\gamma^2}{4} \geq \gamma^3. && f_v \text{ is balanced}
\end{aligned}$$

But in this case $v \in \mathcal{D}$ by definition of $\mathcal{D}$.

2. Let $\mathrm{Vars}(g) \subseteq \mathrm{N}_G(v)$ for some $v \in \mathcal{D} \cup I$. But in this case $g|_\kappa = 1$ imply that $h_v|_\kappa = 1$. That contradicts with the constructions of κ.

$\square$

Theorem 4.12

Let $\varepsilon < \frac{1}{3}$, $G := (L, R, E)$ be an $(r, \Delta, (1-\varepsilon)\Delta)$-expander graph such that $|L| = m$, $|R| = n$. Fix $\gamma := 2^{-\varepsilon\Delta} < \frac{1}{8}$. If $f := \{f_1, \dots, f_m\}$ is a collection of $\left(\frac{1}{4}, 3\varepsilon\Delta\right)$-balanced functions then $\mathrm{hw}^{\gamma^3}_{\mathrm{PRG}_{G,f}|_{\rho^y}}$ of any resolution proof of $\mathrm{PRG}_{G,f}|_{\rho^y}$ is at least $\varepsilon^2 \frac{r}{16}$ where ρ is self-reduction.

Proof. For the sake of contradiction assume that $\pi := (D_1, \dots, D_s)$ is a resolution proof of $\mathrm{PRG}_{G,f}|_{\rho^y}$ of $\mathrm{hw}^{\gamma^3}_{\mathrm{PRG}_{G,f}|_{\rho^y}}$ at most $\varepsilon^2 \frac{r}{16}$. For a clause $D_i \in \pi$ we denote $\mathcal{D}_i := \mathcal{D}^{\gamma^3,(1-2\varepsilon)\Delta}_{D_i,\rho}$.

For the clause D_s an x-assignment ρ is locally consistent, since graph $(G \setminus (L_\rho \cup \mathrm{N}(L_\rho))$ is an $(r, \Delta, (1-2\varepsilon)\Delta)$-expander. We want to show that the existence of a locally consistent assignment κ^D for some clause $D \in \pi$ imply the existence of a locally consistent assignment for at least one of its predecessors in π. In this case the can trace the path from D_s to some initial clause $D_\ell \in \pi \cap \mathrm{PRG}_{G,f}|_{\rho^y}$ and show the existence of a locally consistent assignment κ^{D_ℓ} for this clause. The clause D_ℓ:

- either an extension axiom that corresponds to some some $v \in L$,
- or a clause that encodes the constraint $f_v(x) = 0$ for some $v \in L$.

Let start with the second case. In this case v is 1-heavy for D_ℓ and for any x-assignment σ the condition $f_v(x)|_\sigma = 0$ imply that $D_\ell|_{\rho^y} \equiv 1$. This fact contradicts with the definition of locally consistent assignment. In the first case note that by Lemma 4.11 there is an extension $\sigma \supseteq \kappa^{D_\ell}$ on Vars_v such that $D_\ell|_{\sigma^y} \not\equiv 1$, but for any x-assignment σ on the variables Vars_v the assignment σ^y satisfies all extension axioms that correspond to v and hence σ^y maps D_ℓ to 1.

Suppose a locally consistent assignment κ exists for a clause $D_i \in \pi$ and D_a, D_b its predecessors. Note, that $\mathrm{hw}^{\gamma^3}_{\varphi}$ of these clauses is at most $\varepsilon^2 \frac{r}{16}$, hence Lemma 2.4 together with the upper bound $|L_\kappa| \leq \frac{\varepsilon^2 r}{16}$ imply that the sizes of $\mathcal{D}_i, \mathcal{D}_a, \mathcal{D}_b$ are at most $\varepsilon \frac{r}{16} + \varepsilon \frac{r}{16} = \varepsilon \frac{r}{8}$. By Lemma 4.11 we have an extension $\sigma \supseteq \kappa$ on $\mathrm{N}_G(\mathcal{D}_a \cup \mathcal{D}_b)$ that satisfy constraints from $\mathcal{D}_a \cup \mathcal{D}_b$ but do not satisfy D_i. And since σ do not satisfy D_i it also do not satisfy at least one of its predecessor, wlog it is D_a. And the x-assignment $\sigma \cap \mathrm{N}_G(\mathcal{D}_a)$ is a locally consistent for D_a as desired. $\square$

4.4 Proof of Theorem 4.1

For the sake of contradiction assume that $\pi := D_1, D_2, \dots, D_s$ is a resolution proof of $\mathrm{PRG}_{G,f}$ and $s \leq \exp\left[\delta \frac{\varepsilon^5 r^2}{2^{6\varepsilon\Delta} m}\right]$ for some $\delta \leq 10^{-4}$.

Fix $w := \frac{\varepsilon^2 r}{20}$ and $\gamma := 2^{-\varepsilon\Delta}$. Note that:

$$\exp\left(\frac{\varepsilon^3 r}{32} \cdot \frac{1}{3}\gamma^6 \frac{w}{m}\right) \geq \exp\left(\frac{\varepsilon^3 r}{32} \cdot \frac{1}{3}\gamma^6 \frac{\varepsilon^2 r}{20 \cdot m}\right) \geq \exp\left(\frac{\varepsilon^5}{2000} \cdot \gamma^6 \frac{r^2}{m}\right) > \exp\left(\delta\varepsilon^5 \cdot \gamma^6 \frac{r^2}{m}\right) \geq s,$$

hence we can apply Theorem 4.9 that gives a self-reduction ρ. We hit the proof π by ρ^y and the proof $\pi|_{\rho^y}$ is a proof of $\mathrm{PRG}_{G,f}|_{\rho^y}$. Moreover the $\mathrm{hw}^{\gamma^3}_{\mathrm{PRG}_{G,f}|_{\rho^y}}$ of $\pi|_{\rho^y}$ is at most w.

Since ρ is a self-reduction then by Theorem 4.12 any proof of $\mathrm{PRG}_{G,f}|_{\rho^y}$ required $\mathrm{hw}^{\gamma^3}_{\mathrm{PRG}_{G,f}|_{\rho^y}}$ at least $\varepsilon^2 \frac{r}{16} > w$. Contradiction.

5 Comments and Further Directions

The most imporant is the lower bounds on the Nisan–Widgerson generator with $m \gg n^2$. The technical barrier for doing it is the scaling factor $\frac{1}{m}$ that comes from the step 7 of the algorithm 4.2. And it is a fundamental problem of the general restriction technique that we use in proof complexity. The most promising approach for avoiding this problem is the “pseudowidth” that was created by Razborov in [Raz01; Raz03] and equipped with a closure trick in [Rez+20].

The pseudowidth technique may be viewed as a replacement of the “self-reductions” and algorithm from Section 4.2. Instead of hitting the proof by a restriction we look at the small enough proof and try to add a carefully chosen set of axioms to our formula that allows to transform this formula into a proof of small “pseudowidth”. The pseudowidth measure itself may be considered as an α-heavy width where parameter α can be different for different output bits. Unfortunately, to apply this strategy we have to deal with large enough parameters α, but all results from Section 4.3 used the fact that α is small enough. That leads to another technical, but the important open problem: can one prove that any resolution proof of $\mathrm{PRG}_{G,f}$ has $\frac{1}{100}$-heavy width at least $\Omega(n^\delta)$?

We may also ask to generalize the lower bounds to stronger proof system. It seems adaptation of this technique for Polynomial Calculus (or Sherali–Adams) may be a challenging problem if we want to go beyond the logarithmic threshold, i.e. $\Delta \gg \log n$.

References

[AD08] Albert Atserias and Víctor Dalmau. “A combinatorial characterization of resolution width.” In: *J. Comput. Syst. Sci.* 74.3 (2008), pp. 323–334. DOI: 10.1016/j.jcss.2007.06.025. URL: https://doi.org/10.1016/j.jcss.2007.06.025.

[Ale+02] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. “Space Complexity in Propositional Calculus.” In: *SIAM J. Comput.* 31.4 (2002), pp. 1184–1211. DOI: 10.1137/S0097539700366735. URL: https://doi.org/10.1137/S0097539700366735.

[Ale+04] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. “Pseudorandom Generators in Propositional Proof Complexity.” In: *SIAM J. Comput.* 34.1 (2004), pp. 67–88. DOI: 10.1137/S0097539701389944. URL: https://doi.org/10.1137/S0097539701389944.

[AR03] Michael Alekhnovich and Alexander A. Razborov. "Lower Bounds for Polynomial Calculus: Non-Binomial Case." In: *Proceedings of the Steklov Institute of Mathematics* 242 (2003). Available at http://people.cs.uchicago.edu/~razborov/files/misha.pdf. Preliminary version in *FOCS '01.*, pp. 18–35.

[BP98] Paul Beame and Toniann Pitassi. "Propositional Proof Complexity: Past, Present and Future." In: *Bull. EATCS* 65 (1998), pp. 66–89.

[BW01] Eli Ben-Sasson and Avi Wigderson. "Short proofs are narrow - resolution made simple." In: *J. ACM* 48.2 (2001), pp. 149–169. DOI: 10.1145/375827.375835. URL: https://doi.org/10.1145/375827.375835.

[CEI96] Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. "Using the Groebner Basis Algorithm to Find Proofs of Unsatisfiability." In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996.* 1996, pp. 174–183. DOI: 10.1145/237814.237860. URL: https://doi.org/10.1145/237814.237860.

[CR79] Stephen A. Cook and Robert A. Reckhow. "The Relative Efficiency of Propositional Proof Systems." In: *J. Symb. Log.* 44.1 (1979), pp. 36–50. DOI: 10.2307/2273702. URL: https://doi.org/10.2307/2273702.

[GMT09] Konstantinos Georgiou, Avner Magen, and Madhur Tulsiani. "Optimal Sherali-Adams Gaps from Pairwise Independence." In: *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques.* Ed. by Irit Dinur, Klaus Jansen, Joseph Naor, and José Rolim. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 125–139. ISBN: 978-3-642-03685-9.

[IPS99] Russell Impagliazzo, Pavel Pudlák, and Jirí Sgall. "Lower Bounds for the Polynomial Calculus and the Gröbner Basis Algorithm." In: *Computational Complexity* 8.2 (1999), pp. 127–144. DOI: 10.1007/s000370050024. URL: https://doi.org/10.1007/s000370050024.

[Kra01] Jan Krajíček. "On the weak pigeonhole principle." In: *Fundamenta Mathematicae* 170 (Jan. 2001), pp. 123–140. DOI: 10.4064/fm170-1-8.

[Kra04] Jan Krajíček. "Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds." In: *J. Symb. Log.* 69.1 (2004), pp. 265–286. DOI: 10.2178/jsl/1080938841. URL: https://doi.org/10.2178/jsl/1080938841.

[Kra06] Jan Krajíček. "Proof Complexity Generators." In: *Algorithms and Complexity in Durham 2006 - Proceedings of the Second ACiD Workshop, 18-20 September 2006, Durham, UK.* Ed. by Hajo Broersma, Stefan S. Dantchev, Matthew Johnson, and Stefan Szeider. Vol. 7. Texts in Algorithmics. King's College, London, 2006, p. 3.

[Kra95] Jan Krajíček. *Bounded arithmetic, propositional logic, and complexity theory.* Vol. 60. Encyclopedia of mathematics and its applications. Cambridge University Press, 1995. ISBN: 978-0-521-45205-2.

[NW94] Noam Nisan and Avi Wigderson. "Hardness vs Randomness." In: *J. Comput. Syst. Sci.* 49.2 (1994), pp. 149–167. DOI: 10.1016/S0022-0000(05)80043-1. URL: https://doi.org/10.1016/S0022-0000(05)80043-1.

[Pud00] Pavel Pudlák. "Proofs as Games." In: *Am. Math. Mon.* 107.6 (2000), pp. 541–550. URL: http://www.jstor.org/stable/2589349.

[Raz01] Alexander A. Razborov. "Improved Resolution Lower Bounds for the Weak Pigeonhole Principle." In: *Electron. Colloquium Comput. Complex.* 8.55 (2001). URL: http://eccc.hpi-web.de/eccc-reports/2001/TR01-055/index.html.

[Raz03] Alexander A. Razborov. “Resolution lower bounds for the weak functional pigeonhole principle.” In: *Theor. Comput. Sci.* 303.1 (2003), pp. 233–243. DOI: 10.1016/S0304-3975(02)00453-X. URL: https://doi.org/10.1016/S0304-3975(02)00453-X.

[Raz15] Alexander A. Razborov. “Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution.” In: *Ann. of Math.* 181 (2 2015), pp. 415–472. DOI: https://doi.org/10.4007/annals.2015.181.2.1.

[Raz95] Alexander A. Razborov. “Bounded Arithmetic and Lower Bounds in Boolean Complexity.” In: *Feasible Mathematics II*. Ed. by Peter Clote and Jeffrey B. Remmel. Boston, MA: Birkhäuser Boston, 1995, pp. 344–386. ISBN: 978-1-4612-2566-9.

[Raz96] Alexander A. Razborov. “Lower Bounds for Propositional Proofs and Independence Results in Bounded Arithmetic.” In: *Automata, Languages and Programming, 23rd International Colloquium, ICALP96, Paderborn, Germany, 8-12 July 1996, Proceedings*. Ed. by Friedhelm Meyer auf der Heide and Burkhard Monien. Vol. 1099. Lecture Notes in Computer Science. Springer, 1996, pp. 48–62. DOI: 10.1007/3-540-61440-0_116. URL: https://doi.org/10.1007/3-540-61440-0%5C_116.

[Rez+20] Susanna F. de Rezende, Jakob Nordström, Kilian Risse, and Dmitry Sokolov. “Exponential Resolution Lower Bounds for Weak Pigeonhole Principle and Perfect Matching Formulas over Sparse Graphs.” In: *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*. Ed. by Shubhangi Saraf. Vol. 169. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 28:1–28:24. DOI: 10.4230/LIPIcs.CCC.2020.28. URL: https://doi.org/10.4230/LIPIcs.CCC.2020.28.

[SBI04] Nathan Segerlind, Samuel R. Buss, and Russell Impagliazzo. “A Switching Lemma for Small Restrictions and Lower Bounds for k-DNF Resolution.” In: *SIAM J. Comput.* 33.5 (2004), pp. 1171–1200. DOI: 10.1137/S0097539703428555. URL: https://doi.org/10.1137/S0097539703428555.

[Sok20] Dmitry Sokolov. “(Semi)Algebraic proofs over ± 1 variables.” In: *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*. Ed. by Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy. ACM, 2020, pp. 78–90. DOI: 10.1145/3357713.3384288. URL: https://doi.org/10.1145/3357713.3384288.

[Yao82] Andrew Chi-Chih Yao. “Theory and Applications of Trapdoor Functions (Extended Abstract).” In: *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*. IEEE Computer Society, 1982, pp. 80–91. DOI: 10.1109/SFCS.1982.45. URL: https://doi.org/10.1109/SFCS.1982.45.

A Missed Lemmas

At first we show a simple auxiliary statement.

Lemma A.1

Suppose that $G := (L, R, E)$ is an (r, Δ, c)-boundary expander and that $J \subseteq R$ has size $|J| \leq \Delta r$. Then if $X \subseteq L$ has size $|X| \leq r$ and $|\partial X \setminus J| \leq \nu |X|$ then $X \leq \frac{|J|}{c-\nu}$.

Proof. The expansion property of the graph guarantees that $c|X| - |J| \leq |\partial X \setminus J|$. The conclusion follows. $\square$

Lemma A.2

Let $G := (L, R, E)$ be an $(r, \Delta, (1-\varepsilon)\Delta)$-boundary expander. Then $G \setminus (\{v\} \cup \{N(v)\})$ is an $\left(r-1, \Delta, \left(1-\frac{3}{2}\varepsilon\right)\Delta\right)$ expander where $v \in L$ is an arbitrary vertex.

Proof. Fix some $v \in L$ and denote $G' := G \setminus (\{v\} \cup \{N(v)\})$.

Consider some set of $S \subseteq (L \setminus \{v\})$ of size at most $r-1$ and denote $H := N(S) \cap N(v)$. Since G is an expander:

$$|\partial_G(S \cup v)| = |\partial_{G'} S| + \Delta - |H| \geq (1-\varepsilon)\Delta(|S|+1)$$
$$|\partial_{G'} S| \geq (1-\varepsilon)\Delta|S| - \varepsilon\Delta + |H|.$$

But from the other point of view:

$$|\partial_{G'} S| \geq |\partial_G S| - |H| \geq (1-\varepsilon)\Delta|S| - |H|.$$

Altogether:

$$|\partial_{G'} S| \geq (1-\varepsilon)\Delta|S| - \min(|H|, \varepsilon\Delta - |H|) \geq (1-\varepsilon)\Delta|S| - \frac{\varepsilon}{2}\Delta \geq \left(1 - \frac{3}{2}\varepsilon\right)\Delta|S|.$$

□

Proposition A.3 [Analog of [Sok20]]

For all $i \leq \ell$:

- G_i is an $(r, \Delta, (1-2\varepsilon)\Delta)$-expander;
- $|C_i| \leq |\varepsilon^2 \frac{r}{32}|$.

Proof. At first we prove the second claim $|C_i| \leq \varepsilon^2 \frac{r}{32}$ by induction. C_0 is an empty set. Suppose that $|C_{i-1}| \leq \varepsilon^2 \frac{r}{32}$. There are two steps in the proof:

- we show that $|B_i| \leq \frac{r}{3}$ that give us an opportunity to use expansion property for the set C_i;
- we give a lower bound on size $\partial_G C_i$ by using expansion property and the upper bound by the choice of B_i that together give us an upper bound on size of C_i.

Let start with the first step. $|\partial_G B_i \setminus \mathrm{N}_G(C_{i-1} \cup O_{i+1})| \leq |\partial_{G'_{i+1}} B_i| \leq (1-2\varepsilon)|B_i|$. By definition $|B_i| \leq r$ and hence by Lemma A.1 $|B_i| \leq \frac{|\mathrm{N}_G(C_{i-1} \cup O_{i+1})|}{\varepsilon\Delta} \leq \frac{r}{4} + \frac{\varepsilon}{32} r \leq \frac{r}{3}$. That concludes the first step.

$$
\begin{aligned}
(1-\varepsilon)\Delta|C_i| &\le \\
|\partial_G C_i| &\le && \text{by expansion} \\
\left|\bigcup_{j=1}^{i}(\partial_G B_j \setminus \mathrm{N}_G(C_{j-1}))\right| &\le \\
\left|\bigcup_{j=1}^{i}(\partial_G B_j \setminus (\mathrm{N}_G(C_{j-1}) \cup \mathrm{N}(O_{j+1}))) \cup \mathrm{N}(O_{j+1})\right| &\le \\
\left|\bigcup_{j=1}^{i}\partial_{G'_{j+1}} B_j \cup \mathrm{N}(O_{i+1})\right| &\le && \text{by the choice of } B_j \\
(1-2\varepsilon)\Delta\sum_{j=1}^{i}|B_j| + |\mathrm{N}(O_{i+1})| &\le \\
(1-2\varepsilon)\Delta|C_i| + |\mathrm{N}(O_{i+1})|&.
\end{aligned}
$$

And hence $|C_i| \le \frac{|\mathrm{N}(O_{i+1})|}{\varepsilon\Delta} \le \varepsilon^2\frac{r}{32}$ as desired.

The first claim we prove by contradiction. Pick the minimal i such that $G := G_i$ is not an $(r, \Delta, (1-2\varepsilon))$-boundary expander and $S \subseteq L$ be a witness of it, i.e. $|S| \le r$ and $|\partial_G S| \le (1-2\varepsilon)|S|$. As in previous case $|\partial_G S \setminus (\mathrm{N}_G(C_{i-1}) \cup O_\ell)| \le |\partial_G S| \le (1-2\varepsilon)|S|$ hence by Lemma A.1 $|S| \le \frac{|\mathrm{N}_G(C_{i-1}) \cup O_\ell|}{\varepsilon\Delta} \le \frac{r}{2}$.

Consider a set $S \cup B_{i-1}$ and note that size of it at most r. $\partial_{G'_i}(S \cup B_{i-1}) \subseteq \partial_{G_i} S \cup \partial_{G'_i} B_{i-1}$ by definition of G_i. This implies $|\partial_{G'_i}(S \cup B_{i-1})| \le (1-2\varepsilon)\Delta|S| + (1-2\varepsilon)\Delta|B_{i-1}| = (1-2\varepsilon)\Delta|S \cup B_{i-1}|$. That contradicts with the choice of B_{i-1}. $\square$

Lemma A.4

There is a constant $n_0 \in \mathbb{N}$ such that for any $n > n_0$ if a function $f\colon \{0,1\}^n \to \{0,1\}$ is chosen uniformly at random then whp it is $(\frac{1}{4}, \frac{n}{5})$-balanced.

Proof. There are at most

$$\sum_{i=0}^{n/5}\binom{n}{i} \cdot 2^i \le 2^{(\mathrm{H}(1/5)+1/5)n}$$

different partial assignments of size at most $\frac{n}{10}$ where H is the binary entropy.

A fixed partial assignment ρ of size k corresponds to a boolean subcube $S \subseteq \{0,1\}$ of size 2^{n-k} for which we want to estimate number of ones and zeroes. Note that:

$$\Pr_f[|(f|_\rho)^{-1}(1)| \le \frac{1}{4}2^{n-k}] \le \sum_{i=0}^{2^{n-k}/4}\binom{2^{n-k}}{i} \cdot 2^{-2^{n-k}} \le 2^{-(1-\mathrm{H}(1/4))2^{n-k}} \le 2^{-0.1\cdot 2^{n-k}}.$$

Altogether:

$$
\begin{aligned}
\Pr_f\left[f \text{ is not } \left(\frac{1}{4}, \frac{n}{100}\right)\text{-balanced}\right] &\le \\
\sum_{\rho, |\rho| \le n/5}\left(\Pr_f[|(f|_\rho)^{-1}(1)| \le \frac{1}{4}2^{n-|\rho|}] + \Pr_f[|(f|_\rho)^{-1}(0)| \le \frac{1}{4}2^{n-|\rho|}]\right) &\le \\
2^{(\mathrm{H}(1/5)+1/5)n+1} \cdot 2^{-0.1\cdot 2^{\frac{4}{5}n}} \le 2^{-2^{\Omega(n)}}&.
\end{aligned}
$$

$\square$

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il