TOPIC 5
Resolution Lower Bounds for the Weak Pigeonhole Principle

(Related sections: 4.8, 18, 19)

Summary: Proof that even the weak version of the pigeonhole principle PHP_n^m, where the number $m \geq n+1$ of pigeons may be *arbitrary large*, has no resolution refutation proof shorter than $2^{\Omega(n^{1/4})}$. This resolves an old and most intriguing open problem about the power of resolution.

The pigeonhole principle PHP_n^m asserts that if $m \geq n+1$ then m pigeons cannot sit in n holes so that every pigeon is alone in its hole. In terms of 0-1 matrices, this principle asserts that, if $m \geq n+1$ then every $m \times n$ 0-1 matrix satisfies *precisely one* of the following two conditions:[1]

1. Every row has at least one 1.
2. Every column has at most one 1.

Exponential lower bounds on the length of the resolution resolution refutation proof of $\neg PHP_n^m$ were long known for the case when the number m of pigeons is not too large: $m \leq n^2/\log n$. The larger m is, the more true the principle PHP_n^m is, and it could be that $\neg PHP_n^m$ could be refuted by much shorter resolution refutation proof. And indeed, all attempts to overcome this "n^2 barrier" in last 15 years failed.

The problem was recently solved by Ran Raz.

Theorem 5.1 (Raz 2001). *For every $m \geq n+1$, every resolution refutation proof of $\neg PHP_n^m$ has length at least $2^{\Omega(n^{1/10})}$.*

Shortly after, Razborov (2001) has found a new, considerably simpler argument which even leads to a higher lower bound $2^{\Omega(n^{1/3})}$. This is already quite close to the best known upper bound $2^{\Omega(\sqrt{n \log n})}$ due to Buss and Pitassi (1996).

As an intermediate step, Razborov (2001) gives an even simpler proof of a slightly weaker lower bound $2^{\Omega(n^{1/4})}$, which already illustrated all major ideas, and we present this proof bellow.

Theorem 5.2 (Razborov 2001). *For every $m \geq n+1$, every resolution refutation proof of $\neg PHP_n^m$ has length at least $2^{\Omega(n^{1/4})}$.*

[1] Note that Condition 1 allows that a row has more than one 1. In terms of pigeons this means that one pigeon can be splitted between several holes. In a more friendly (with respect to the pigeons) version of PHP_n^m, this condition is replaced by: every row has exactly one 1 (so that each pigeon sits comfortably in some one hole). This is the *functional version* of the PHP_n^m, and exponential lower bounds on the length of the resolution proofs of it were obtained by Razborov, via an appropriate modification of the "filtering" argument described in this lecture. For more information on the proof complexity of different versions of the pigeonhole principle, visit Razborov's home page at http://genesis.mi.ras.ru/~razborov/.

Our first goal is to show that, in the case of the pigeonhole principle, we can restrict our attention to so-called *monotone* resolution refutation proof.

5.1. Monotone refutation proofs

Recall that the negation $\neg PHP_n^m$ of the pigeonhole principle asserts that m pigeons can be arranged into n pigeonholes so that no two pigeons sit in one hole. If we let

$$x_{i,j} = 1 \iff \text{the } i\text{-th pigeon sits in the } j\text{-th hole},$$

then $\neg PHP_n^m$ can be written as an unsatisfiable CNF,[2] which is a conjunction of the following clauses (we call them *axioms*):[3]

- **Pigeon Axioms:** each of the m pigeon sits in at least one of n holes:

$$x_{i,1} \vee x_{i,2} \vee \cdots \vee x_{i,n} \quad \text{for all } i = 1, \ldots, m.$$

- **Hole Axioms:** no two pigeons sit is one hole:

$$\overline{x}_{i_1,j} \vee \overline{x}_{i_2,j} \quad \text{for all } i_1 \neq i_2 \text{ and } j = 1, \ldots, n.$$

Resolution is a proof system which operates with clauses and has one rule of inference:[4]

$$\frac{C_0 \vee x_{i,j} \qquad C_1 \vee \overline{x}_{i,j}}{C} \ (C_0 \vee C_1 \leq C).$$

A *resolution refutation* of a CNF $\mathcal{F}$ is a resolution proof of the empty clause 0 from the clauses appearing in $\mathcal{F}$. The *length* (or *size*) of a resolution refutation proof P is the overall number $|P|$ of clauses in it.

A clause is *positive* if it has no negated variables. Monotone refutation for $\neg PHP_n^m$ is a proof system which operates with positive clauses and has one rule of inference:

$$\frac{C_0 \vee X_{I_0,j} \qquad C_1 \vee X_{I_1,j}}{C} \ (C_0 \vee C_1 \leq C; I_0 \cap I_1 = \emptyset),$$

where $X_{I,j} = \bigvee_{i \in I} x_{i,j}$. Note that, in general, this rule *is not* sound: there are assignments[5] satisfying both assumptions but falsifying the conclusion.[6] Still, the rule *is* sound if we consider only assignments satisfying all hole axioms; we call such assignments "legal." That is, an assignment a is *legal* if it sends no two pigeons to the same hole.

By a *monotone refutation* of $\neg PHP_n^m$ we will mean a monotone refutation of the set of pigeon axioms

$$X_{i,[n]} = x_{i,1} \vee x_{i,2} \vee \cdots x_{i,n} \quad i = 1, \ldots, m.$$

The following theorem reduces the lower bounds problem for the resolution refutation of $\neg PHP_n^m$ to the lower bounds problem of the monotone refutation of $\neg PHP_n^m$.

---

[2]Recall that a CNF is a set of clauses, each clause being an Or of literals (variables or their negations). A CNF is unsatisfiable if none of the assignments of 0-1 values to the variables can satisfy all its clauses.

[3]Note that in the book, for ease of notation, this set of axioms was denoted by PHP_n^m.

[4]Here and throughout, $C \leq C'$ means that every literal appearing in C also appears in C'.

[5]An assignment is a mapping a which gives each variable $x_{i,j}$ a value $a_{i,j} \in \{0, 1\}$. Thus, $a_{i,j} = 1$ means that a sends the i-th pigeon to the j-th hole.

[6]Just take $a_{i_0,j} = a_{i_1,j} = 1$ for some $i_0 \in I_0, i_1 \in I_1$, and let $C_0 = C_1 = C = 0$ (the empty clause). Then $X_{I_0,j}(a) = X_{I_1,j}(a) = 1$ but $0(a) = 0$.

Theorem 5.3 (Buss–Pitassi 1996). [7] *If $\neg PHP_n^m$ has a resolution refutation of length L, then $\neg PHP_n^m$ also has a monotone refutation of length at most L.*

Ex. 5.4. Prove this theorem. *Hint*: Replace each $\overline{x}_{i,j}$ by $\bigvee_{l\neq i} x_{l,j}$.

Ex. 5.5. (Buss–Pitassi 1996) A resolution refutation P is *tree-like* if no clause $C \in P$ participates as an assumption in more than one application of the inference rule (i.e., the underlying graph of P is a binary tree). Prove that, for any $m \geq n+1$, any tree-like monotone refutation P of $\neg PHP_n^m$ has length at least 2^n. *Hint*: Induction on n. For the induction step, take the clauses $C_0, C_1 \in P$ from which 0 is derived by the last application of the inference rule; consider the corresponding subproofs P_0, P_1, and apply the induction hypothesis.

Thus, Theorem 5.2 is a direct consequence of the following

Theorem 5.6 (Razborov 2001). *For every $m \geq n+1$, every monotone refutation of $\neg PHP_n^m$ has length at least $2^{\Omega(n^{1/4})}$.*

The rest of this note is devoted to the proof of this theorem, due to Razborov.

5.2. Proof idea: the pseudo-width of refutation proofs

Suppose we have a monotone refutation proof P of the pigeon axioms

$$X_{i,[n]} = \bigvee_{j=1}^{n} x_{i,j}, \qquad i = 1, \ldots, m.$$

To analyze the refutation P, we are going to allow also axioms [8] of the form

$$X_{i,J} := \bigvee_{j\in J} x_{i,j}, \qquad i \in \{1, \ldots, m\}$$

where $|J|$ exceeds a certain threshold d_i; the threshold will depend on the pigeon i. In this way we will be able to simplify the refutation P by "filtering out" of it all clauses C containing at least one such axiom (we just replace each such clause by the corresponding axiom). For this purpose we consider the "degree of freedom" $d_i(C)$ of each pigeon i in a clause C: this is the number of holes offered by C to this pigeon, that is, the number of holes j such that $x_{i,j} \in C$. The clause C is "filtered out" from the proof (i.e. can be replaced by an axiom) if $d_i(C) \geq d_i$ for at least one pigeon i.

Our first task (Fact 1 below) will be to show that if the thresholds d_i are chosen in a clever way, then in every clause C passing this filter *almost all*, namely, at least $m - O(\log |P|)$ ***pigeons pass it safely***, i.e., their "degree of freedom" in C is well below the corresponding threshold d_i (is $\leq d_i - \delta$ for particular δ). Thus, the number of pigeons who *narrowly* (= non-safely) pass the filter $(d_1, \ldots, d_m)$ is at most $O(\log |P|)$. The second task (Fact 2 below) will be to show that the number of pigeons who *narrowly* passed the filter must be at least $\Omega\left(n/(\log |P|)^3\right)$. This implies $\log |P| \geq \Omega(n^{1/4})$, as desired.

Now let us formulate these two tasks more precisely.

[7] Buss and Pitassi proved that the converse also holds: If $\neg PHP_n^m$ has a monotone refutation of length L, then $\neg PHP_n^m$ also has a resolution refutation of length at most $L^{O(1)}$.

[8] This general and often very useful trick is known as the "Contrivances Paradox:" stronger statements are sometimes easier to prove, because their analysis becomes more robust. (Proof of Theorem 27.5 from the book gives another illustration of this trick.)

For a clause C let $J_i(C)$ be the set of holes *offered* by C to the i-th pigeon,

$$J_i(C) := \{j : x_{i,j} \text{ occurs in } C\}.$$

and let

$$d_i(C) := |J_i(C)|$$

be the number of these holes, the *degree of freedom* of the i-th pigeon in the clause C.

Given a vector $d = (d_1, \ldots, d_m)$ of positive integers, a *d-axiom* is an arbitrary clause of the form $X_{i,J}$where $|J| \geq d_i$; we will also say that $X_{i,J}$ is the axiom for the i-th pigeon. Note that every monotone refutation of $\neg PHP_n^m$ is a monotone refutation of the set of d-axioms for $d_1 = \ldots = d_m = n$.

> **Ex. 5.7.** Let $m \geq n+1$ and $\mathcal{A}$ be a set of d-axioms. Suppose that it has at least one axiom for every pigeon. Show that $\mathcal{A}(a) = 0$ for all legal assignments a.

Let δ be another parameter. Say that the degree of freedom $d_i(C)$ of the i-th pigeon in a clause C is *large* if $d_i(C) \geq d_i - \delta$. We let [9]

$$I_{d,\delta}(C) := \{i : d_i(C) \geq d_i - \delta\}$$

to denote the set of those pigeons whose degree of freedom in C is not far away from the threshold d_i.

Definition 5.8. [10] The *pseudo-width* $w_{d,\delta}(P)$ of the refutation P is the maximum number of pigeons whose degree of freedom is large in at least one clause $C \in P$, that is, $w_{d,\delta}(P)$ is the maximum, over all $C \in P$, of

$$w_{d,\delta}(C) := |I_{d,\delta}(C)|.$$

Razborov's proof of Theorem 5.6 consists of two steps, establishing the following two facts.

Fact 1. *If $\neg PHP_n^m$ has a monotone refutation of length L then there exist a vector $d = (d_1, \ldots, d_m)$ with all $d_i > n/\log m$, and a set $\mathcal{A}$ of d-axioms such that $|\mathcal{A}| \leq L$, and $\mathcal{A}$ has a monotone refutation P of length at most L and pseudo-width*

$$w_{d,n/\log m}(P) \leq O(\log L).$$

Fact 2. *Let $\mathcal{A}$ be an arbitrary set of d-axioms and $\delta < d_i$ for all i. If P is a monotone refutation of $\mathcal{A}$, then*

$$w_{d,\delta}(P) \geq \Omega\left(\frac{\delta^2}{n \cdot \log|\mathcal{A}|}\right).$$

> **Ex. 5.9.** Show that these two fact imply that if $\neg PHP_n^m$ has a monotone refutation of length L, then $\log L = \Omega(n^{1/4})$. *Hint*: We may assume that $m \leq 2L$. (Why?)

[9] Note that the universes of $J_i(C)$ and $I_{d,\delta}(C)$ are different! The first consist of *holes* whereas the second consists of *pigeons*.

[10] Usually, the width of a refutation is defined as the maximum length of (=the number of literals in) its clauses. However, in the case of pigeonhole principle, such (natural) notion of width does not work (see Final Remark bellow).

5.2.1. Short proofs have small pseudo-width

To prove Fact 1 we have to somehow "filter out" clauses of large pseudo-width. For this we need the following combinatorial lemma (we give its proof in Sect. 5.3):

Lemma 5.10. (Pigeon filter lemma) *Let $R = \{r_{i,k}\}$ be an $m \times L$ matrix with integer entries. If L is sufficiently large, then there exists a sequence $r_1, \ldots, r_m$ of integers such that $r_i < \lfloor \log m \rfloor$ and for every column k at least one of the following two events happen:*

(i) *$r_{i,k} \le r_i$ for at least one row i;*
(ii) *$r_{i,k} \le r_i + 1$ for at most $O(\log L)$ rows i.*

Suppose now that $\neg PHP_n^m$ has a monotone refutation P' of length L. Set $\delta := n/\log m$, and consider the $m \times L$ matrix $R = \{r_{i,C}\}$ whose rows are pigeons i and columns are clauses $C \in P'$, and

$$r_{i,C} := \left\lfloor \frac{n - d_i(C)}{\delta} \right\rfloor + 1.$$

Let $r_1, \ldots, r_m$ be a sequence of integers guaranteed by Lemma 5.10. Set

$$d_i := \lfloor n - \delta r_i \rfloor + 1,$$

and note that $d_i > \delta$ because $r_i < \log m$.

Now take an arbitrary clause $C \in P'$. Our goal is to show that either or C contains a d-axiom (and C can be replaced by that axiom which reduces its pseudo-with $w_{d,\delta}(C)$ to 1) or $w_{d,\delta}(C) \le O(\log L)$. To show this, consider the column of M, corresponding to the clause C.

If the first case (i) in Lemma 5.10 takes place, then

$$\left\lfloor \frac{n - d_i(C)}{\delta} \right\rfloor + 1 = r_{i,C} \le r_i$$

for some pigeon i. This implies $d_i(C) \ge d_i$, because d_i is the minimal integer for which $\lfloor \frac{n-d_i}{\delta} \rfloor + 1 \le r_i$. Thus, in this case, C contains a subclause $X_{i,J}$ which is a d-axiom, and can be replaced by this axiom.

In the second case (ii) the number of pigeons i, for which $r_{i,C} \le r_i + 1$, does not exceed $O(\log L)$. By the definition, $w_{d,\delta}(C)$ is the number of those pigeons i for which $d_i(C) \ge d_i - \delta$. For each such pigeon i we have $\left\lfloor \frac{n-d_i(C)}{\delta} \right\rfloor \le \lfloor \frac{n-d_i+\delta}{\delta} \rfloor \le r_i$ or, equivalently, $r_{i,C} \le r_i + 1$. Thus, the number of such pigeons i, and hence, the pseudo-width $w_{d,\delta}(C)$ of C, cannot exceed $O(\log L)$. □

5.2.2. Pigeonhole proofs have large pseudo-width

Now we prove Fact 2.

Let $d = (d_1, \ldots, d_m)$ be an integer vector, $\mathcal{A}$ be an arbitrary set of d-axioms $\mathcal{A}$, and δ be any number such that $\delta < d_i$ for all i. Let

$$w_0 := \frac{\varepsilon \delta^2}{n \log |\mathcal{A}|}$$

where $\varepsilon > 0$ is a sufficiently small constant. Take an arbitrary monotone refutation P of $\mathcal{A}$. We will show that $w_{d,\delta}(P) > w_0$.

Suppose the opposite, i.e., that $w_{d,\delta}(C) \le w_0$ for all clauses $C \in P$. Our goal is to show that then $0 \notin P$ (i.e., that P is *not* a refutation of $\mathcal{A}$).

For an assignment a to the variables $x_{i,j}$, let

$$J_i(a) := \{j \,:\, a_{i,j} = 1\}$$

and

$$\ell := \lfloor \frac{\delta}{4w_0} \rfloor.$$

Let D be the set of all legal assignments[11] a such that $|J_i(a)| \leq \ell$ for all pigeons i. Note that legality of a implies that [12] $J_{i_1}(a) \cap J_{i_2}(a) = \emptyset$ for all $i_1 \neq i_2$.

For a set Γ of positive clauses and another positive clause C, let $\Gamma \models C$ mean that every assignment $a \in D$ satisfying all clauses from Γ also satisfies C. In this case we say that Γ *semantically implies* C.

Recall that each clause in $\mathcal{A}$ has the form $X_{i,J} := \bigvee_{j \in J} x_{i,j}$ for some pigeon i and some set J of $|J| \geq d_i$ holes; $X_{i,J}$ is the axiom for the pigeon i. Let $\mathcal{A}_i$ denote the set of all such axioms in $\mathcal{A}$, and let $\mathcal{A}_I := \bigcup_{i \in I} \mathcal{A}_i$. For a clause C, let $\mathcal{A}_C := \mathcal{A}_{I_{d,\delta}(C)}$ where, as before,

$$I_{d,\delta}(C) = \{i \,:\, d_i(C) \geq d_i - \delta\}$$

is the set of those pigeons i for which $d_i(C) \geq d_i - \delta$. That is,

$$\mathcal{A}_C = \{X_{i,J} \,:\, |J| \geq d_i \text{ and } i \text{ is such that } d_i(C) \geq d_i - \delta\}$$

contains axioms of only those pigeons who are "free enough" in the clause C.

For a clause $C \in P$ we will show, by induction on the number of steps in the derivation of C, that

$$\mathcal{A}_C \models C.$$

This gives the desired contradiction, because $\delta < d_i$ for all i implies that $I_{d,\delta}(0) = \emptyset$; hence, $\mathcal{A}_0 \not\models 0$ because $\mathcal{A}_0 = \emptyset$, implying that $0 \notin P$ (i.e., P is not a refutation of $\mathcal{A}$).

Base case $C \in \mathcal{A}$ is obvious since then $C \in \mathcal{A}_C$.

Inductive step. Suppose that $\mathcal{A}_{C_0} \models C_0$, $\mathcal{A}_{C_1} \models C_1$ and C is obtained from C_0, C_1 by a single application of the monotone refutation rule.

Since the rule is sound on D, $\{C_0, C_1\} \models C$. Hence, if we take

$$I = I_{d,\delta}(C_0) \cup I_{d,\delta}(C_1),$$

then $|I| \leq 2w_0$ and $\mathcal{A}_I \models C$. Let us choose a minimal $I \subseteq \{1, \ldots, m\}$ such that $\mathcal{A}_I \models C$; then still $|I| \leq 2w_0$. We will show that, in fact, $I \subseteq I_{d,\delta}(C)$; this will obviously imply [13] $\mathcal{A}_C \models C$.

Assume the contrary, and pick an arbitrary $i_0 \in I \setminus I_{d,\delta}(C)$. Since I is minimal,

$$\mathcal{A}_{I \setminus \{i_0\}} \not\models C.$$

Hence, there is an assignment $a \in D$ which satisfies all clauses in $\mathcal{A}_{I \setminus \{i_0\}}$ but falsifies C. We may assume that $a_{i,j} = 0$ for all j and all $i \notin I \setminus \{i_0\}$ (because C is positive and none of such variables $x_{i,j}$ appears in $\mathcal{A}_{I \setminus \{i_0\}}$). Let now $J_1 := \{1, \ldots, n\} \setminus J_0$ where[14]

$$J_0 = \bigcup_{i \in I \setminus \{i_0\}} J_i(a) \cup J_{i_0}(C).$$

[11] That is, D is the set of all $m \times n$ matrices with at most ℓ 1's in each row.
[12] No two pigeons are sent by a to the same hole.
[13] Because $\Gamma \models C$ and $\Gamma' \supseteq \Gamma$ implies $\Gamma' \models C$.
[14] Recall that $J_{i_0} = \{j : x_{i_0,j} \in C\}$.

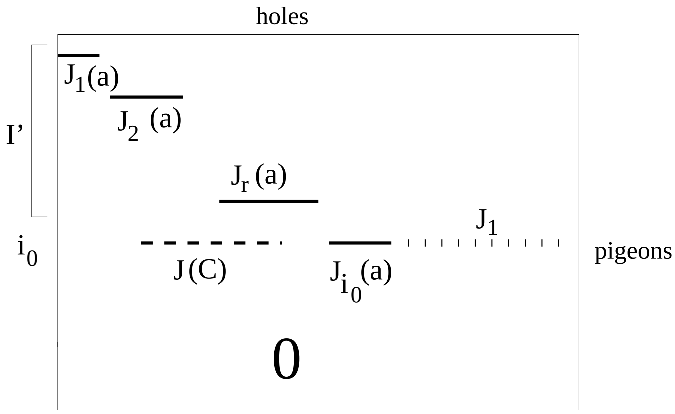

Figure 1. $I = I' \cup \{i_0\}$ with $I' = \{1, \dots, r\}$

Since $i_0 \notin I_{d,\delta}(C)$, we know that $|J_{i_0}(C)| = d_{i_0}(C) < d_{i_0} - \delta$. Hence,

$$|J_1| \geq n - \big(|I| \cdot \ell + |J_{i_0}(C)|\big) \geq n - \big(2w_0\ell + (d_{i_0} - \delta)\big) \geq n - d_{i_0} + \delta/2. \tag{5.11}$$

By its definition, J_1 is the set of holes "permissible" for the pigeon i_0 (see Fig. 1): if we pick an arbitrary ℓ-element subset J of J_1 and change the assignment a by letting $a_{i_0,j} = 1$ iff $j \in J$, then we will get an assignment a' in D which still satisfies all clauses in $\mathcal{A}_{I\setminus\{i_0\}}$ (we have not touched other pigeons) but falsifies C. We want to show that J can be chosen in such a way that this new assignment will also satisfy all clauses in $\mathcal{A}_{i_0}$; this will give the desired contradiction with $\mathcal{A}_I \not\models C$.

For this purpose, pick $\mathbf{J}$ uniformly and at random among all ℓ-element subsets of J_1, and let $\mathbf{a}$ be the random assignment resulting from the assignment a by setting to 1 all $a_{i_0,j}$ with $j \in \mathbf{J}$.

Take an arbitrary axiom $A \in \mathcal{A}_{i_0}$. Since $|J_{i_0}(A)| \geq d_{i_0}$, by (5.11) we have

$$|J_{i_0}(A) \cap J_1| \geq \delta/2.$$

A fixed element appears in $J_{i_0}(A) \cap \mathbf{J}$ with probability

$$p = \frac{|\mathbf{J}|}{|J_1|} \leq \frac{\ell}{n - d_{i_0} + \delta/2}.$$

Hence, applying Chernoff's inequality we obtain

$$\Pr[A(\mathbf{a}) = 1] = \Pr[J_{i_0}(A) \cap \mathbf{J} \neq \emptyset] \geq 1 - e^{-\Omega(p\cdot\delta)} \geq 1 - e^{-\Omega(\delta\ell/n)}.$$

Since

$$\frac{\delta\ell}{n} \geq \frac{\delta^2}{4w_0 n} = \frac{\delta^2}{4n} \cdot \frac{n \cdot \log|\mathcal{A}|}{\varepsilon\delta^2} = \frac{\log|\mathcal{A}|}{4\varepsilon},$$

we obtain that

$$\Pr[A(\mathbf{a}) = 1] \geq 1 - |\mathcal{A}|^{-2},$$

if the constant ε is sufficiently small. Since clearly, $|\mathcal{A}_{i_0}| < |\mathcal{A}_{i_0}|^2 \leq |\mathcal{A}|^2$, this implies that, for at least one choice a' of $\mathbf{a}$, *all* axioms in $\mathcal{A}_{i_0}$ will be satisfied. Since (as we observed above) the assignment a' also satisfies all axioms in $\mathcal{A}_{I\setminus\{i_0\}}$ but falsifies C, we obtained a contradiction with $\mathcal{A}_I \not\models C$.

This completes the proof of Fact 2, and thus, the proof of Theorem 5.6 and Theorem 5.2. $\square$

Final Remark. As we have seen, the whole proof is based on a concept of *pseudo-width* $w_{d,\delta}(P)$ of (monotone) resolution refutation P. This concept (as it was defined) makes sense only for resolution refutations of $\neg PHP_n^m$. On the other hand, one may define the *width* $w(P)$ of a resolution refutation P of an *arbitrary* CNF as the maximum number of literals in a clause from P. Ben-Sasson and Wigderson (1999) established a very general trade-off between the length $|P|$ of P and its width $w(P)$. For a CNF $\mathcal{F}$, let $w(\mathcal{F})$ (resp., $L(\mathcal{F})$) be the minimum width (resp., length) of a resolution refutation of $\mathcal{F}$. Then, for every unsatisfiable CNF $\mathcal{F}$,

$$w(\mathcal{F}) \leq O\left(\sqrt{N \cdot \log L(\mathcal{F})}\right) \qquad (*)$$

where N is the number of variables in $\mathcal{F}$. It is much easier to bound the width $w(\mathcal{F})$ than the length $L(\mathcal{F})$ and, remarkably, Ben-Sasson and Wigderson pointed out that (apparently) *all* lower bounds on $L(\mathcal{F})$ known at that time can be viewed [15] as lower bounds on $w(\mathcal{F})$ followed by applying the inequality (*). Unfortunately, this "width method" seemed to fail for CNFs $\mathcal{F}$ with a huge number of variables N, as is in the case of $\mathcal{F} = \neg PHP_n^m$ where $N = n \cdot m$ and m is much larger than n. To get a super-polynomial lower bound on the length $L(\mathcal{F})$ using (*) we would need a to show that the width $w(\mathcal{F})$ is at least the square root $\sqrt{N}$ of the *total* number of variables $n \cdot m$. Using pseudo-width instead of width for this CNF was crucial: in this case a lower bound for the pseudo-width of oder $n/\log m$ was enough!

5.3. Proof of the pigeon filter lemma

The lemma follows from the following property of randomly chosen numbers (show this!). Let m and L be positive integers. Set $t := \lfloor \log m \rfloor - 1$, and let $\mathbf{r}$ be a random variable taking its values in $\{1, \ldots, t\}$ with probabilities

$$\Pr[\mathbf{r} = t] = \frac{2}{2^t}$$

and

$$\Pr[\mathbf{r} = s] = \frac{1}{2^s} \quad \text{for each} \quad s = 1, 2, \ldots, t-1.$$

Ex. 5.12. Why we cannot take just $\Pr[\mathbf{r} = s] = 2^{-s}$ for *all* $s \leq t$? *Hint*: $\sum_{i=1}^n a^i = (a^{n+1} - a)/(a-1)$.

Lemma 5.13. *Let $x = (x_1, \ldots, x_m)$ be a sequence of integers from $\{1, \ldots, t\}$. Let $\mathbf{r}_1, \ldots, \mathbf{r}_m$ be m independent copies of $\mathbf{r}$. Then, with probability at least $1 - O(L^{-2})$ at least one of the following two events happens:*

(A_x) *$\mathbf{r}_i \geq x_i$ for at least one integer x_i;*

(B_x) *$\mathbf{r}_i < x_i - 1$ for all but at most $O(\log L)$ integers x_i.*

Proof. Our goal is to show that at least one of $\Pr[\neg A_x]$ and $\Pr[\neg B_x]$ is at most $O(L^{-2})$. Define the "weight" of x as $W(x) := \sum_{i=1}^m 2^{-x_i}$. We consider two cases depending on whether $W(x) \leq 2 \ln L$ or not.

Case 1. $W(x) \geq 2 \ln L$.

[15] Note that the proof of Haken's lower bound for $\neg PHP_n^{n+1}$ in the book also follows this frame.

Let $I = \{i : x_i \leq t\}$ and note that $\sum_{i \notin I} 2^{-x_i} \leq m2^{-(t+1)} \leq 2$. Therefore, $\sum_{i \in I} 2^{-x_i} \geq W(x) - 2 \geq 2 \ln L - 2$. On the other hand, for every $i \in I$ we have

$$\Pr[\mathbf{r}_i < x_i] = \sum_{s=1}^{x_i - 1} \Pr[\mathbf{r} = s] = \sum_{s=1}^{x_i - 1} 2^{-s} \leq 1 - 2^{-x_i}.$$

Since the events "$\mathbf{r}_i < x_i$" are independent,[16] and $\Pr[\mathbf{r}_i < x_i] = 1$ for all $i \notin I$, we have that in this case

$$\Pr[\neg A_x] = \Pr[\forall i : \mathbf{r}_i < x_i] = \prod_{i \in I} \left(1 - 2^{-x_i}\right) \leq \exp\left(-\sum_{i \in I} 2^{-x_i}\right) \leq O(L^{-2}).$$

Case 2. $W(x) \leq 2 \ln L$.

We first show that $\Pr[\mathbf{r} \geq x_i - 1] \leq 2^{2-x_i}$ for every i. Indeed, if $x_i > t$ then either $x_i = t + 1$ and $\Pr[\mathbf{r} \geq x_i - 1] = \Pr[\mathbf{r} = t] = 2^{1-t} = 2^{2-x_i}$, or $x_i \geq t + 2$ and $\Pr[\mathbf{r} \geq x_i - 1] = 0$. If $x_i \leq t$ then

$$\Pr[\mathbf{r} \geq x_i - 1] = \sum_{s=x_i-1}^{t} 2^{-s} \leq 2^{1-x_i} \sum_{j=0}^{\infty} 2^{-j} \leq 2^{2-x_i}.$$

Hence, the expected number of i for which $\mathbf{r}_i \geq x_i - 1$ does not exceed

$$\sum_{i=1}^{m} 2^{2-x_i} = 4 \sum_{i=1}^{m} 2^{-x_i} = 4W(x) \leq 8 \ln L.$$

Since these events "$\mathbf{r}_i \geq x_i - 1$" are independent, we may apply Chernoff's inequality and conclude that, for any sufficiently large constant C,

$$\Pr[\neg B_x] = \Pr[|\{i : \mathbf{r}_i \geq x_i - 1\}| \geq C \log L] \leq L^{-2}.$$

$\square$

Let now $R = \{r_{i,k}\}$ be an $m \times L$ matrix with integer entries. If $x = (x_1, \ldots, x_m)$ is a column of R, the say that the (random) sequence $\mathbf{r}_1, \ldots, r_m$ is *bad* for this column if neither of the events A_x and B_x happens. By Lemma 5.13, the sequence is bad for one (fixed) row of R with probability at most $p = O(L^{-2})$. Since we have only L columns, the sequence is good (not bad) for *all* columns with probability at least $1 - L \cdot p = 1 - O(1/L)$. If L is large enough, this probability is nonzero. Hence, there is a particular choice of the sequence $r_1, \ldots, r_n$ which is good for all columns of R.

This completes the proof of Lemma 5.10.

[16] Each r_i is an *independent* copy of $\mathbf{r}$.