Extended Nullstellensatz proof systems

Jan Krajíček

Faculty of Mathematics and Physics
Charles University*

Abstract

For a finite set $\mathcal{F}$ of polynomials from $\mathbf{F}_p[\overline{x}]$ (p is a fixed prime) containing all polynomials $x^2 - x$, a Nullstellensatz proof of the unsolvability of the system

$$f = 0 \ , \quad \text{all } f \in \mathcal{F}$$

in $\mathbf{F}_p$ is an $\mathbf{F}_p[\overline{x}]$-linear combination $\sum_{f \in \mathcal{F}} h_f \cdot f$ that equals to 1 in $\mathbf{F}_p[\overline{x}]$. The measure of complexity of such a proof is its degree: $\max_f deg(h_f f)$.

We study the problem to establish degree lower bounds for some *extended* NS proof systems: these systems prove the unsolvability of $\mathcal{F}$ (in $\mathbf{F}_p$) by proving the unsolvability of a bigger set $\mathcal{F} \cup \mathcal{E}$, where the set $\mathcal{E} \subseteq \mathbf{F}_p[\overline{x}, \overline{r}]$ contains all polynomials $r^p - r$ and satisfies the following soundness condition:

- Any $0,1$-assignment $\overline{a}$ to variables $\overline{x}$ can be appended by an $\mathbf{F}_p$-assignment $\overline{b}$ to variables $\overline{r}$ such that for all $g \in \mathcal{E}$ it holds that $g(\overline{a}, \overline{b}) = 0$.

We define a notion of pseudo-solutions of $\mathcal{F}$ and prove that the existence of pseudo-solutions with suitable parameters implies lower bounds for two extended NS proof systems ENS and UENS defined in [6]. Further we give a combinatorial example of $\mathcal{F}$ and candidate pseudo-solutions based on the pigeonhole principle.

1 Introduction

Let $\mathbf{F}_p$ be the p-element field where p is a fixed prime, and let $\mathbf{F}_p[\overline{x}]$ be the ring of polynomials with variables $\overline{x} = x_1, \dots, x_N$, for some $N \geq 1$. Given a finite set $\mathcal{F} \subseteq \mathbf{F}_p[\overline{x}]$ containing all polynomials $x_i^2 - x_i$, $1 \leq i \leq N$, we consider the question whether the system of polynomial equations

$$f = 0 \ , \quad \text{all } f \in \mathcal{F} \tag{1}$$

has a solution (we shall simply speak about the solvability of $\mathcal{F}$ rather than of (1)). Due to the presence of polynomials $x_i^2 - x_i$ such a solution must be Boolean,

*Sokolovská 83, Prague, 186 75, The Czech Republic, `krajicek@karlin.mff.cuni.cz`

i.e. from $\{0,1\}$. The restriction to Boolean values is due to our primary interest in proof complexity.

In computational and proof complexity we need to represent polynomials as input to algorithms. We shall use dense representation: a list of coefficients from $\mathbf{F}_p$ for all monomials up to the degree of the respective polynomial. Hence a degree d polynomial over N variables is represented by a string of $O(N^d)$ bits. Multiplying or adding polynomials or checking whether two polynomials are identical can be then done by a polynomial time (shortly p-time) algorithm. Note that the bit size of $\mathcal{F}$ is $O(N^d|\mathcal{F}|)$ if d bounds the degree of all polynomials in $\mathcal{F}$.

The problem of solvability of $\mathcal{F}$ in $\mathbf{F}_p$ belongs to the computational complexity class NP. This class can be conveniently defined using the notion of a **proof system**. A language (a set of binary strings) is in NP iff there is a **p-bounded** proof system: a p-time decidable relation $P(x,y)$ (provability relation) and a constant $c \geq 1$ such that for any binary string u:

- $u \in L$ iff $\exists w(|w| \leq |u|^c)\ P(u,w)$.

The existence of such a p-bounded system for the solvability problem is easy to see: w is an assignment to variables and the provability relation P simply says that all polynomials in $\mathcal{F}$ vanish under the assignment. In fact, it is well-known that the problem is equally hard as the Boolean satisfiability problem and hence it is NP-complete.

Our research in this paper is motivated by the fundamental problem of proof complexity whether NP is closed under complementation (the NP vs. coNP problem). By the NP-completeness mentioned above, this problem is thus equivalent to the question whether one can also find a p-bounded proof system for the unsolvability of (1). More precisely, is there a p-time decidable relation $P(x,y)$ and a constant $c \geq 1$ such that for any $\mathcal{F}$:

- $\mathcal{F}$ is unsolvable iff $\exists w(|w| \leq len(\mathcal{F})^c)\ P(\mathcal{F},w)$

where $len(\mathcal{F})$ denotes the bit size of the representation of $\mathcal{F}$.

An example of a proof system (but not p-bounded) for the unsolvability is based on Hilbert's Nullstellensatz and was introduced into proof complexity in [3]. An **NS-refutation** of (the solvability of) a set of polynomials $\mathcal{F}$ with variables $Var(\mathcal{F})$ and containing all polynomials $x^2 - x$ for all $x \in Var(\mathcal{F})$ is a tuple of polynomials $h_f \in \mathbf{F}_p[Var(\mathcal{F})]$, for $f \in \mathcal{F}$, such that

$$\sum_{f \in \mathcal{F}} h_f \cdot f \ = \ 1$$

holds in $\mathbf{F}_p[Var(\mathcal{F})]$. The **degree of the refutation** is

$$\max_{f \in \mathcal{F}} deg(h_f f)\ .$$

It turns out that in natural situations the degree is the main measure we should care for. Namely, in order to show some asymptotic lower bound it often suffices to consider finite sets of polynomials $\mathcal{F}_n$ over $\mathbf{F}_p$ containing the polynomials $x^2 - x$ for $x \in Var(\mathcal{F}_n)$ such that for some constant $c \geq 1$ and all $n \geq 1$:

$$|\mathcal{F}_n| \leq n^c \ , \ N := |Var(\mathcal{F}_n)| \leq n^c \ \text{ and } \ \max\{deg(f) \mid f \in \mathcal{F}_n\} \leq c \ . \qquad (2)$$

A degree d NS-refutation of $\mathcal{F}_n$ has thus bit size $O(|\mathcal{F}_n|N^d) = O(n^{2c+d})$ which is polynomial in the bit size $len(\mathcal{F}_n) = O(n^{3c})$ of $\mathcal{F}_n$ iff d is bounded by a constant. In other words, to show that the NS proof system is not p-bounded one needs a non-constant lower bound for d as n grows[1]. Such lower bounds are actually known, cf. [3, 6] and references therein.

In this paper we study **extended** NS proof systems which are stronger than the NS proof system. The general idea of these proof systems is the following. Before looking for an NS refutation of $\mathcal{F} \subseteq \mathbf{F}_p[\overline{x}]$ extend it by a finite set $\mathcal{E} \subseteq \mathbf{F}_p[\overline{x}, \overline{r}]$ of polynomials (to be called extension polynomials) in possibly more variables (to be called extension variables) than those of $\mathcal{F}$, containing polynomials $r^p - r$ for all new variables r, and having the following **soundness property**:

- Any $0, 1$ assignment $\overline{a}$ to variables $\overline{x}$ can be appended by an $\mathbf{F}_p$-assignment $\overline{b}$ to variables $\overline{r}$ such that for all $g \in \mathcal{E}$ it holds that $g(\overline{a}, \overline{b}) = 0$.

Then find an NS-refutation of $\mathcal{F} \cup \mathcal{E}$. Such proof may allow for a smaller degree than a mere NS refutation of $\mathcal{F}$. However, a subtle point is that to make it a proof system one has to be able to check the soundness property of $\mathcal{E}$ in p-time. This is a non-trivial requirement and for the two extended NS systems we consider in Section 2 this is enforced by syntactic requirements on sets $\mathcal{E}$.

In Section 3 we define a notion of pseudo-solutions of $\mathcal{F}$ and prove that the existence of pseudo-solutions with suitable parameters implies lower bounds for two extended NS proof systems ENS and UENS defined in [6]. In Section 4 we give a combinatorial example of $\mathcal{F}$ and candidate pseudo-solutions based on the pigeonhole principle. In Section 5 we discuss a motivation for extended NS proof systems coming originally from logic (proof complexity). The reader can find more proof complexity background in [11, 6].

A convention: all logarithms are base 2.

2 Proof systems ENS and UENS

Both examples of extended NS proof systems in this section, to be denoted ENS and UENS, are from [6].

Definition 2.1 ([6])

[1] For some other questions in proof complexity stronger lower bounds are needed, e.g. of the form $(\log n)^{\omega(1)}$ or even $n^{\Omega(1)}$.

1. *Let $\overline{g} = g_1, \ldots, g_m$ be polynomials in any variables over $\mathbf{F}_p$ and let $h \geq 1$ be a parameter. For $i \leq m$ define polynomials:*

$$E_{i,\overline{g}} \ := \ g_i \cdot \Pi_{u \leq h}(1 - \sum_{j \leq m} r_{uj} g_j) \qquad (3)$$

where r_{uj} are new **extension variables** *common to all $i \leq m$. The polynomials $E_{i,\overline{g}}$ are called the* **extension polynomials of accuracy** *h corresponding to $\overline{g}$.*

2. *A set $\mathcal{E}$ of extension polynomials can be* **stratified into ℓ levels** *iff $\mathcal{E}$ can be partitioned as $\mathcal{E}_1 \cup \ldots \cup \mathcal{E}_\ell$ where:*

   - *If $E_{i,\overline{g}} \in \mathcal{E}_t$, some t and i, then also all companion polynomials $E_{j,\overline{g}}$ are in $\mathcal{E}_t$, all $j \leq m$.*
   - *Variables in the polynomials g_j in $E_{i,\overline{g}}$ in $\mathcal{E}_1$ are among $Var(\mathcal{F}_n)$ and no extension variable from $E_{i,\overline{g}}$ occurs among $Var(\mathcal{F}_n)$ or in other extension polynomials in $\mathcal{E}_1$ except in the companion polynomials.*
   - *Variables in the polynomials g_j in the axioms $E_{i,\overline{g}}$ in $\mathcal{E}_{t+1}$, $1 \leq t < \ell$, are among the variables occurring in $Var(\mathcal{F}_n \cup \bigcup_{s \leq t} \mathcal{E}_s)$ (including the extension variables from these levels) and no extension variable from $E_{i,\overline{g}}$ does occur among them or in other extension polynomials in $\mathcal{E}_{t+1}$ except in the companion polynomials.*

3. *For a set $\mathcal{E}$ of extension polynomials put*

   - *$\mathcal{R}(\mathcal{E})$ to be the set of polynomials $r^p - r$, for all extension variables r occurring in $\mathcal{E}$.*

An **ENS-refutation** of $\mathcal{F}$ consists of a triple $(h, \mathcal{E}, L)$, where $h \geq 1$ is its accuracy, $\mathcal{E}$ is a set satisfying Definition 2.1 and L is an NS-refutation of $\mathcal{F} \cup \mathcal{E} \cup \mathcal{R}(\mathcal{E})$. Its degree is the degree of L.

Lemma 2.2 *If $\mathcal{F}$ has an ENS-refutation of any level $\ell \geq 1$ and any accuracy $h \geq 1$ then it is unsolvable.*

Proof :

Let $\overline{a}$ be an assignment to variables $\overline{x}$. Take any extension polynomial $E_{i,\overline{g}}$ in the first of $\mathcal{E}$ and its factor $(1 - \sum_{j \leq m} r_{1j} g_j)$. If all g_j vanish under $\overline{a}$ put $r_{1j} := 0$. If some g_j does not vanish, put $r_{1j'} := 0$ for $j' \neq j$ and $r_{1j} := g_j(\overline{a})^{-1}$. Further put $r_{ij} := 0$ for all $i > 1$ and any j.

This evaluation will also kill all companion polynomials $E_{i,\overline{g}}$, all i. After you treat analogously other first level extension polynomials, move to the second level, etc. Finally note that polynomials in $\mathcal{R}(\mathcal{E})$ vanish for any $\overline{b}$.

q.e.d.

Extension polynomials were introduced in [6] so that the proof system can simulate in a sense Boolean combinations of equations. Namely, assuming that the equations $E_{i,\overline{g}} = 0$ hold for all $i \leq m$, we can express the truth value of the disjunction

$$\bigvee_{i \leq m} (g_i \neq 0)$$

by a polynomial

$$\mathsf{disj}_{\overline{g}} \ := \ 1 \ - \ \Pi_{u \leq h}(1 - \sum_{j \leq m} r_{uj} g_j)$$

of degree $h(1 + \max_i(deg(g_i))$ which may be much smaller, if h is small, than $(p-1)\sum_j deg(g_i)$ required by the obvious definition $1 - \Pi_i(1 - g_i^{p-1})$. Clearly if all $g_j = 0$ also $\mathsf{disj}_{\overline{g}} = 0$ and if $g_i \neq 0$ for some i then, by $E_{i,\overline{g}} = 0$, $\mathsf{disj}_{\overline{g}} = 1$. We shall discuss the motivation for introducing ENS in more detail in Section 5.

Extension polynomials can be also introduced in an unstructured form. A motivation for this construction in [6] came from Boolean complexity.

Definition 2.3 ([6]) *An unstructured extension polynomial of accuracy $h \geq 1$ is any polynomial from $\mathbf{F}_p[\overline{x}, \overline{r}]$ of the form*

$$(g_1 - r_1) \cdot \ldots \cdot (g_h - r_h)$$

where no r_i occurs in any g_j (but may occur in other such unstructured extension polynomials in $\mathcal{E}$).

Lemma 2.4 *Let $h \geq 1$ and let $\mathcal{E}$ be a set of unstructured extension polynomials of accuracy h such that $|\mathcal{E}| < e^{h/p}$. Assume that $\mathcal{F} \cup \mathcal{E} \cup \mathcal{R}(\mathcal{E})$ has an NS-refutation. Then $\mathcal{F}$ is unsolvable.*

Proof :

For a given assignment $\overline{a}$ to variables $\overline{x}$ choose an assignment $\overline{b}$ to $\overline{r}$ uniformly at random from all $\mathbf{F}_p$-assignments. The probability that one extension polynomial $(g_1 - r_1) \cdot \ldots \cdot (g_h - r_h)$ does not vanish under $\overline{a}, \overline{b}$ is at most $(1 - 1/p)^h < e^{-h/p}$. Using the hypothesis that $|\mathcal{E}| < e^{h/p}$ it follows by averaging that there is some $\overline{b}$ such that all polynomials in $\mathcal{E}$ vanish under $\overline{a}, \overline{b}$. Finally note that polynomials in $\mathcal{R}(\mathcal{E})$ vanish for any $\overline{b}$.

q.e.d.

We can use this lemma to define a sound proof system: a **UENS-refutation** of $\mathcal{F} \subseteq \mathbf{F}_p[\overline{x}]$ is a triple $(h, \mathcal{E}, L)$, where $h \geq 1$ is its accuracy, $\mathcal{E}$ is a set satisfying satisfying Definition 2.3 and also the size condition $|\mathcal{E}| < e^{h/p}$, and L is an NS-refutation of $\mathcal{F} \cup \mathcal{E} \cup \mathcal{R}(\mathcal{E})$. Its degree is the degree of L.

UENS is at least as strong as ENS in the sense of the following statement.

Lemma 2.5 ([6, Thm.6.14(1)]) *For every extension polynomial $E_{i,\overline{g}}$ of accuracy $h \geq 1$ from Definition 2.1 there exists an unstructured extension polynomial $E'_{i,\overline{g}}$ of the same accuracy, such that $E_{i,\overline{g}}$ can be expressed in $\mathbf{F}_p[\overline{x}, \overline{r}]$ as a linear combination of polynomials from the set $E'_{i,\overline{g}}$, $x^2 - x$ for all x and $r^p - r$ for all r. of degree at most $(ph+1) \cdot \max_j deg(g_j) + h$.*

Noting that the maximum degree of $E_{i,\overline{g}}$ for $j \leq m$ is $h(1 + \max_j deg(g_j)) + \max_j deg(g_j)$ we get the following.

Corollary 2.6 *Assume that there is an ENS-refutation $h, \mathcal{E}, L$ of $\mathcal{F}$ of degree d. Then there is an UENS-refutation $h, \mathcal{E}', L'$ of $\mathcal{F}$ of degree $O(pd)$.*

3 Pseudo-solutions

For $d \geq 0$ let $\mathbf{F}_p{}^{\leq d}[\overline{x}]$ be the $\mathbf{F}_p$-vector space of polynomials from $\mathbf{F}_p[\overline{x}]$ of degree at most d. We consider finite sets of polynomials $\mathcal{F}_n$ over $\mathbf{F}_p$ in variables forming the set $Var(\mathcal{F}_n)$, containing for each $x \in Var(\mathcal{F}_n)$ the polynomial $x^2 - x$, and such that for some constant $c \geq 1$ conditions (2) are satisfied for $n \geq 1$. We shall denote variables in $Var(\mathcal{F}_n)$ simply $\overline{x}$.

A **degree** d $\mathcal{F}_n$**-design** is any map

$$\omega \ : \ \mathbf{F}_p{}^{\leq d}[\overline{x}] \rightarrow \mathbf{F}_p$$

satisfying the following three conditions:

1. For all $a \in \mathbf{F}_p$: $\omega(a) = a$.
2. For all $g, h \in \mathbf{F}_p{}^{\leq d}[\overline{x}]$:
$$\omega(g) + \omega(h) = \omega(g + h) \ .$$
3. For any two polynomials $f \in \mathcal{F}_n$ and $g \in \mathbf{F}_p{}^{\leq d}[\overline{x}]$, if $deg(fg) \leq d$ then:
$$\omega(fg) = 0 \ .$$

This notion was defined by P. Pudlák in an informal electronic Prague-San Diego seminar that run in early 1990s and it was used first in [3] to establish the non-existence of constant degree NS-proofs of one modular counting principle from another, cf. also [11, Sec.16.1] for an exposition of this and subsequent results.

An $\mathbf{F}_p{}^{\leq d}[\overline{x}]$**-tree** T is a finite p-ary tree whose each inner node (i.e. a non-leaf) is labeled by a query $g = ?$ for some polynomial $g \in \mathbf{F}_p{}^{\leq d}[\overline{x}]$ and the p outgoing edges are labeled by $g = a$, for all $a \in \mathbf{F}_p$. The leaves are labeled by elements of some set $I \neq \emptyset$. The **height of** T is the maximum number of edges on a path from the root to a leaf. An $\mathbf{F}_p{}^{\leq d}[\overline{x}]$-tree of height $\leq e$ will be abbreviated as (d, e)**-tree**.

Let T be an $\mathbf{F}_p{}^{\leq d}[\overline{x}]$-tree whose leaves are labeled by elements of a non-empty set I. The tree T and any map $\omega : \mathbf{F}_p{}^{\leq d}[\overline{x}] \rightarrow \mathbf{F}_p$ define a path in T as follows: start at the root and answer the queries by ω. The label of a leaf the path so defined reaches will be denoted $T(\omega)$. In particular, T defines a map from the set of all degree d $\mathcal{F}_n$-designs to I.

We shall consider systems $\mathcal{F}_n$ that have no solution in $\mathbf{F}_p$. This means that no degree d $\mathcal{F}_n$-design ω can be a homomorphism and there must be **conflict pairs** of polynomials $g, g' \in {\mathbf{F}_p}^{\leq d}[\overline{x}]$, such that $deg(gg') \leq d$ and

$$\omega(g) \cdot \omega(g') \neq \omega(gg') \ .$$

The following notion was inspired by the model-theoretic construction in [9, Cht.22] (it corresponds to the notion of sample space there).

Definition 3.1 (pseudo-solutions)

*For any $d, e \geq 0$ and $1 \geq \gamma \geq 0$, a (d, e, γ)-**solution** of $\mathcal{F}_n$ is a non-empty finite set Ω of degree d $\mathcal{F}_n$-designs ω such that for any (d, e)-tree T:*

$$Prob_{\omega \in \Omega}[T(\omega) \text{ is } \textbf{not} \text{ a conflict pair for } \omega\ ] \geq \gamma \ .$$

*A **pseudo-solution** is a collective name for (d, e, γ)-solutions.*

Theorem 3.2 *Let $(h, \mathcal{E}, L)$ be an ENS- or UENS-refutation of $\mathcal{F}$ of degree d. Let $S := |\mathcal{E}|$ and assume $e^{h/p} \geq 2S^2$. Then there is no $(d, h + \log S, S^{-1})$ pseudo-solution of $\mathcal{F}$.*

In particular, if h is minimal such that $e^{h/p} \geq S^2$ holds then there is no $(d, (2p + 1) \log S, S^{-1})$ pseudo-solution of $\mathcal{F}$.

The proof is summarized at the end of the section after establishing some lemmas.

Utilizing Corollary 2.6 we could prove the theorem only for UENS. However, because of the importance of ENS for the logic problem discussed in Section 5 we shall formulate the proof directly for ENS and avoid the detour via UENS; the argument can be easily modified for UENS. The idea is to transform in a sense the averaging argument for Lemma 2.4 to the setting where we have $\mathbf{F}_p$-linear maps $\omega : {\mathbf{F}_p}^{\leq d}[\overline{x}] \to \mathbf{F}_p$ instead of evaluation of variables by elements of $\mathbf{F}_p$.

For $E_{i,\overline{g}}$ as in (3), any of the $h + 1$ polynomials

$$g_i \ \text{ and } \ 1 - \sum_{j \leq m} r_{uj} g_j \ , \quad \text{for} \quad u \leq h \tag{4}$$

will be called a **factor polynomial of $E_{i,\overline{g}}$**.

Lemma 3.3

Assume that Ω is a finite non-empty set of $\mathbf{F}_p$-linear maps from ${\mathbf{F}_p}^{\leq d}[\overline{x}]$ to $\mathbf{F}_p$. Let $\overline{g} = g_1, \ldots, g_m$ be polynomials in variables $\overline{x}$ and let $E_{i,\overline{g}}$, $i \leq m$, be the companion extension polynomials of accuracy $h \geq 1$ using extension variables r_{uj} as in (3). Assume that all $E_{i,\overline{g}}$ have degree $\leq d$.

Then for any $\omega \in \Omega$ and any $i \leq m$, the probability over uniform random choices $\overline{b}$ that

$$\omega(g'(\overline{x}, \overline{b})) \neq 0$$

holds for all factor polynomials $g'(\overline{x}, \overline{r})$ of $E_{i,\overline{g}}$ is at most $e^{-h/p}$.

Proof :

Let ω and $i \leq m$ be fixed and fix at random all b_{uj} with $u \leq h$ and $j \neq i$. Assume $\omega(g_i) \neq 0$.

Think of the remaining h values b_{ui}, $u \leq h$, as being chosen from $\mathbf{F}_p$ uniformly and independently at random. Using the $\mathbf{F}_p$-linearity of ω we see that the probability to satisfy the inequality

$$\omega(\sum_{j \leq m, j \neq i} b_{uj} g_j) + b_{ui}\omega(g_i) \neq 1 \ .$$

for one $u \leq h$ is $\frac{p-1}{p}$. Hence we fail to violate it for all $u \leq h$ with the probability at most $(1 - \frac{1}{p})^h \leq e^{-h/p}$.

q.e.d.

Having Lemma 3.3 we may now proceed as level by level, bottom up, to find a suitable assignment of values from $\mathbf{F}_p$ to all extension variables in $\mathcal{E}$. In particular, take one block of m companion extension polynomials in $\mathcal{E}_1$ and choose (by an averaging argument) a suitable assignment to its extensions variables such that some of them fails to contain a factor polynomial that vanishes for at most a fraction of $m \cdot e^{-h/p}$ of all ω, and substitute it in the whole of $\mathcal{E}$. Then do the same consecutively for all blocks of companion polynomials in the first level. We lose altogether at most $|\mathcal{E}_1| \cdot e^{-h/p}$ elements ω. After we have substituted values from $\mathbf{F}_p$ for all extension variables occurring in the first level, all polynomials g_i in the second level $\mathcal{E}_2$ have only variables $\overline{x}$ left. Hence we can repeat the process. This yields the following statement.

Lemma 3.4

Assume that Ω is a finite non-empty set of $\mathbf{F}_p$-linear maps from ${\mathbf{F}_p}^{\leq d}[\overline{x}]$ to $\mathbf{F}_p$. Let $\mathcal{E}$ be a leveled set of extension polynomials of accuracy h of the form as in Def.2.1, all of degree at most d.

Then there is an evaluation $\overline{r} := \overline{b}$ of the extension variables in $\mathcal{E}$ by values from $\mathbf{F}_p$ such that for all $\omega \in \Omega$ but a fraction of $|\mathcal{E}|e^{-h/p}$ it holds that

- *each extension polynomial in $\mathcal{E}$ has a factor polynomial $g'(\overline{x}, \overline{r})$ such that*

$$\omega(g'(\overline{x}, \overline{b})) = 0 \ .$$

Now we are ready for **Proof of Theorem 3.2**. Assume that $\mathcal{F}_n$ has an ENS-refutation $(h, \mathcal{E}, L)$ of degree d and that $2S^2 \leq e^{h/p}$ holds where $S := |\mathcal{E}|$. Hence:

$$|\mathcal{E}|e^{-h/p} \leq 1/(2S) \tag{5}$$

Note that, in particular, if h was minimal to satisfy (5) then

$$h = O(\log S) \ . \qquad (6)$$

Let L:

$$1 \ = \ \sum_{f \in \mathcal{F}_n} h_f f \ + \ \sum_{E \in \mathcal{E}} p_E E \ + \ \sum_{g \in \mathcal{R}(\mathcal{E})} q_g \cdot g$$

be some NS-refutation of $\mathcal{F}_n \cup \mathcal{E} \cup \mathcal{R}(\mathcal{E})$ of degree d.

Assume that Ω is a $(d, h + \log S, S^{-1})$-solution of $\mathcal{F}_n$. Substitute for all extension variables in $\mathcal{E}$ an evaluation $\bar{b}$ by elements of $\mathbf{F}_p$ with the property stated in Lemma 3.4. In particular, after the substitution let Ω_0 be the part of Ω consisting of ω satisfying the property in that lemma. Note that by the choice of h

$$|\Omega_0| \ \geq (1 - 1/(2S)) \cdot |\Omega| \ . \qquad (7)$$

All polynomials $g \in \mathcal{R}(\mathcal{E})$ vanish after the substitution and because maps $\omega \in \Omega$ are designs also $\omega(\sum_{f \in \mathcal{F}_n} h_f(\bar{b}) f) = 0$ holds. Hence we have that

$$1 \ = \ \omega(\sum_{E \in \mathcal{E}} p_E(\bar{b}) E(\bar{b})) \qquad (8)$$

where the polynomials $p_E(\bar{b}), E(\bar{b})$ have variables left only from $Var(\mathcal{F}_n)$.

We shall construct in two steps a particular (d, e)-tree T^*:

1. Use binary search to the sum in the right-hand side of (8) to get a $(d, \log S)$-tree T_1 that finds, for any $\omega \in \Omega$ a term $p_E E$ in the sum which is of the form $E = E_{i,\bar{g}}$ and $\omega(p_E E) \neq 0$.
2. To get T^* extend T_1 as follows. At leaves labeled by $p_E E$ with $E = E_{i,\bar{g}}$, ask for values of all factor polynomials $1 - \sum_{j \leq m} r_{uj} g_j$ for $u \leq h$. By the choice of Ω_0, if $\omega \in \Omega_0$, at least one gets by ω value 0. Hence we can write $p_E E$ as a product $g' g''$ with $\omega(g' g'') \neq 0 \wedge \omega(g') = 0$. Label the corresponding leaf by (g', g'').

Note that the height e of T^* is $h + \log S$ and that for all $\omega \in \Omega_0$ it holds that $T^*(\omega)$ is a conflict pair for ω.

By the definition of pseudo-solutions we have that $T^*(\omega)$ can be a conflict pair for at most $(1 - 1/S)$-part of Ω but Ω_0 is bigger. This is a contradiction and Theorem 3.2 is proved.

q.e.d.

The relevance of the following problem is described in Section 5.

Problem 3.5 *Construct families $\mathcal{F}_n$ (containing all polynomials $x^2 - x$ and obeying (2) for some constant $c \geq 1$) and for any constant $r \geq 1$ and $n >> 1$ an $((\log n)^r, r \log n, n^{-r})$ pseudo-solution of $\mathcal{F}_n$.*

4 A combinatorial example

The propositional formula PHP_n:

$$\bigvee_i \bigwedge_j \neg p_{ij} \;\vee\; \bigvee_{i_1 \neq i_2, j} (p_{i_1 j} \wedge p_{i_2 j}) \;\vee\; \bigwedge_{i, j_1 \neq j_2} (p_{ij_1} \wedge p_{ij_2})$$

with i, i_1, i_2 ranging over $[n+1] = \{1, \ldots, n+1\}$ and j, j_1, j_2 over $[n]$ is the most famous tautology in proof complexity, introduced by Cook and Reckhow [7]. If it would be falsified by some evaluation $p_{ij} := a_{ij} \in \{0, 1\}$ then the set of all pairs (i, j) such that $a_{ij} = 1$ would be the graph of an injective function from $[n+1]$ into $[n]$. Hence the fact that PHP_n is logically valid is equivalent to the pigeonhole principle.

The formula PHP_n requires long proofs in a number of proof systems and its advanced variants may be hard for all proof systems (cf. [9, Chpts.29-30] or [11, Chpt.19]). It has a polynomial size (measured in its size $O(n^3)$) proof in the ordinary propositional calculus using the DeMorgan language and based on a finite number of axiom schemes and schematic inference rules, a Frege system in the established terminology of [7]; this was proved by Buss [4]. In fact, it has a simple polynomial size proof in a TC^0-Frege system, a proof system operating with bounded depth formulas using also the threshold connectives, and Buss's argument shows that Frege systems do p-simulate these systems when such a connective is defined by a suitable DeMorgan formula. One of the crucial results in proof complexity is Ajtai's theorem [1] that proofs of PHP_n in AC^0-Frege systems, subsystems of Frege systems operating with DeMorgan formulas of a bounded depth, require super-polynomial number of steps (this was later improved to an exponential lower bound in [12, 13]).

The negation of PHP_n can be reformulated (following [3]) as the following unsolvable system $\neg\mathcal{PHP}_n$ of polynomial equations over $\mathbf{F}_p$ in variables x_{ij}, $i \in [n+1], j \in [n]$:

- $x_{i_1 j} \cdot x_{i_2 j} = 0$, for each $i_1 \neq i_2 \in [n+1]$ and $j \in [n]$.
- $x_{ij_1} \cdot x_{ij_2} = 0$, for each $i \in [n+1]$ and $j_1 \neq j_2 \in [n]$.
- $1 - \sum_{j \in [n]} x_{ij} = 0$, for each $i \in [n+1]$.
- $x_{ij}^2 - x_{ij}$, for all $i \in [n+1], j \in [n]$.

The left-hand sides of the equations in the first three items will be denoted $Q_{i_1,i_2;j}$, $Q_{i;j_1,j_2}$ and Q_i, respectively. We included the polynomials $x_{ij}^2 - x_{ij}$ in $\neg\mathcal{PHP}_n$ to conform with the requirement put on systems $\mathcal{F}_n$ but it is easy to see that they are simple linear combinations of the other polynomials:

$$x_{ij}^2 - x_{ij} \;=\; \sum_{k \in [n], k \neq j} Q_{i;j,k} \;-\; x_{ij} Q_i .$$

NS-refutations of $\neg\mathcal{PHP}_n$ need degree $n/2$ and that implies the following well-known fact.

Lemma 4.1 ([14, 5, 2]) *For $n \geq 2$ there are degree $n/2$ $\neg\mathcal{PHP}_n$-designs (over any $\mathbf{F}_p$).*

For a partial injective map $\rho :\subseteq [n+1] \to [n]$ define the **restriction** of a polynomial g over $Var(\neg\mathcal{PHP}_n)$ to be the polynomial to be denoted g^ρ resulting from g by the following partial substitution of $0/1$ values for some variables:

$$x_{ij}^\rho = \begin{cases} 1 & \text{if } i \in dom(\rho) \wedge \rho(i) = j \\ 0 & \text{if } i \in dom(\rho) \wedge \rho(i) \neq j \\ 0 & \text{if } j \in rng(\rho) \wedge \rho^{(-1)}(j) \neq i \\ x_{ij} & \text{otherwise} \end{cases}$$

Further define $D^\rho := [n+1] \setminus dom(\rho)$, $R^\rho := [n] \setminus rng(\rho)$ and $n_\rho := |R^\rho| (= n - |\rho|)$. Note that $x_{ij}^\rho = x_{ij}$ iff $(i,j) \in D^\rho \times R^\rho$.

If we apply a restriction ρ to all polynomials in $\neg\mathcal{PHP}_n$ we get a set $(\neg\mathcal{PHP}_n)^\rho$ of polynomials that expresses $\neg$PHP over D^ρ and R^ρ (plus the zero polynomial) and that is isomorphic to $\neg\mathcal{PHP}_{n_\rho}$. In particular, by Lemma 4.1 there are degree $n_\rho/2$ designs for $(\neg\mathcal{PHP}_n)^\rho$.

Definition 4.2 *For $n \geq 1$ and $\epsilon > 0$ such that $n^\epsilon \geq 1$ let $\Omega_{n,\epsilon}$ be the set of all $\neg\mathcal{PHP}_n$-designs ω that are defined as follows:*

1. *Pick*
   - *(a) a restriction $\rho :\subseteq [n+1] \to [n]$ with $n_\rho = n^\epsilon$,*
   - *(b) a degree $n_\rho/2$-design L for $(\neg\mathcal{PHP}_n)^\rho$.*
2. *For $g \in \mathbf{F}_p{}^{\leq d}[Var(\neg\mathcal{PHP}_n)]$ put:*

$$\omega(g) \; := \; L(g^\rho) \; .$$

We shall write $\omega = (\rho_\omega, L_\omega)$ with ρ_ω and L_ω denoting the respective ρ and L defining ω.

The next lemma interprets the task to find conflict pairs over $\Omega_{n,\epsilon}$ more combinatorially.

Lemma 4.3 *Let T be a (d,e)-tree over $\mathbf{F}_p{}^{\leq d}[Var(\neg\mathcal{PHP}_n)]$. Then there is (d,e')-tree T' with $e' \leq e + O(d \log n)$ such that for any $\omega = (\rho_\omega, L_\omega) \in \Omega_{n,\epsilon}$ if $T(\omega)$ is a conflict pair for ω then $T'(\omega)$ is a pair $(i,j) \in D^\rho \times R^\rho$.*

Proof :

Assume T found a conflict pair g, g' for ω. Write g as an $\mathbf{F}_p$-linear combination of monomials ($\leq n^{O(d)}$ of them) and use binary search to find one monomial u such that

$$\omega(u \cdot g') \neq \omega(u) \cdot \omega(g') \; .$$

If u is a product of variables $x_{i_1 j_1} \cdot \ldots \cdot x_{i_t j_t}$ then by at most $2t \leq 2d$ questions about values of

$$x_{i_s j_s} \;\text{ and }\; x_{i_1 j_1} \cdot \ldots \cdot x_{i_s j_s} \cdot g'$$

for $s = 1, \ldots, t$ we find one variable $x_{i_s j_s}$ such that

$$\omega(x_{i_s j_s}) \cdot \omega(x_{i_1 j_1} \cdot \ldots \cdot x_{i_{s-1} j_{s-1}} \cdot g') \neq \omega(x_{i_1 j_1} \cdot \ldots \cdot x_{i_s j_s} \cdot g') \ .$$

By the definition of restrictions this means that $x^{\rho}_{i_s j_s} = x_{i_s j_s}$. That is

$$(i_s, j_s) \in D^{\rho} \times R^{\rho} \ .$$

q.e.d.

Problem 4.4 *Do families $\neg\mathcal{PHP}_n$ and sets $\Omega_{n,\epsilon}$ for some fixed $\epsilon > 0$ solve Problem 3.5?*

Are $\Omega_{n,\epsilon}$, in fact, $(n^{\Omega(1)}, n^{\Omega(1)}, 2^{-n^{\Omega(1)}})$ pseudo-solutions of $\neg\mathcal{PHP}_n$, ?

5 Proof complexity motivation for ENS

The problem to extend the lower bound for PHP_n, or for any other formula for that matter, from AC^0-Frege systems to $\mathrm{AC}^0[p]$-Frege systems operating with formulas of a bounded depth in the DeMorgan language augmented by connectives counting modulo p, p a prime, received a considerable attention over the last three decades. Proof-theoretically the most elegant definition of AC^0 proof systems is using the formalism of sequent calculus LK (cf. [8, 11]) but we shall stick to Frege systems: we will refer to a result from [6] and that used Frege systems. It is well known that the two formalisms yield equivalent subsystems, except possibly for a change in the depth by an additive constant (cf. [11, Chpt.3]).

Let F be any Frege system in the DeMorgan language $0, 1, \neg, \vee, \wedge$. We shall denote by $F(\mathrm{MOD}_p)$ the proof system whose language extends the DeMorgan one by unbounded arity connectives $\mathrm{MOD}_{p,i}$ for p a prime and $i = 0, \ldots, p-1$. The formula $\mathrm{MOD}_{p,i}(y_1, \ldots, y_k)$ is true iff $\sum_j y_j \equiv i \pmod p$. The proof system has all Frege rules of F accepted for all formulas of the extended language and, in addition, the following set of MOD_p-axioms (cf. [8, Sec.12.6]):

- $\mathrm{MOD}_{p,0}(\emptyset)$
- $\neg\mathrm{MOD}_{p,i}(\emptyset)$, for $i = 1, \ldots, p-1$
- $\mathrm{MOD}_{p,i}(\Gamma, \phi) \ \equiv \ [(\mathrm{MOD}_{p,i}(\Gamma) \wedge \neg\phi) \vee (\mathrm{MOD}_{p,i-1}(\Gamma) \wedge \phi)]$

  for $i = 0, \ldots, p-1$, where $0 - 1$ means $p - 1$ and where Γ stands for any sequence (possibly empty) of formulas.

The **depth** of a constant or of an atom is 0, the use of the negation or of any of $\mathrm{MOD}_{p,i}$ increases the depth by 1, and a formula formed from formulas A_i none of which starts with $\vee$ (resp. with $\wedge$) by a repeated use of $\vee$ (resp. of $\wedge$) has the depth 1 plus the maximum depth of formulas A_i. In particular, the depth of PHP_n is 3. The subsystem of $F(\mathrm{MOD}_p)$ allowed to use only formulas of depth at most ℓ will be denoted by $F_{\ell}(\mathrm{MOD}_p)$.

Any polynomial equation $f = 0$ over $\mathbf{F}_p$ is, in particular, also a depth 2 formula in the language of $F(\mathrm{MOD}_p)$: monomials in f can be defined by conjunctions and $f = 0$ is expressed using $\mathrm{MOD}_{p,0}$ applied to them. Therefore we can talk about $F(\mathrm{MOD}_p)$-refutations of $\mathcal{F}_n$. The following lemma is straightforward (cf. also [3]).

Lemma 5.1 *The two formulations $\neg PHP_n$ and $\neg \mathcal{PHP}_n$ can be derived form each other in $F_4(MOD_p)$ by proofs of size $n^{O(1)}$.*

Having an $F_\ell(\mathrm{MOD}_p)$-proof we can translate it into a proof using only low degree polynomials; first define big conjunctions $\bigwedge$ via big disjunctions $\bigvee$ and $\neg$, and then translate bottom up all $\bigvee$ by disj as described after Lemma 2.2, while systematically introducing all needed extension polynomials. This yields the following result.

Theorem 5.2 ([6, Thm.6.7(1)])

Let $\ell \geq 2$ be a constant. Let $\mathcal{F}_n$ be a set of polynomials obeying (2) and containing all polynomials $x^2 - x$ for all $x \in Var(\mathcal{F}_n)$, and assume it has an $F_\ell(MOD_p)$-refutation with k steps. Let $h \geq 1$ be any parameter.

Then for any $h \geq 1$ there exists a set $\mathcal{E}$ of $S := k^{O(1)}$ extension polynomials of accuracy h stratified into $\ell + O(1)$ levels such that $\mathcal{F}_n \cup \mathcal{E} \cup \mathcal{R}(\mathcal{E})$ has an NS-refutation of degree at most

$$(O(1) + \log k)(h + 1)^{O(1)} \ . \qquad (9)$$

(The constant $O(1)$ in term $k^{O(1)}$ and the additive constant $O(1)$ depend on the underlying Frege system F only but the $O(1)$ in the exponent in (9) depends also on ℓ: the construction underlying the proof in [6] yields the bound $O(\ell)$.)

Should there be refutations of $\mathcal{F}_n$ in any $F_\ell(\mathrm{MOD}_p)$, fixed $\ell \geq 2$, with $k = n^{O(1)}$ steps, we can choose minimal $h \geq 1$ such that $e^{h/p} \geq 2S^2$, S provided by Theorem 5.2. Such h is $O(\log n)$ and hence we would get ENS-refutations $(h, \mathcal{E}, L)$ of degree

$$d \leq (O(1) + \log k)(h + 1)^{O(1)} \leq (\log n)^c$$

where c depends on ℓ. This connection[2] to ENS, and Theorem 3.2 , is the reason why we are interested in Problem 2.2.

Note that should it be answered by $\neg \mathcal{PHP}_n$ (Problem 4.4) it would imply also a lower bound for UENS-refutations of $\neg \mathcal{PHP}_n$. This would disprove a causal remark[3] at the end of [6] that size S Extended Frege (EF) refutations can be transformed into $(\log S)^{O(1)}$ degree UENS-refutations as it is well-known that EF admits p-size proofs of PHP, cf. [7].

[2] An earlier reduction in [10] reduced the lengths-of-proofs problem for $\mathrm{AC}^0[p]$-Frege systems to a different and seemingly harder problem about algebraic search trees.

[3] The construction in [6] seems to yield a non-trivial degree upper bound on ENS proof when transforming Frege proofs of logical depth $o(\log n)$ only.

Note that it is also unknown if EF simulates UENS.

Acknowledgments. I am indebted to the anonymous referee for a number of suggestions.

References

[1] M. Ajtai, The complexity of the pigeonhole principle, in: *Proc. IEEE 29th Annual Symp. on Foundation of Computer Science*, (1988), pp. 346-355.

[2] P. Beame, S. A. Cook, J. Edmonds, R. Impagliazzo and T. Pitassi, The Relative Complexity of NP Search Problems, *J. Computer Systems Sciences*, **57**, (1998), pp.3-19.

[3] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák: Lower bounds on Hilbert's Nullstellensatz and propositional proofs, *Proceedings of the London Mathematical Society*, **(3) 73**, (1996), pp.1-26.

[4] S. R. Buss, Polynomial size proofs of the propositional pigeonhole principle, *J. Symbolic Logic*, **52**, (1987), pp.916-927.

[5] S. R. Buss, Lower bounds on Nullstellensatz proofs via designs, in: *Proof Complexity and Feasible Arithmetics*, eds. S. Buss and P. Beame, American Mathematical Society, Providence RI, (1998), pp. 59-71.

[6] S. R. Buss, R. Impagliazzo, J. Krajíček, P. Pudlák, A. A. Razborov, and J. Sgall: Proof complexity in algebraic systems and bounded depth Frege systems with modular counting, *Computational Complexity*, **6(3)**, (1996/1997), pp.256-298.

[7] S. A. Cook and R. A. Reckhow, The relative efficiency of propositional proof systems, *J. Symbolic Logic*, **44(1)**, (1979), pp.36-50.

[8] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[9] J. Krajíček, *Forcing with random variables and proof complexity*, London Mathematical Society Lecture Note Series, No. **382**, Cambridge University Press, (2011).

[10] J. Krajíček, A reduction of proof complexity to computational complexity for $AC^0[p]$ Frege systems, *Proceedings of the AMS*, **143(11)**, (2015), pp.4951-4965.

[11] J. Krajíček, *Proof complexity*, Encyclopedia of Mathematics and Its Applications, Vol. **170**, Cambridge University Press, (2019).

[12] J. Krajíček, P. Pudlák, and A. Woods, An Exponential Lower Bound to the Size of Bounded Depth Frege Proofs of the Pigeonhole principle", *Random Structures and Algorithms*, **7(1)**, (1995), pp.15-39.

[13] T. Pitassi, P. Beame, and R. Impagliazzo, Exponential lower bounds for the pigeonhole principle, *Computational Complexity*, **3**, (1993), pp.97-308.

[14] A. A. Razborov, Lower Bounds for the Polynomial Calculus, *Computational Complexity*, **7(4)**, (1998), pp.291-324.