INSTITUTE OF MATHEMATICS

THE CZECH ACADEMY OF SCIENCES

New relations and separations of conjectures about incompleteness in the finite domain

Erfan Khaniki

Preprint No. 64-2018

PRAHA 2018

New relations and separations of conjectures about incompleteness in the finite domain

Erfan Khaniki[*]

Department of Mathematical Sciences
Sharif University of Technology
Tehran, Iran

December 14, 2018

Abstract

Our main results are in the following three sections:

1. We prove new relations between proof complexity conjectures that are discussed in [1].
2. We investigate the existence of p-optimal proof systems for TAUT, assuming the collapse of $\mathcal{C}$ and $\mathsf{N}\mathcal{C}$ (the nondeterministic version of $\mathcal{C}$) for some new classes $\mathcal{C}$ and also prove new conditional independence results for strong theories, assuming nonexistence of p-optimal proof systems.
3. We construct two new oracles $\mathcal{V}$ and $\mathcal{W}$. These two oracles imply several new separations of proof complexity conjectures in relativized worlds, among them, we prove that existence of a p-optimal proof system for TAUT and existence of a complete problem for TFNP are independent of each other in relativized worlds which is not known before.

1 Introduction

Proof complexity is a branch of mathematical logic and computational complexity in which it concerns with the length of proofs of tautologies in different proof systems. The main goal is to develop techniques to prove lower bounds for all propositional proof systems, which would entail $\mathsf{NP} \neq \mathsf{CoNP}$. In [1], the main conjectures of proof complexity like the existence of p-optimal proof systems, the existence of a complete problem TFNP with respect to the

[*] e.khaniki@gmail.com

poly time reductions are investigated from point of view of logical strength to prove these statements. Actually, for every one of the main conjectures of proof complexity, an equivalent conjecture is proposed in terms of unprovability of statements in strong enough theories. So it makes the possibility of using the mathematical logic methods to attack these conjectures. The logical methods e.g., a version of forcing used in [15], indeed were successful in some very important results in proof complexity. See [3, 2, 16, 17].

This paper contains three sections. In the first section, we prove new relations between conjectures of [1]. In section 2, We investigate the existence of p-optimal proof systems TAUT, assuming the collapse of $\mathcal{C}$ and $\mathsf{N}\mathcal{C}$ for some new classes $\mathcal{C}$. This investigation leads to a generalization of the conjectures in [1] to use reductions in complexity classes quasipolynomial or subexponential time computable functions. These generalized conjectures have the same relation among each other like the relations between conjectures of [1]. We prove new relations between collapsing complexity classes and the existence of the optimal proof systems and we show that proving the collapse of some complexity classes constructively implies the existence of optimal proof systems for TAUT. Also, we prove for every strong enough theory T , there is a language $L \in \mathsf{N}\mathcal{C}$, such that for every natural definition of a language $L' \in \mathcal{C}$, $T \not\vdash L = L'$ for some classes $\mathcal{C}$ assuming that there is no p-optimal proof system. In section 3, we construct two new oracles. Relative to the first oracle, p-optimal proof systems for TAUT exists, but the class of disjoint CoNP problems does not have complete problems with respect to the poly time functions. Relative to the second oracle TFNP is equal to FP, but length optimal proof systems do not exist. These two oracles imply several new separations of conjectures of [1] in relativized worlds.

2 Preliminaries

Following the notation of [1], we use first order theories of arithmetic in a fixed language. The language is the standard language of the Bounded Arithmetic which is

$$\mathcal{L}_{BA} = \{0, S, +, \cdot, |x|, \lfloor x/2 \rfloor, x\#y\}.$$

The intended meaning of the $\lfloor x/2 \rfloor$ is clear. The meaning of the $|x|$ is $\lceil \log_2(x+1) \rceil$. $x\#y$ is interpreted as $2^{|x|\cdot|y|}$.

A sharply bounded quantifier is of the form $Qx < |t|, Q \in \{\forall, \exists\}$. The class of bounded formulas Σ_n^b, Π_n^b, $n \geq 1$ is defined by counting alternations of bounded quantifiers while ignoring sharply bounded quantifiers. The class of Δ_n^b formulas is the class of Σ_i^b formulas that have an equivalent Π_i^b definition. The theory S_2^1 is defined by some basic axioms defining the usual properties of the function symbols and by induction axioms

$$\phi(0) \wedge \forall x(\phi(\lfloor x/2 \rfloor) \to \phi(x)) \to \forall x \phi(x)$$

for all Σ_1^b formulas. S_2^1 is the base theory in provability with respect to the Bounded Arithmetic hierarchy like $\mathbf{I}\Sigma_1$ with respect to the Peano Arithmetic. One of the main properties of the S_2^1 is that Σ_1^b definable functions of S_2^1 are poly time computable. Also, all of the poly time computable functions are Δ_1^b definable in S_2^1 (A Σ_1^b formula ϕ is Δ_1^b definable in T iff there exists a Π_1^b formula ψ such that $T \vdash \phi \equiv \psi$). For more information about Bounded Arithmetics see [4].

Let $\mathcal{T}$ be the set of all consistent first order theory $\mathsf{S}_2^1 \subseteq T$ in $\mathcal{L}_{BA}$ such that the set of axioms of T is poly time decidable. The main objects of concern in [1] are unprovability and provability results with respect to the members of $\mathcal{T}$. [1] translates the well known conjectures in complexity theory and proof complexity to unprovability statements about members of $\mathcal{T}$.

Now we will explain notations and definitions for Proof complexity conjectures and their translation in [1].

2.1 TFNP class

TFNP or Total NP search problem is the class of true $\forall\Sigma_1^b$ sentences. More formally, a total NP search problem is defined by pair (p, R) such that:

1. $p(x)$ is a polynomial,
2. $R(x, y)$ is poly time computable relation (Δ_1^b definable in S_2^1),
3. $\mathbb{N} \models \forall x \exists y(|y| \leq p(|x|) \wedge R(x, y))$.

For comparing the complexity of TFNP problems, reductions are defined as follow.

Definition 2.1 *Suppose P and Q are in* TFNP*. We say P is polynomially reducible to Q if the search problem P can be solved in polynomial time using an oracle that gives the answer to the search problem Q.*

There are different classes of TFNP which are defined by reductions in seminal paper [5]. These classes are of the form of *all* TFNP *problems that are reducible to a* TFNP *problem P*. Another way to compare the complexity of TFNP problems is measuring how much axioms we need to prove a search problem is total. This approach has reductions implicitly in it. The next definition formalizes this notion which is defined in [1].

Definition 2.2 *Suppose T is in $\mathcal{T}$. We say (p, R) is provably total in T or $(p, R) \in \mathsf{TFNP}(T)$ iff there exists a pair (q, ϕ) such that:*

1. *q is a polynomial,*
2. *$\phi(x, y)$ is Δ_1^b definable in S_2^1,*
3. *$\mathbb{N} \models \forall x, y((|y| \leq p(|x|) \wedge R(x, y)) \equiv (|y| \leq q(|x|) \wedge \phi(x, y)))$,*
4. *$T \vdash \forall x \exists y(|y| \leq q(|x|) \wedge \phi(x, y))$.*

Also, we define $\mathsf{TFNP}^*(T)$ *as the class of all* TFNP *problems that is reducible to a problem in* $\mathsf{TFNP}(T)$*.*

$\mathsf{TFNP}(T)$ is characterized for many bounded arithmetics $T \in \mathcal{T}$. Actually, $\mathsf{TFNP}(T)$ for a bounded arithmetic theory $T \in \mathcal{T}$ is a measurement of the strength of the bounded arithmetics T like the provably total recursive functions for strong theories. The following theorem shows the relationship between the strength of reduction and provability.

Theorem 2.1 *([1]) The following statements are equivalent:*

1. *There exists a problem $(p, R) \in \mathsf{TFNP}$ that is complete with respect to the polynomial reductions for class TFNP,*
2. *There exists $T \in \mathcal{T}$ such that $\mathsf{TFNP}^*(T) = \mathsf{TFNP}$.*

The main conjecture about TFNP class is that it does not have a complete problem with respect to the polynomial reductions. We will show this conjecture by TFNP_c.

2.2 Proof systems

Following the definition of Cook-Reckhow, a proof system for set $C \subseteq \mathbb{N}$ is a poly time computable function $P : \mathbb{N} \to \mathbb{N}$ (The graph of P is Δ_1^b in S_2^1) such that $R_P = C$. We assume that different objects like formulas, proofs and etc are coded in a natural way in binary strings, hence every binary code x can be shown by natural number with binary expansion $1x$ which we will show it by $\llcorner x \lrcorner$. To code sequence of finite binary strings x_1 to x_n that is shown by $\langle x_1, ..., x_n \rangle$, we use the following coding $x_1^* x_2^* ... x_{n-1}^* x_n$ in which for a binary string z, z^* is obtained from z by doubling its digit and appending the string 01 at the end of it. Note that we can use the same coding schema for coding a finite sequence of natural numbers. By this explanation, we can define proof systems for different sets like propositional tautologies (TAUT) or satisfiable propositional formulas (SAT). By length of an object (formulas, proofs,...) with the natural number n as its code, we mean $|n|$. For every object A, we will use the notation $\ulcorner A \urcorner$ to show the numerical code of A.

A proof system P for set C is poly bounded iff there exists a polynomial $q(x)$ such that for every $n \in C$, there exists a proof $\pi \in \mathbb{N}$ such that $P(\pi) = n$ and $|\pi| \leq q(|n|)$. One of the most important conjectures in Proof Complexity is nonexistence if a poly bounded proof system for TAUT. In terms of Complexity theory language, this conjecture is equivalent to $\mathsf{NP} \neq \mathsf{CoNP}$. Another concept that is weaker than poly boundedness is optimality. The following definition formalizes the ingredient of this concept.

Definition 2.3 *Suppose P and Q are proof systems for set C. We say that P non-uniformly p-simulates Q iff there exists a polynomial $h(x)$ such that:*

$$\forall \pi \in \mathbb{N}, \forall n \in C(Q(\pi) = n \to \exists \pi' \in \mathbb{N}(|\pi'| \leq h(|\pi|) \wedge P(\pi') = n))$$

We say that P p-simulates Q iff there exists a poly time function f such that:

$$\forall \pi \in \mathbb{N}, \forall n \in C(Q(\pi) = n \to P(f(\pi)) = n)$$

Normally, non-uniformly p-simulation calls simulation in the literature, but because we will generalize these concepts to bigger complexity classes we named it in this way to make it distinguishable with generalize cases.

We call a proof system P for set C is (non-uniformly) p-optimal iff for every proof system Q for set C, P (non-uniformly) p-simulates Q. One of the main conjecture about (non-uniformly) p-optimality is that there is no (non-uniformly) p-optimal proof system for TAUT. We will show these conjectures with CON and $\mathsf{CON}^{\mathsf{N}}$ in which N stands for nonuniform. Another important conjecture about p-optimality is that there is no p-optimal proof system for SAT which we call it SAT_c. To translate these conjectures to provability and unprovability of theories in $\mathcal{T}$ we need to define some machinery. Note that for every $T \in \mathcal{T}$, because the axioms of T are poly time decidable, there exists a poly time computable relation $Pr_T(x, y)$ in which it is true iff x is code of a T-proof in usual Hilbert style calculi of a formula in $\mathcal{L}_{BA}$ with code y. One of the important properties of $Pr_T(x, y)$ is the following theorem.

Theorem 2.2 *([4]) For every $T \in \mathcal{T}$, every Σ_1^b formula $\phi(x)$, there exists a polynomial $p(x)$ such that $T \vdash \forall x(\phi(x) \to \exists y(|y| \leq p(|x|) \wedge Pr_T(y, \ulcorner \phi(\dot{x}) \urcorner))$.*

Note that for every nonempty set $C \subseteq \mathbb{N}$, C has a proof system iff C is recursively enumerable. Suppose $C \subseteq \mathbb{N}$ is a nonempty recursively enumerable set. Let $\phi_C(x)$ be a Σ_1 formula in $\mathcal{L}_{BA}$ defining C. To define a proof system for $\phi_C(x)$ from a theory $T \in \mathcal{T}$ we need to define a natural number in $\mathcal{L}_{BA}$ in an efficient way. The following definition gives us an efficient way of defining the numerals.

Definition 2.4

$$\bar{n} = \begin{cases} 0 & n = 0 \\ SS0 \cdot \bar{k} & n = 2k \\ S(SS0 \cdot \bar{k}) & n = 2k+1 \end{cases}$$

Note that the coded version of $\bar{n}$ needs $O(\log_2 n)$ bits. Also the notation $\ulcorner \phi(\dot{n}) \urcorner$ for formula $\phi(x)$ in $\mathcal{L}_B A$ is a poly time computable function that is output the code of formula $\phi(\bar{n})$.

Suppose a is in C. Now we define the proof system P_T^C associated with T for C as follows:

1. Given π, if $\mathbb{N} \models Pr_T(\pi, \ulcorner \phi_C(\dot{n}) \urcorner)$ for some n, then outputs n,

2. otherwise outputs a.

Let $Con_T(n)$ be the formula $\forall x(|x| \leq n \to \neg Pr_T(x, \ulcorner \bot \urcorner))$. Using above notations and definitions we can express theorems that shows relationship between optimality of proof systems and provability in members of $\mathcal{T}$.

Theorem 2.3 *([2]) The following statements are equivalent:*

1. *There exists a nonuniform p-optimal proof system for* TAUT,

2. *There exists $T \in \mathcal{T}$ such that for every $S \in \mathcal{T}$, the shortest T-proofs of $Con_S(\bar{n})$ is bounded by a polynomial in n.*

To work with propositional tautologies and satisfiable formulas we use poly time computable relation $\mathsf{SAT}(x, y)$ that it means propositional formula with code x is satisfiable in assignment with code y. Also, we use Π_1^b notation $\mathsf{TAUT}(x) := \forall y(y \leq x \rightarrow sat(x, y))$ to define propositional tautologies.

Theorem 2.4 *([2]) The following statements are equivalent:*

1. *There exist a p-optimal proof system for* TAUT,

2. *There exists $T \in \mathcal{T}$ such that for every $S \in \mathcal{T}$, there exists a poly time computable function h that for every n, $h(n)$ is a T-proof of $Con_S(\bar{n})$.*

3. *There exists $T \in \mathcal{T}$ such that for every proof system P for* TAUT, *there exists a poly time formalization $P'(x, y)$ of relation $P(x) = y$ that*

$$T \vdash \forall x, y(P'(x, y) \rightarrow \mathsf{TAUT}(y)).$$

The following theorem gives translation of the nonexistence of p-optimal proof system for SAT.

Theorem 2.5 *([1]) The following statements are equivalent:*

1. *There exist a p-optimal proof system for* SAT,

2. *There exists $T \in \mathcal{T}$ such that for every proof system P for* SAT, *there exists a poly time formalization $P'(x, y)$ of relation $P(x) = y$ that*

$$T \vdash \forall x, y(P'(x, y) \rightarrow \exists z(z < y \wedge \mathsf{SAT}(y, z))).$$

2.3 Disjoint NP pairs, Disjoint CoNP pairs

The concept of Disjoint NP pairs and Disjoint CoNP pairs are discussed in [1] to define stronger conjectures than TFNP_c and $\mathsf{CON}^{\mathsf{N}}$. A pair of $(\mathsf{Co})\mathsf{NP}$ languages (U, V) is a disjoint $(\mathsf{Co})\mathsf{NP}$ pair iff $U \cap V = \varnothing$. We will show this class of pairs by $\mathsf{Disj}(\mathsf{Co})\mathsf{NP}$. To compare complexity of disjoint $(\mathsf{Co})\mathsf{NP}$ pairs reductions are defined as follow:

Definition 2.5 *Suppose (U_0, U_1) and (U'_0, U'_1) are disjoint* $(\mathsf{Co})\mathsf{NP}$ *pairs. We say (U_0, U_1) is polynomial reducible to (U'_0, U'_1) iff there exists a poly time computable function f such that for $i \in \{0, 1\}$:*

$$\forall n \in \mathbb{N}(n \in U_i \rightarrow f(n) \in U'_i)$$

Again, another way to compare complexity of disjoint $(\mathsf{Co})\mathsf{NP}$ pairs is measuring how much axioms we need to prove such a pair is disjoint. The next definition formalize this notion.

Definition 2.6 *Suppose T is in $\mathcal{T}$. We say* $\mathsf{(Co)NP}$ *pair* (U_0, U_1) *is provably disjoint in* T *or* $(U_0, U_1) \in \mathsf{Disj(Co)NP}(T)$ *iff there exists a* (Π_1^b) Σ_1^b *pair* (ϕ_0, ϕ_1) *such that:*

1. $\mathbb{N} \models \forall x(x \in U_i \equiv \phi_i(x)), i \in \{0, 1\}$,
2. $T \vdash \forall x(\neg\phi_0(x) \vee \neg\phi_1(x))$.

Like theorem 2.1, the following theorem shows the relationship between the strength of reduction and provability.

Theorem 2.6 *([1]) The following statements are equivalent:*

1. *There exists a pair* $(U, V) \in \mathsf{Disj(Co)NP}$ *that is complete with respect to the polynomial reductions for class* $\mathsf{Disj(Co)NP}$*,*
2. *There exists* $T \in \mathcal{T}$ *such that* $\mathsf{Disj(Co)NP}(T) = \mathsf{Disj(Co)NP}$.

The main conjecture about disjoint $\mathsf{(Co)NP}$ pairs is that it does not have a complete problem with respect to the polynomial reductions. We will show this conjecture by $\mathsf{Disj(Co)NP}_c$.

2.4 A finite reflection principle

A finite reflection principle for Σ_1^b formulas is defined in [1] to propose a conjecture that connects defined conjectures in this section. To define the conjecture we need the following theorem.

Theorem 2.7 *([7]) For every $i \geq 1$ there exists a Σ_i^b formula μ_i such that for every Σ_i^b formula $\phi(x)$ there exists natural number e and polynomial p such that:*

$$\mathsf{S}_2^1 \vdash \forall x, y(|y| \geq p(|x|) \to (\mu_i(\bar{e}, x, y) \equiv \phi(x)))$$

The finite reflection principle is defined as follows.

Definition 2.7 *For every $T \in \mathcal{T}$, $n \in \mathbb{N}$, the $\Sigma_1^b\mathsf{RFN}_T(\bar{n})$ is defined by*

$$\forall e, u, x, z(|e|, |u|, |x|, |z| \leq \bar{n} \wedge Pr_T(u, \ulcorner \mu_1(\dot{e}, \dot{x}, \dot{z}) \urcorner) \to \mu_1(e, x, z)).$$

The following conjectures are defined in [1]:

1. $\mathsf{RFN}_1^{\mathsf{N}}$: For every $T \in \mathcal{T}$, there exists $S \in \mathcal{T}$ such that the T-proofs of $\Sigma_1^b\mathsf{RFN}_{1T}(\bar{n})$ is not polynomially bounded in n.
2. RFN_1: For every $T \in \mathcal{T}$, there exists $S \in \mathcal{T}$ such that the T-proofs of $\Sigma_1^b\mathsf{RFN}_{1T}(\bar{n})$ can not be constructed in polynomial time.

The following figure shows the relation between conjectures of this section. For more information about proof of these relations see [1].

$$\begin{tikzcd}
\mathsf{DisjNP}_c \arrow[d] & & \mathsf{DisjCoNP}_c \arrow[d] \\
\mathsf{CON}^{\mathsf{N}} \arrow[d] \arrow[dr] & & \mathsf{TFNP}_c \arrow[d] \\
\mathsf{RFN}_1^{\mathsf{N}} \arrow[d] \arrow[dr] & \mathsf{CON} \arrow[d] & \mathsf{SAT}_c \arrow[dl] \\
\mathsf{NP} \neq \mathsf{CoNP} \arrow[dr] & \mathsf{RFN}_1 \arrow[d] & \\
& \mathsf{P} \neq \mathsf{NP} &
\end{tikzcd}$$

Figure 1: Relations between conjectures

3 Incompleteness in the finite domain

3.1 Some observations on TFNP class

As we see in the previous section, the logical equivalent conjectures that are discussed are of the following form:

For every $T \in \mathcal{T}$ there exists some sentence(s) ϕ that it does not have T-proof(s) with some properties.

The above form is work for all of the conjectures that we discussed except TFNP_c. The logical form of TFNP_c conjecture uses $\mathsf{TFNP}^*(T)$ instead of $\mathsf{TFNP}(T)$. Here we want to investigate what happens if we use $\mathsf{TFNP}(T)$. This new conjecture which we call it TFNP_c^w is weaker than TFNP_c. The next proposition shows that it is stronger than SAT_c.

Proposition 3.1 *If for every $T \in \mathcal{T}$ we have $\mathsf{TFNP}(T) \neq \mathsf{TFNP}$, then there is no p-optimal proof system for SAT.*

Proof. Suppose P is a p-optimal proof system for SAT. Define $T := \mathsf{S}_2^1 + \forall x \exists y \mathsf{SAT}(P(x), y)$. Let (p, R) be a TFNP problem and (q, ϕ) be one of its formalizations. Suppose F is a proof system for SAT. Let θ_n be the usual propositional translation polynomial time relation $|y| \leq q(|\bar{n}|) \wedge \phi(\bar{n}, y)$. Define proof system P_ϕ for SAT as follows:

$$P_\phi(x) = \begin{cases} F(n) & x = 2n \\ \theta_n & x = 2n+1 \end{cases}$$

Because P is a p-optimal proof system, there exists a poly time function h such that $\mathbb{N} \models \forall x(P(h(x)) = P_\phi(x))$. This implies that

$$\mathbb{N} \models \forall x, y\big((|y| \leq q(|x|) \wedge \phi(x, y)) \equiv \mathsf{SAT}(P(h(2x+1)), f(y))\big)$$

for some poly time function f, hence $\mathsf{SAT}(P(h(2x+1)), f(y))$ is another formalization of (p, R). Note that by definition of T we have $T \vdash \forall x \exists y \mathsf{SAT}(P(h(2x+1)), f(y))$ which means $(p, R) \in \mathsf{TFNP}(T)$. ■

We can not prove that TFNP_c^w implies TFNP_c, but one way to show that the latter conjecture is probably stronger is to find a $T \in \mathcal{T}$ such that $\mathsf{TFNP}(T) \neq \mathsf{TFNP}^*(T)$. It is conjectured that such a T exists, but we observed that existence of such a T implies $\mathsf{TFNP} \neq \mathsf{FP}$, hence proving this conjecture unconditionally is hard. We need the following lemma to prove previous implication.

Lemma 3.2 $\mathsf{TFNP}(\mathsf{S}_2^1) = \mathsf{FP}$.

Proof. By the fact that Σ_1^b definable functions of S_2^1 is poly time computable we get $\mathsf{TFNP}(\mathsf{S}_2^1) \subseteq \mathsf{FP}$, so it is sufficient to prove $\mathsf{FP} \subseteq \mathsf{TFNP}(\mathsf{S}_2^1)$. Let (p, R) be a TFNP problem which can be solved by the poly time function f. Let ϕ be the Δ_1^b formalization of f in S_2^1. Also, let (q, ψ) be a formalization of (p, R). Note that $(q, \psi \vee \phi)$ is a formalization of (p, R) and also, $\mathsf{S}_2^1 \vdash \forall x \exists y(|y| \leq q(|x|) \wedge (\psi(x, y) \vee \psi(x, y))$, hence $(p, R) \in \mathsf{TFNP}(\mathsf{S}_2^1)$, which implies $\mathsf{FP} \subseteq \mathsf{TFNP}(\mathsf{S}_2^1)$. ■

Corollary 3.3 *If there exists* $T \in \mathcal{T}$ *such that* $\mathsf{TFNP}(T) \neq \mathsf{TFNP}^*(T)$*, then* $\mathsf{TFNP} \neq \mathsf{FP}$.

Proof. Suppose TFNP is equal to FP, hence for every $T \in \mathcal{T}$, $\mathsf{TFNP}(T) \subseteq \mathsf{FP}$, which implies $\mathsf{TFNP}^*(T) \subseteq \mathsf{FP}^{\mathsf{FP}} = \mathsf{FP}$. Also, by definition of T and lemma 3.2, $\mathsf{FP} = \mathsf{TFNP}(\mathsf{S}_2^1) \subseteq \mathsf{TFNP}(T)$, hence $\mathsf{TFNP}(T) = \mathsf{TFNP}^*(T) = \mathsf{FP}$ which completes the proof. ■

3.2 On Proof systems and RFN_1 Conjecture

As we saw, every conjecture that discussed in the previous section has two formalizations, one in terms of proof complexity notations and one in terms of incompleteness in the finite domain notations except RFN_1 and $\mathsf{RFN}_1^{\mathsf{N}}$. Here we want to show that these conjectures have equivalent forms in terms of optimal proof systems for Σ_1^q-TAUT. Σ_i^q (Π_i^q)propositional formulas are quantified propositional formulas and defined like the hierarchy of bounded formulas in $\mathcal{L}_{BA}$. The next theorem is similar to the theorems 2.4 and 2.5 for CON and $\mathsf{CON}^{\mathsf{N}}$.

Theorem 3.4

1. *The following statements are equivalent:*

   (a) *For every $T \in \mathcal{T}$, there exists $S \in \mathcal{T}$ such that the T-proofs of $\Sigma_1^b\mathsf{RFN}_{1T}(\bar{n})$ are not polynomially bounded in n.,*

   (b) *Σ_1^q-TAUT does not have a nonuniform p-optimal proof system,*

2. *The following statements are equivalent:*

   (a) *For every $T \in \mathcal{T}$, there exists $S \in \mathcal{T}$ such that the T-proofs of $\Sigma_1^b\mathsf{RFN}_{1T}(\bar{n})$ can not be constructed in polynomial time.,*

   (b) *Σ_1^q-TAUT does not have a p-optimal proof system,*

   (c) *For every theory $T \in \mathcal{T}$, there exists a proof system P for Σ_1^q-TAUT such that T does not prove the soundness of any formalization of P.*

Proof. Here we prove the second part. The proof of the first part is similar.

$(a) \Rightarrow (b)$. Suppose (b) is false. Let P be a p-optimal proof system for Σ_1^q-TAUT. Let $T := \mathsf{S}_2^1 + \forall\pi,\phi(P(\pi,\phi) \to \mathsf{TAUT}_{\Sigma_1^q}(\phi))$ in which $\mathsf{TAUT}_{\Sigma_1^q}$ is the Π_2^b formula that checks wether a Σ_1^q propositional formula is true or not. Let $S \in \mathcal{T}$. Note that for every $n \in \mathbb{N}$, the translation of $\Sigma_1^b\mathsf{RFN}_S(\bar{n})$ is Σ_1^q formula θ_n such that $\mathsf{S}_2^1 \vdash \Sigma_1^b\mathsf{RFN}_S(\bar{n}) \equiv \mathsf{TAUT}_{\Sigma_1^q}(\theta_n)$ and this proof can be constructed in poly time $(*)$. Let P' be a proof system defined as follow:

$$P'(x) = \begin{cases} \theta_n & x = \theta_n \text{ for some } n \\ P(x) & \text{o.w.} \end{cases}$$

Let f be the poly time function that $P(f(\pi)) \equiv P'(\pi)$ for every $\pi \in \mathbb{N}$. Note that for every $n \in \mathbb{N}$ the proof of $\mathsf{S}_2^1 \vdash P(f(\theta_n), \theta_n)$ can be constructed in poly time, therefore by soundness of P which is provable in T and $(*)$, the proof of $T \vdash \Sigma_1^b\mathsf{RFN}_S(\bar{n})$ for every $n \in \mathbb{N}$ can be constructed in poly time too.

$(b) \Rightarrow (c)$. Suppose (c) is false. Let $T \in \mathcal{T}$ be a theory that falsifies (c). We want to prove that $P_T^{\Sigma_1^q}$ is p-optimal . Let P' be a proof system and P'' be one of its formalization such that $T \vdash \forall\pi,\phi(P''(\pi,\phi) \to \mathsf{TAUT}_{\Sigma_1^q}(\phi))$. Note that there exists a poly time function f such that

$$T \vdash \forall\pi,\phi(P''(\pi,\phi) \to Pr_T(f(\pi,\phi), \ulcorner P''(\dot{\pi},\dot{\phi})\urcorner)).$$

Without loss of generality we can assume that there exists a poly time function g such that for every π-proof in P'', $\mathbb{N} \models P''(\pi, g(\pi))$, hence there exists a poly time function h such that $P''(\pi,\phi) \equiv P_T^{\Sigma_1^q}(h(\pi),\phi)$, for all $\pi,\phi \in \mathbb{N}$.

$(c) \Rightarrow (a)$. Suppose (a) is false. Let $T \in \mathcal{T}$ be a theory that witness this fact. First, we show that $P_T^{\Sigma_1^q}$ is p-optimal. Let $\mathsf{SAT}_{\Sigma_1^q}(\phi, v)$ be the Σ_1^b formula that it can check satisfiability of Σ_1^q propositional formulas. Without loss of generality, suppose P is a proof system such that by knowing a π-proof in P, we can find ϕ_π such that $P(\pi,\phi_\pi)$ is true. Define $T' := \mathsf{S}_2^1 + \forall\pi,\phi,v(P(\pi,\phi) \to \mathsf{SAT}_{\Sigma_1^q}(\phi,v))$. If $P(\pi,\phi_\pi)$ is true, then we can find a proof

π' in poly time such that $P_{T'}^{\Sigma_1^q}(\pi', \phi_\pi)(*)$. Note that there exists a poly time function f such that

$$\mathbb{N} \models \forall \pi, v, \phi(|v| \leq |\phi| \wedge P_T^{\Sigma_1^q}(\pi, \phi) \rightarrow P_T^{\Sigma_1^q}(f(\pi, v), \phi[v/\vec{p}])).$$

Let $T'' = \mathsf{S}_2^1 + \forall \pi, v, \phi(|v| \leq |\phi| \wedge P_T^{\Sigma_1^q}(\pi, \phi) \rightarrow P_T^{\Sigma_1^q}(f(\pi, v), \phi[v/\vec{p}]))$. Note that T falsifies RFN_1, hence P_T is p-optimal proof system for propositional formulas, this means P_T p-simulates $P_{T''}(**)$. Note that propositional translation of $\forall \pi, v, \phi(|v| \leq |\phi| \wedge P_T^{\Sigma_1^q}(\pi, \phi) \rightarrow P_T^{\Sigma_1^q}(f(\pi, v), \phi[v/\vec{p}]))$ has short proof in $P_{T''}$ and these proofs can be constructed in poly time, hence by (*) and (**) we can find a T-proof π'' of $\forall v(|v| \leq |\phi| \rightarrow P_{T'}^{\Sigma_1^q}(f(\pi', v), \phi_\pi[v/\vec{p}]))$ in poly time, therefore by constructing a $\Sigma_1^b\mathsf{RFN}_{T'}(n)$ for some suitable n which is polynomial in size of ϕ, we can get a proof π_T such that $P_T^{\Sigma_1^q}(\pi_T, \phi_\pi)$. So $P_T^{\Sigma_1^q}$ is p-optimal, therefore theory $\mathsf{S}_2^1 + \forall \pi, \phi(P_T^{\Sigma_1^q}(\pi, \phi) \rightarrow \mathsf{TAUT}_{\Sigma_1^q}(\phi))$ falsifies (c).

■

Note that the previous theorem can be generalized for finite reflection principle conjectures for Σ_i^b formulas which is RFN_i.

By looking at the figure 1, we observe that the upper conjectures are stronger from those that are behind them and it is not known whether an opposite implication can be proved, i.e. a weak conjecture implies a stronger one. The next theorem shows a kind of opposite implication. In terms of defined notations the next theorem shows RFN_1 implies $\mathsf{CON} \vee \mathsf{SAT}_c$.

Theorem 3.5 *At least one of the following statements is true:*

1. *There is no p-optimal proof system for* SAT*,*
2. *There is no p-optimal proof system for* TAUT*,*
3. *There exists a $T \in \mathcal{T}$ such that for every $S \in \mathcal{T}$, the T-proofs of $\Sigma_1^b\mathsf{RFN}_{1T}(\bar{n})$ can be constructed in polynomial time.*

Proof. Suppose (1) and (2) are false. Let $T \in \mathcal{T}$ be the theory that falsifies (1) and (2) simultaneously. Suppose is S in $\mathcal{T}$. We want to show that there exists a poly time function h such that for every S-proof π of $\forall u(|u| \leq |\phi| \rightarrow \mathsf{SAT}_{\Sigma_1^q}(\phi, u))$, $h(\pi)$ is a T-proof of $\forall u(|u| \leq |\phi| \rightarrow \mathsf{SAT}_{\Sigma_1^q}(\phi, u))$ and hence $\neg\mathsf{RFN}$. Note that there exists a poly time function f such that

$$\mathbb{N} \models \forall \pi, v, \phi(|v| \leq |\phi| \wedge P_S^{\Sigma_1^q}(\pi, \phi) \rightarrow P_S^{\Sigma_1^q}(f(\pi, v), \phi[v/\vec{p}])).$$

Because $Pr_S(\pi, \ulcorner \forall u(|u| \leq |\phi| \rightarrow \mathsf{SAT}_{\Sigma_1^q}(\phi, u))\urcorner)$ is true, we can find a short T-proof of $Pr_S(\pi, \ulcorner \forall u(|u| \leq |\phi| \rightarrow \mathsf{SAT}_{\Sigma_1^q}(\phi, u))\urcorner)$ in poly time $(*)$.

Define $S' := \mathsf{S}^1_2 + \forall\pi, v, \phi(|v| \leq |\phi| \wedge P_S^{\Sigma^q_1}(\pi, \phi) \rightarrow P_S^{\Sigma^q_1}(f(\pi, v), \phi[v/\vec{p}]))$. Because T falsifies (2) and S' has short proof of $\forall\pi, v, \phi(|v| \leq |\phi| \wedge P_S^{\Sigma^q_1}(\pi, \phi) \rightarrow P_S^{\Sigma^q_1}(f(\pi, v), \phi[v/\vec{p}]))$, we can find a short T-proof of

$$\forall v(|v| \leq |\phi| \wedge Pr_S(\pi, \ulcorner \forall u(|u| \leq |\phi| \rightarrow \mathsf{SAT}_{\Sigma^q_1}(\phi, u))\urcorner) \rightarrow Pr_S(f(\pi, v), \ulcorner \mathsf{SAT}_{\Sigma^q_1}(\phi, \dot{v})\urcorner))$$

in poly time. Therefore by $(*)$ we get a T-proof of $\forall v(|v| \leq |\phi| \rightarrow Pr_S(f(\pi, v), \ulcorner \mathsf{SAT}_{\Sigma^q_1}(\phi, \dot{v})\urcorner))$ $(**)$. Because of the fact that T falsifies (1), T proves that the SAT proof system defined from S is sound and hence by $(**)$ the T-proof of $\forall v(|v| \leq |\phi| \rightarrow \mathsf{SAT}_{\Sigma^q_1}(\phi, v))$ can be constructed in poly time. ■

4 Nondeterministic vs Deterministic computations and existence of optimal proof systems

In this section we investigate the relationship between equality of nondeterministic and deterministic computation and existence of optimal proof systems. The trivial case is $\mathsf{P} = \mathsf{NP}$ that implies the existence of a poly time computable proofs for TAUT. The first step in this direction was done in [2]. They showed that $\mathsf{E} = \mathsf{NE}$ implies existence of p-optimal proof systems for TAUT. Latter, It was shown in [9] that the condition $\mathsf{EE} = \mathsf{NEE}$ is sufficient. This phenomenon was investigated further in [10] by defining the Fat and Slim complexity classes and proving the following results about them:

1. (a) For every slim class $\mathcal{C}$, $\mathcal{C} = \mathsf{CoN}\mathcal{C}$ implies existence of a nonuniform p-optimal proof system for TAUT.

   (b) For every slim class $\mathcal{C}$, $\mathsf{N}\mathcal{C} = \mathsf{CoN}\mathcal{C}$ implies existence of a p-optimal proof system for TAUT.

2. (a) For every fat class $\mathcal{C}$, there exists an oracle A such that $\mathcal{C}^A = \mathsf{CoN}\mathcal{C}^A$, but there is no p-optimal proof system for TAUT^A.

   (b) For every fat class $\mathcal{C}$, there exists an oracle A such that $\mathsf{N}\mathcal{C}^A = \mathsf{CoN}\mathcal{C}^A$, but there is no nonuniform p-optimal proof system for TAUT^A.

First of all, we show a similar sufficient conditions for existence of nonuniform and uniform p-optimal proof system for Σ^q_1-TAUT. Note that by theorem 3.4 existence of a such proof systems is equivalent to $\neg\mathsf{RFN}^{\mathsf{N}}_1$ and $\neg\mathsf{RFN}_1$ respectively. It is shown in [1] that $\mathsf{RFN}^{\mathsf{N}}_1$ implies $\mathsf{NP} \neq \mathsf{CoNP}$. The next proposition strengthens this result. To state next proposition, we need to define k'th Exponential Time Hierarchy.

Definition 4.1 *Define the following functions inductively:*

1. $|x|_n = \begin{cases} |x|_0 = x \\ |x|_{n+1} = ||x|_n| \end{cases}$, *2.* $2^x_n = \begin{cases} 2^x_0 = x \\ 2^x_{n+1} = 2^{2^x_n} \end{cases}$.

Definition 4.2 *For every k define k'th* **Exponential Time Hierarchy** *(EH_k) as follows:*

- *For every $L \subseteq \mathbb{N}$, L is in E_k iff there exists a Δ^b_1 formula $\phi(x)$ in S^1_2 such that $\forall n(n \in L \leftrightarrow \phi(2^n_k))$,*
- *For every $L \subseteq \mathbb{N}$, L is in $\Sigma^{\mathsf{E}_k}_i$ for some $i > 0$ iff there exists a Σ^b_i formula $\phi(x)$ such that $\forall n(n \in L \leftrightarrow \phi(2^n_k))$,*
- *For every $L \subseteq \mathbb{N}$, L is in $\Pi^{\mathsf{E}_k}_i$ for some $i > 0$ iff there exists a Π^b_i formula $\phi(x)$ such that $\forall n(n \in L \leftrightarrow \phi(2^n_k))$.*

Note that we do not have a exponentiation function symbol in $\mathcal{L}_{BA}$, therefore by formula $\forall n\phi(2^{f(n)}_k)$ for some poly time function f and some fix k, we mean $\forall m, n(\psi_{f,k}(m, n) \to \phi(m))$ in which $\psi_{f,k}(m, n)$ is a Δ^b_1 formula in S^1_2 that is true iff $m = 2^{f(n)}_k$.

Proposition 4.1 *The following statements are true:*

1. *If for every $T \in \mathcal{T}$, there exists $S \in \mathcal{T}$ such that the T-proofs of $\Sigma^b_1\mathsf{RFN}_{1T}(\bar{n})$ is not polynomially bounded in n, then $\mathsf{NE} \neq \Sigma^{\mathsf{E}}_2$.*
2. *If for every $T \in \mathcal{T}$, there exists $S \in \mathcal{T}$ such that the T-proofs of $\Sigma^b_1\mathsf{RFN}_{1T}(\bar{n})$ can not be constructed in polynomial time, then $\mathsf{E} \neq \Sigma^E_2$.*

Proof. Here we prove the statement (1). The statement (2) has a similar proof. Let $\mathsf{NE} = \Sigma^{\mathsf{E}}_2$. This implies that $\mathsf{NE} = \Pi^{\mathsf{E}}_2$, because $\mathsf{CoNE} \subseteq \Sigma^{\mathsf{E}}_2$. Define the following complete languages:

1. $L_{\Pi^{\mathsf{E}}_2} = \{n = \langle e, x, m\rangle \in \mathbb{N} : \mathbb{N} \models \neg\mu_2(e, x, 2^{2^{|m|}})\} \in \Pi^{\mathsf{E}}_2$-complete,
2. $L_{\mathsf{NE}} = \{n = \langle e, x, m\rangle \in \mathbb{N} : \mathbb{N} \models \mu_1(e, x, 2^{2|m|})\} \in \mathsf{NE}$-complete.

By definition there exist the following predicates:

1. There exists a Π^b_2 predicate $\mathsf{U}_{\Pi^b_2}$ such that $\mathbb{N} \models \forall n(\mathsf{U}_{\Pi^b_2}(2^n) \leftrightarrow n \in L_{\Pi^{\mathsf{E}}_2})$,
2. There exists a NP predicate U_{NP} such that $\mathbb{N} \models \forall n(\mathsf{U}_{\mathsf{NP}}(2^n) \leftrightarrow n \in L_{\mathsf{NE}})$.

Note that $\mathsf{NE} = \Pi^{\mathsf{E}}_2$ implies that there exists a linear time function f such that

$$\mathbb{N} \models \forall n(\mathsf{U}_{\Pi^b_2}(2^n) \leftrightarrow \mathsf{U}_{\mathsf{NP}}(2^{f(n)})).$$

Let $T \in \mathcal{T}$ be a theory with the following properties:

1. $T \vdash \mathsf{U}_{\mathsf{NP}}(2^n)$ is NE-complete with respect to the poly time reductions,
2. $T \vdash \mathsf{U}_{\Pi^b_2}(2^n)$ is Π^{E}_2-complete with respect to the poly time reductions,

3. $T \vdash \forall n(\mathsf{U}_{\Pi_2^b}(2^n) \leftrightarrow \mathsf{U}_{\mathsf{NP}}(2^{f(n)}))$

Let T' be in $\mathcal{T}$. This implies $\Sigma_1^b\mathsf{RFN}_{T'}(x) \in \Pi_2^{\mathsf{E}}$, so by mentioned properties of T there exists a linear time function g such that $T \vdash \forall n\big(\Sigma_1^b\mathsf{RFN}_{T'}(n) \leftrightarrow \mathsf{U}_{\mathsf{NP}}(2^{f(g(n))})\big)$. Because $\mathsf{U}_{\mathsf{NP}}(x)$ is Σ_1^b and also $\mathsf{S}_2^1 \subseteq T$, there exists a polynomial $r(x)$ such that

$$T \vdash \forall x\big(\mathsf{U}_{\mathsf{NP}}(x) \to \exists y\big(|y| \leq r(|x|) \wedge Pr_T\big(y, \ulcorner \mathsf{U}_{\mathsf{NP}}(\dot{x})\urcorner\big)\big)\big).$$

This implies

$$T \vdash \forall x\big(\mathsf{U}_{\mathsf{NP}}(2^{f(g(x))}) \to \exists y\big(|y| \leq r(f(g(x))+1) \wedge Pr_T\big(y, \ulcorner \mathsf{U}_{\mathsf{NP}}(2^{f(g(\dot{x}))})\urcorner\big)\big)\big).$$

Note that $\mathbb{N} \models \forall n \mathsf{U}_{\mathsf{NP}}(2^{f(g(n))})$, so for every $n \in \mathbb{N}$, $T \overset{r(f(g(n))+1)}{\vdash} \mathsf{U}_{\mathsf{NP}}(2^{f(g(\bar{n}))})$, hence there exists a polynomial $p(x)$ such that for every $n \in \mathbb{N}$, $T \overset{p(n)}{\vdash} \Sigma_1^b\mathsf{RFN}_{T'}(\bar{n})$. ■

In the next theorem, we will investigate that how much optimality we can get by assuming the equality of nondeterministic and (co-non)deterministic computation for fat classes in sense of [10] like EXP and E_k for $k > 2$. To state the theorem we need some definitions. Let $2^{o(n)}$ and $2^{(\log n)^{O(1)}}$ be sub exponential (subExp) and quasi polynomial (Qp) respectively. The concept of simulations and reductions can be defined in terms of other time classes like sub-exponential or quasi-polynomial time instead of polynomial time and the relations in figure 1 remain true, hence it is natural to ask whether these new conjectures are true or not. An oracle is constructed in [11] that DisjNP pairs do not have complete problems with respect to the poly time reductions. It is not hard to modify that construction to make an oracle in which DisjNP pairs do not have complete problem with respect to the sub exponential time reductions, hence conjectures weaker than it are true with respect to that oracle. For the other branch, we will construct an oracle that $\mathsf{DisjCoNP}$ pairs do not have complete problems with respect to the poly time reductions and it is easy to modify the construction in such a way that $\mathsf{DisjCoNP}$ pairs do not have complete problems with respect to the sub-exponential time reductions, hence as an evidence these new conjectures are true with respect to some oracles.

Theorem 4.2 *The following statements are true:*

1. *If there is no nonuniform subExp-optimal proof system for* TAUT*, then for every* k, $\mathsf{NE}_k \neq \mathsf{CoNE}_k$.

2. *If there is no subExp-optimal proof system for* TAUT*, then for every* k, $\mathsf{E}_k \neq \mathsf{NE}_k$.

3. *If there is no nonuniform Qp-optimal proof system for* TAUT*, then* $\mathsf{NEXP} \neq \mathsf{CoNEXP}$.

4. *If there is no Qp-optimal proof system for* TAUT*, then* $\mathsf{EXP} \neq \mathsf{NEXP}$.

Proof. Here we only prove the statement (1). The proof of the other statements is similar. Let $\mathsf{NE}_k = \mathsf{CoNE}_k$ for some $k > 0$. Define the following complete languages:

1. $L_{\mathsf{NE}_k} = \{n = \langle e, x, m\rangle \in \mathbb{N} : \mathbb{N} \models \mu_1(e, x, 2^{|m|}_{k+1})\} \in \mathsf{NE}_k$-complete,

2. $L_{\mathsf{CoNE}_k} = \{n = \langle e, x, m\rangle \in \mathbb{N} : \mathbb{N} \models \neg\mu_1(e, x, 2^{|m|}_{k+1})\} \in \mathsf{CoNE}_k$-complete.

By definition there exist the following predicates:

1. There exists a NP predicate U_{NP} such that $\mathbb{N} \models \forall n(\mathsf{U}_{\mathsf{NP}}(2^n_k) \leftrightarrow n \in L_{\mathsf{NE}_k})$,

2. There exists a CoNP predicate $\mathsf{U}_{\mathsf{CoNP}}$ such that $\mathbb{N} \models \forall n(\mathsf{U}_{\mathsf{CoNP}}(2^n_k) \leftrightarrow n \in L_{\mathsf{CoNE}_k})$.

Note that $\mathsf{NE}_k = \mathsf{CoNE}_k$ implies that there exists a linear time function f such that

$$\mathbb{N} \models \forall n(\mathsf{U}_{\mathsf{CoNP}}(2^n_k) \leftrightarrow \mathsf{U}_{\mathsf{NP}}(2^{f(n)}_k)).$$

Let $T \in \mathcal{T}$ be a theory with the following properties:

1. $T \vdash \mathsf{U}_{\mathsf{NP}}(2^n_k)$ is NE_k-complete with respect to the poly time reductions,

2. $T \vdash \mathsf{U}_{\mathsf{CoNP}}(2^n_k)$ is CoNE_k-complete with respect to the poly time functions,

3. $T \vdash \forall n(\mathsf{U}_{\mathsf{CoNP}}(2^n_k) \leftrightarrow \mathsf{U}_{\mathsf{NP}}(2^{f(n)}_k))$

Let T' be in $\mathcal{T}$. For every i, define $\mathsf{Con}^i_{T'}(x) := \forall y(|y|_i \leq x \to \neg Pr_{T'}(y, \ulcorner\bot\urcorner)$, hence $\mathsf{Con}^k_{T'}(x) \in \mathsf{CoNE}_k$. So by mentioned properties of T there exists a linear time function g such that $T \vdash \forall n\big(\mathsf{Con}^k_{T'}(n) \leftrightarrow \mathsf{U}_{\mathsf{NP}}(2^{f(g(n))}_k)\big)$. Because $\mathsf{U}_{\mathsf{NP}}(x)$ is Σ^b_1 and also $\mathsf{S}^1_2 \subseteq T$, there exists a polynomial $r(x)$ such that

$$T \vdash \forall x\big(\mathsf{U}_{\mathsf{NP}}(x) \to \exists y\big(|y| \leq r(|x|) \wedge Pr_T\big(y, \ulcorner\mathsf{U}_{\mathsf{NP}}(\dot{x})\urcorner\big)\big)\big).$$

This implies

$$T \vdash \forall x\big(\mathsf{U}_{\mathsf{NP}}(2^{f(g(x))}_k) \to \exists y\big(|y| \leq r(2^{f(g(x))}_{k-1} + 1) \wedge Pr_T\big(y, \ulcorner\mathsf{U}_{\mathsf{NP}}(2^{f(g(\dot{x}))}_k)\urcorner\big)\big)\big).$$

Note that $\mathbb{N} \models \forall n \mathsf{U}_{\mathsf{NP}}(2^{f(g(n))}_k)$, so for every $n \in \mathbb{N}$, $T \vdash^{r(2^{f(g(n))}_{k-1}+1)} \mathsf{U}_{\mathsf{NP}}(2^{f(g(\bar{n}))}_k)$, hence there exists a polynomial $p(x)$ such that for every $n \in \mathbb{N}$, $T \vdash^{p(2^{f(g(n))}_{k-1})} \mathsf{Con}^k_{T'}(\bar{n})$, hence $T \vdash^{p(2^{f(g(|n|_{k-1}))}_{k-1})} \mathsf{Con}^k_{T'}(|\bar{n}|_{k-1})$, so there exists a polynomial $q(x)$ such that for every $n \in \mathbb{N}$, $T \vdash^{q(2^{f(g(|n|_{k-1}))}_{k-1})} \mathsf{Con}^1_{T'}(\bar{n})$. Note that there exists $0 < \epsilon < 1$ such that $q(2^{f(g(|n|_{k-1}))}_{k-1}) = O(2^{n^\epsilon})$. By the fact that proof of theorem 2.3 is adoptable in case of quasi polynomial and subexponential the proof is completed. ■

Note that similar theorems can be proved for $\mathsf{RFN}^{\mathsf{N}}_1$ and RFN_1. The main problem in the theorem 4.2 that does not permit us to prove that nonexistence of nonuniform p-optimal proof systems implies separation of NE_k and CoNE_k for $k > 1$ is that these classes are not closed under reductions, but we can separate these classes if we strengthen our assumption like the following theorem.

Theorem 4.3 *Let $k > 0$, then at least one of the following statement is true:*

1. *There is no recursive function $F(x)$ such that*

$$\mathbb{N} \models \forall e, x(\neg\mu_1(e, 2^x_k, 2^{(2^x_{k-1}+1)^e}) \leftrightarrow \mu_1(F(e), 2^x_k, 2^{(2^x_{k-1}+1)^{F(e)}})),$$

2. *There is no nonuniform p-optimal proof system for* TAUT.

Also, a similar statement is true for p-optimality and equality of E_k *and* NE_k.

Proof. Let (1) be false. This implies that we can find a theory $T \in \mathcal{T}$ such that it effectively prove $\mathsf{NE}_k = \mathsf{CoNE}_k$ and because T is Σ_1-complete, T can prove $\mathsf{Con}^k_{T'}(x)$ for some $T' \in \mathcal{T}$ is equivalent to $\phi(2^x_k)$ for some $\phi \in \Sigma^b_1$. The rest of the proof is like the proof of theorem 4.2. ∎

Theorem 4.3 has interesting corollaries.

Corollary 4.4 *The following statements are true:*

1. *If there is no nonuniform p-optimal proof system for* TAUT, *then for every $T \in \mathcal{T}$ and for every $k > 0$, there is a Π^b_1 formula ϕ such that for every Σ^b_1 formula ψ, $T \not\vdash \forall n(\phi(2^n_k) \leftrightarrow \psi(2^n_k))$.*

2. *If there is no p-optimal proof system for* TAUT, *then for every $T \in \mathcal{T}$ and for every $k > 0$, there is a Δ^b_1 formula ϕ in S^1_2 such that for every Σ^b_1 formula ψ, $T \not\vdash \forall n(\phi(2^n_k) \leftrightarrow \psi(2^n_k))$.*

Proof. The following argument is working for both cases. Suppose k is fixed. If there is a $T \in \mathcal{T}$ such that for every Π^b_1 formula ϕ, there exists a Σ^b_1 formula ψ such that $T \vdash \forall n(\phi(2^n_k) \leftrightarrow \psi(2^n_k))$, then the following algorithm defines a recursive function, by giving an input e, enumerate all T-proofs and for every proof check whether it is a T-proof of $\forall n(\neg\mu_1(e, 2^x_k, 2^{(2^x_{k-1}+1)^e}) \leftrightarrow \phi(2^n_k))$ for some Σ^b_1 formula ϕ. Note that this enumeration and checking process is recursive because the axioms of T are poly time decidable, also, note that by assumption this algorithm always find such a ψ, hence we can find its code and output it, hence by theorem 4.3 there is a nonuniform p-optimal proof system. ∎

The next corollary shows that theorem 4.3 implies conditional independence for strong intuitionistic theories.

Corollary 4.5 *Let T be an intuitionistic theory such that any arithmetical theorem of T is recursive realizable, then:*

1. *If there is no nonuniform p-optimal proof system for* TAUT, *then for every $k > 0$, $T \nvdash \mathsf{NE}_k = \mathsf{CoNE}_k$,*

2. *If there is no p-optimal proof system for* TAUT, *then for every $k > 0$, $T \nvdash \mathsf{E}_k = \mathsf{NE}_k$.*

Proof. If $T \vdash \mathsf{NE}_k = \mathsf{CoNE}_k$ for some $k > 0$, it actually give us a recursive function $F(x)$ such that $\mathbb{N} \models \forall e, x(\neg\mu_1(e, 2^x_k, 2^{(2^x_{k-1}+1)^e}) \leftrightarrow \mu_1(F(e), 2^x_k, 2^{(2^x_{k-1}+1)^{F(e)}}))$ by recursive realizability, hence by theorem 4.3 it implies the existence of a nonuniform p-optimal proof system for TAUT. Proof of the second statement is similar. ∎

Note that arithmetical theorems of strong intuitionistic theories like HA (Heyting Arithmetic), CZF (Constructive Zermelo-Fraenkel) and IZF (Intuitionistic Zermelo-Fraenkel) are recursively realizable. For more information about soundness of these theories with respect to the recursive realizability see [12] and [13].

5 Relativized Worlds

In this section we will construct two oracles that imply several separations between conjectures of the two branches in figure 1. Our constructions are based on usual definition of forcing in arithmetic.

Definition 5.1 *A nonempty set $\mathcal{P}$ of functions from natural numbers to $\{0,1\}$ (for every $p \in \mathcal{P}$, $D_p \subseteq \mathbb{N}$ and $R_p \subseteq \{0,1\}$) is a forcing notion iff for every $p \in \mathcal{P}$, there exists a $q \in \mathcal{P}$ such that $p \subsetneq q$. We call members of a forcing notation, condition.*

Let α be a new unary relation symbol. For every $p \in \mathcal{P}$ and every $\mathcal{L}_{BA}(\alpha)$ sentence ϕ we will define $p \Vdash \phi$ by induction on complexity of ϕ as follow:

1. $p \nVdash \bot$,

2. $p \Vdash s = t$, if $\mathbb{N} \models s = t$,

3. $p \Vdash \alpha(n)$ for some $n \in \mathbb{N}$, if $p(n) = 1$,

4. $p \Vdash \psi \wedge \eta$, if $p \Vdash \psi$ and $p \Vdash \eta$,

5. $p \Vdash \psi \vee \eta$, if $p \Vdash \psi$ or $p \Vdash \eta$,

6. $p \Vdash \psi \rightarrow \eta$, if for every $q \in \mathcal{P}$ that $p \subseteq q$, if $q \Vdash \psi$, then $q \Vdash \eta$,

7. $p \Vdash \exists x\psi(x)$, if there exists $n \in \mathbb{N}$ such that $p \Vdash \psi(n)$,

8. $p \Vdash \forall x\psi(x)$, if for every $q \in \mathcal{P}$ that $p \subseteq q$ and for every $n \in \mathbb{N}$, $q \Vdash \psi(n)$.

For the next theorem we use the forcing notion $\mathcal{P} = \{p : p \text{ is a finite function from } \mathbb{N} \text{ to } \{0,1\}\}$. Since we use functions as the forcing conditions, we show domain of function f by notation D_f. In the rest of the paper we use notation $[n] = \{0, 1, ..., n\}$. Also, by t_A for some computational machine A (FP functions, Σ^b_i relations, etc) we mean the time complexity of A.

Theorem 5.1 *There exists an oracle $\mathcal{V}$ such that $\mathsf{DisjCoNP}^{\mathcal{V}}$ is true, but $\mathsf{E}^{\mathcal{V}} = \mathsf{NE}^{\mathcal{V}}$.*

Proof. Let $(\phi_{f(n)}, \psi_{g(n)}, R_{h(n)})$ be an enumeration of $\Pi^b_1(\alpha) \times \Pi^b_1(\alpha) \times \mathsf{FP}^\alpha$. We want to construct a sequence $p_0 \subseteq p_1 \subseteq p_2 \subseteq ...$ of $\mathcal{P}$ such that $\mathcal{V} = \bigcup_i p_i^{-1}(1)$ and $\mathsf{DisjCoNP}^{\mathcal{V}}$ is true, but $\mathsf{E}^{\mathcal{V}} = \mathsf{NE}^{\mathcal{V}}$ if α is interpreted by $\mathcal{V}$.

For every i, j define the following $\Pi^b_1(\alpha)$ sets:

1. $L^1_{(i,j)} = \{n : \forall |y| = |n| (2\left\langle 2^i, 2^j, 1, n, y \right\rangle \in \alpha)\}$,
2. $L^2_{(i,j)} = \{n : \forall |y| = |n| (2\left\langle 2^i, 2^j, 2, n, y \right\rangle \in \alpha)\}$.

Let L_{NE} be the relativized version of NE-complete problem defined in theorem 4.1 and $\mathsf{U_{NP}}(x)$ be a $\Sigma^b_1(\alpha)$ predicate such that

$$(\mathbb{N}, A) \models \forall n (n \in L \leftrightarrow \mathsf{U_{NP}}(2^n)).$$

for every A. Let $t_{\mathsf{U_{NP}}}(n) \leq n^c + c$ for some $c > 0$. We want to code membership of L in $\mathcal{V}$ such that

$$(\mathbb{N}, \mathcal{V}) \models \forall n (n \in L \leftrightarrow 2^{(n+1)^c + c} + 1 \in \alpha).$$

Note that $\mathsf{U_{NP}}(2^n)$ can not query $2^{(n+1)^c+c} + 1$. Suppose we construct $p_{i-1} : \mathcal{M}_{i-1} \to \{0, 1\}$. Let n be big enough (We compute how big should n be). Suppose $\max(t_{\phi_{f(i)}}(n), t_{\psi_{g(i)}}(n), t_{R_{h(i)}}(n)) \leq n^d + d$. Define $p_{i-1} \subseteq q$ as follow:

1. $D_q \subseteq [2^{n^d+d}]$,
2. $\{2\left\langle 2^{f(i)}, 2^{g(i)}, v, x, y \right\rangle : |x| = |y| = n, v \in \{1, 2\}\} \cap D_q = \varnothing$,
3. $(D_q \setminus D_{p_{i-1}}) \cap \{2^{(m+1)^c+c} + 1 : m \in \mathbb{N}\} = \varnothing$,
4. $\{2\left\langle 2^a, 2^b, v, x, y \right\rangle : a, b, x, y \in \mathbb{N}, v \in \{1, 2\}, |x| = |y|, |x| \neq n\} \setminus D_{p_{i-1}} \subseteq q^{-1}(0)$

Now we want to extend q to make sure the coding requirement. Let $u_0 = q$. For each $j > 0$ such that $2^{(j+1)^c+c} + 1 < 2^{n^d+d}$ we construct u_j by the following rules:

1. If $2^{(j+1)^c+c} + 1 \in D_{u_{j-1}}$, then put $u_j = u_{j-1}$,
2. otherwise,
   (a) If $u_{j-1} \Vdash \neg \mathsf{U_{NP}}(2^j)$, put $u_j = u_{j-1} \cup \{(2^{(j+1)^c+c} + 1, 0)\}$.
   (b) otherwise, extend u_{j-1} to u_j such that:
      - $u_j \Vdash \mathsf{U_{NP}}(2^j)$,
      - $2^{(j+1)^c+c} + 1 \in u_j^{-1}(1)$,
      - $|u_j \setminus u_{j-1}| \leq (j+1)^c + c + 1$, we can force this condition because only we need to know the queries of $\mathsf{U_{NP}}(2^j)$ in its accepting path.

Let q' be unions of u_j for $2^{(j+1)^c+c} + 1 < 2^{n^d+d}$. For each x such that $|x| = n$, define $S_x = \{2\left\langle 2^{f(i)}, 2^{g(i)}, v, x, y\right\rangle : |y| = n, v \in \{1, 2\}\}$. Let $k = |\{j \in \mathbb{N} : 2^{(j+1)^c+c} + 1 < 2^{n^d+d}\}|$, therefore we have :

$$|q' \setminus q| \leq \sum_{j=0}^{k-1} (j+1)^c + c + 1 \leq k(k^c + c + 1)$$

. Because $k \leq (n^d+d-c)^{\frac{1}{c}}$, we have $|q' \setminus q| \leq (n^d+d-c)^{\frac{1}{c}}(n^d+d+1)$. If n be big enough, then $\max\{(n^d + d - c)^{\frac{1}{c}}(n^d + d + 1), 3(n^d + d)\} < 2^n$ which means there exists z with length of n such that $S_z \cap D_{q'} = \varnothing$. Note that by our construction $q' \nVdash \exists x(x \in L^1_{(f(i),g(i))} \wedge x \in L^2_{(f(i),g(i))})$. Now we have enough rooms to extend q' in such a way that either $(\phi_{f(i)}, \psi_{g(i)})$ is not disjoint or $(L^1_{(f(i),g(i))}, L^2_{(f(i),g(i))})$ is not reducible to $(\phi_{f(i)}, \psi_{g(i)})$ by $R_{h(i)}$. We compute $R_{h(i)}(2^n - 1)$ and answer new oracle questions by the following rule:

1. For oracle question y, if $y \in S_z$, then accept y and put y in $\mathcal{A}$,
2. if $(y, 1) \in q'$ accept y,
3. otherwise, reject y.

Let $R_{h(i)}(2^n - 1) = x$. Let $\mathcal{P}^* \subseteq \mathcal{P}$ such that for every $u \in \mathcal{P}^*$, the following properties are true:

1. $D_u \subseteq [2^{n^d+d}]$,
2. $u|_{D_{q'}} = q'$,
3. $\mathcal{A} \subseteq u^{-1}(1)$,
4. $u^{-1}(0) \cap S_z = \varnothing$,
5. $(F \setminus (S_z \cup D_{q'})) \subseteq u^{-1}(0)$,
6. $|D_u \cap S_z| \leq 2(n^d + d)$,

Now there are two cases that can occur:

1. If for every $u \in \mathcal{P}^*$, $u \nVdash \neg\phi_{f(i)}(x)$ and also $u \nVdash \neg\psi_{g(i)}(x)$, then define $p' : [2^{n^d+d}] \to \{0, 1\}$ by the following definition:

   $$p'(m) = \begin{cases} q'(m) & m \in D_{q'} \\ 1 & m \in S_z \\ 0 & \text{o.w.} \end{cases}$$

   Note that $p' \nVdash \neg\phi_{f(i)}(x)$ and also $p' \nVdash \neg\psi_{g(i)}(x)$, because if for example $p' \Vdash \neg\phi_{f(i)}(x)$, then there exists a subset $F \subseteq [2^{n^d+d}]$ such that $p'|_F \in \mathcal{P}^*$ and $p'|_F \Vdash \neg\phi_{f(i)}(x)$ which contradicts our assumption, hence $p' \nVdash \neg\phi_{f(i)}(x)$ and also $p' \nVdash \neg\psi_{g(i)}(x)$, but this implies $p' \Vdash \phi_{f(i)}(x) \wedge \psi_{g(i)}(x)$, because p' have answer of oracle questions for all of numbers with length of less than $n^d + d + 1$. This means that $\phi_{f(i)}$ and $\psi_{g(i)}$ are not disjoint relative to our oracle construction and we define p_i as p'.

2. otherwise, without loss of generality we can assume that there exists a $u \in \mathcal{P}^*$ such that $u \Vdash \neg\phi_{f(i)}(x)$. Let $S = \{2\left\langle 2^{f(i)}, 2^{g(i)}, 1, z, y\right\rangle : |y| = n\}$ and define p_i as a condition by the following properties:

   (a) $D_{p_i} = [2^{n^d+d}]$,

   (b) $u \subseteq p_i$,

   (c) $S \subseteq p_i^{-1}(1)$,

   (d) $[2^{n^d+d}] \setminus (D_u \cup S) \subseteq p_i^{-1}(0)$.

   therefore we have the following facts:

   (a) $p_i \Vdash \neg\phi_{f(i)}(x)$,

   (b) $p_i \Vdash 2^n - 1 \in L^1_{(f(i),g(i))}$

   This implies that $(L^1_{(f(i),g(i))}, L^2_{(f(i),g(i))})$ is not reducible to $(\phi_{f(i)}, \psi_{g(i)})$ by $R_{f(i)}$ relative to our oracle construction.

By explanations of the above cases our oracle construction is completed. ■

In the rest of the paper we want to construct an oracle $\mathcal{W}$ such that $\mathsf{TFNP}^{\mathcal{W}} = \mathsf{FP}^{\mathcal{W}}$, but there is no nonuniform p-optimal proof system for $\mathsf{TAUT}^{\mathcal{W}}$. We will use the Kolmogorov generic construction idea that is defined in [14]. Here we borrow definitions and notation from [14]. Note that because we explained how to code binary strings in natural numbers and vice versa, we use both natural numbers and strings in the rest of the paper without loss of generality.

Definition 5.2 *For every partial computable function $F(x, y)$ and every $x, y \in \{0, 1\}^*$, the Kolmogorove complexity of x conditional to y with respect to the F which it will be shown by $C_F(x|y)$ is defined as follows:*

$$C_F(x|y) = \min\{|e| : e \in \{0, 1\}, F(e, y) = x\}$$

We will say that $C_F(x|y)$ for some partial computable function $F(x, y)$ is universal method iff for every partial computable $G(x, y)$, there exists a constant k such that

$$\forall x, y \in \{0, 1\}^*(C_F(x|y) \leq C_G(x|y) + k).$$

According to Solomonoff-Kolmogorov theorem there exists a universal method. We will show it by $C(x|y)$. Also, we define the unconditional Kolmogorov complexity of x with $C(x) = C(x|\lambda)$ in which λ is the empty string. Here we list some properties of Kolmogorov complexity that are stated in [14].

1. For all x and y, $C(x|y) \leq C(x) + O(1)$,

2. There exists a constant k such that for all x, $C(x) \leq |x| + k$,

3. For all n and m, there is a n bit string x such that $C(x) \geq n - m$. In particular, for every n there is a n bit string x such that $C(x) \geq n$. Such strings are called incompressible.

4. For every computable function $f(x_1, ..., x_n)$,
$$C(f(x_1, ..., x_n)) \leq 2|x_1| + 2|x_2| + ... + 2|x_{n-1}| + |x_n| + O(1)$$

For every $n > 0$ fix a $n2^n$ bit string Z_n such that $C(Z_n) \geq n2^n$. Divide Z_n into 2^n string z_1^n to $z_{2^n}^n$, each of length n. Define $\mathcal{K} = \{\llcorner \langle i, z_i^j \rangle \lrcorner : \exists k \in \mathbb{N}(j = 2_k^1), i \in \{0,1\}^j\}$. We define forcing notion $\mathcal{P}_K = \{p : p \text{ is a function from } \mathcal{K} \text{ to } \{0,1\}, \mathcal{K} \setminus D_p \text{ is infinite}\}$.

Theorem 5.2 *There exists an oracle $\mathcal{W}$ such that there is no nonuniform p-optimal proof system for $\mathsf{TAUT}^{\mathcal{W}}$, but $\mathsf{TFNP}^{\mathcal{W}} = \mathsf{FP}^{\mathcal{W}}$.*

Proof. Following the argument in [14], we construct an oracle $\mathcal{W}$ such that there is no nonuniform p-optimal proof system for $\mathsf{TAUT}^{\mathcal{W}}$, but $\mathsf{TFNP}^{\mathcal{W}} = \mathsf{FP}^{\mathcal{W}}$, assuming $\mathsf{FP} = \mathsf{FPSPACE}$. As we will see, the oracle construction still works if we first relativize things with a PSPACE-complete set H and then construct $\mathcal{W}$ with the desired properties. Note that relativizing to H implies $\mathsf{FP}^H = \mathsf{FPSPACE}^H$ and hence we are free from the assumption $\mathsf{FP} = \mathsf{FPSPACE}$. Also, note that relativizing first to H and then relativizing to $\mathcal{W}$ is equivalent to relativizing with $H \oplus \mathcal{W}$ in which $A \oplus B = \{2n : n \in A\} \cup \{2n+1 : n \in B\}$. Let $\{f_i(x)\}_{i \in \mathbb{N}}$ and $\{(r_i, \phi_i(x,y))\}_{i \in \mathbb{N}}$ be an enumeration of $\mathsf{FP}(\alpha)$ functions and $\mathbb{N} \times \Delta_1^b(\alpha)$ in which $\phi_i(x,y)$ defines a poly time relation with access to α. In the rest of the proof we construct a sequence $p_0 \subseteq p_1 \subseteq ...$ of $\mathcal{P}_K$ such that $\mathcal{W} = \bigcup_i p_i^{-1}(1)$ and there is no nonuniform p-optimal proof system for $\mathsf{TAUT}^{\mathcal{W}}$, but $\mathsf{TFNP}^{\mathcal{W}} = \mathsf{FP}^{\mathcal{W}}$ if α is interpreted by $\mathcal{W}$. For every $i, k \in \mathbb{N}$ define $\theta_{i,k}$ be the usual relativiezed propositional translation of $\Pi_1^b(\alpha)$ sentence $\forall x(|x| = \bar{3}\bar{n} + \bar{3} \to \neg\alpha(x))$ in which $n = 2_{\langle i,k \rangle}^1$. For every $i, j \in \mathbb{N}$ define $S_j^i = \{\theta_{i,k} : k \geq j\}$ and $B_j^i = \{x : x \in \mathcal{K}, |x| = 3(2_{\langle i,j \rangle}^1 + 1)\}$. Suppose we construct $p_{i-1} : M_{i-1} \to \{0,1\}$. We extend p_{i-1} to p_i as follow:

1. If $i = 2a$, then we want to make sure that f_a will not be a proof system or f_a will not have short proofs for members of the set $S_{c_a}^a$ for some c_a relative to $\mathcal{W}$. Let $t_{f_a} \leq n^d + d$. Choose c_a such that $D_{p_{i-1}} \cap \left(\bigcup_{c_a \leq j} B_j^a\right) = \varnothing$ and also for every $m \geq c_a$, $4md^{d \log_2 4m} + d < 2^m$. Now, there are two cases that can happen:

   (a) There is a $p_{i-1} \subseteq q \in \mathcal{P}_K$, some $\theta \in S_{c_a}^a$ and $\pi \in \mathbb{N}$ such that
   $$q \Vdash |\pi| \leq |\theta|^{d \log_2 |\theta|} + d \wedge f_a(\pi) = \theta.$$
   This implies that there is a $p_{i-1} \subseteq q' \in \mathcal{P}_K$ such that $|D_{q'} \setminus D_{p_{i-1}}| \leq |\theta|^{d \log_2 |\theta|} + d$ and $q' \Vdash |\pi| \leq |\theta|^{d \log_2 |\theta|} + d \wedge f_a(\pi) = \theta$, because f_a only needs at most $|\theta|^{d \log_2 |\theta|} + d$ query answers from $\mathcal{W}$ on input π. Let θ be $\theta_{a,k}$ for some k. This means $|\theta|^{d \log_2 |\theta|} + d < |B_k^a| = 2^n$ in which $n = 2_{\langle a,k \rangle}^1$, hence there is a $z \in B_k^a \setminus D_{q'}$. Define $p_i := q' \cup \{(z, 1)\}$. This implies that f_a relative to $\mathcal{W}$ will not be a proof system for $\mathsf{TAUT}^{\mathcal{W}}$, because it proves $\theta_{a,k}$, but $\theta_{a,k}$ is not a tautology relative to $\mathcal{W}$.

(b) otherwise, we define $p_i := p_{i-1} \cup \{(x, 0) : \exists k \in \mathbb{N}(k \geq c_a \wedge x \in B^a_k)\}$. Note that in this case, for every $\theta \in S^a_{c_a}$, there is no $|\theta|^{d \log_2 |\theta|} + d$ length proof of θ in f_a relative to $\mathcal{W}$.

So by construction of p_i we make sure that f_a is not a proof system or f_a is not a nonuniform p-optimal proof system for $\mathsf{TAUT}^{\mathcal{W}}$, because $S^a_{c_a}$ is poly time decidable.

2. If $i = 2a + 1$, then we want to make sure that $(n^{r_a} + r_a, {}_a(x, y))$ will not define a TFNP problem relative to $\mathcal{W}$ or it can be computed by some function in $\mathsf{FP}^{\mathcal{W}}$. The construction in this case is very easy. If there is a $p_{i-1} \subseteq q \in \mathcal{P}_K$ such that $q \Vdash \exists x \forall y(|y| \leq |x|^{r_a} + r_a \to \neg\phi_a(x, y))$, then there is some $p_{i-1} \subseteq q' \in \mathcal{P}_K$ such that $|D_{q'} \setminus D_{p_{i-1}}|$ is finite and $q' \Vdash \exists x \forall y(|y| \leq |x|^{r_a} + r_a \to \neg\phi_a(x, y))$. In this case we define $p_i := q'$, otherwise if there is no such extension, then we define $p_i := p_{i-1}$.

Suppose $(n^{r_a} + r_a, \phi_a(x, y))$ defines a TFNP problem relative to $\mathcal{W}$. Now we want to show there is a function $f \in \mathsf{FP}^{\mathcal{W}}$ such that it solves $(n^{r_a} + r_a; \phi_a(x, y))$. Let $t_{\phi_a} \leq (|x| + |y|)^b + b$, then on input u with solution v, $\phi_a(u, v)$ asks at most $(|u| + |u|^{r_a} + r_a)^b + b$ questions from $\mathcal{W}$. Choose e such that $(n + n^{r_a} + r_a)^b + b \leq n^e + e$. The function f work as follows on input x:

Let $n = 2^1_k$ be the biggest tower of two such that $n \leq 4|x|^{2e}$. Note that for computing a solution of this problem we only need to know the oracle answers for members $\bigcup_{i \leq n} Y_i$. First, f asks the value of $\mathcal{W}$ for every member of $\bigcup_{i \leq \log_2 n} Y_i$ and put the answers in G. Then it proceeds as the following procedure by starting with $Q_1 = \varnothing$: In the i'th iteration, using the power of PSPACE (we assumed that $\mathsf{FP} = \mathsf{FPSPACE}$) find the least $|v_i| \leq |x|^{r_a} + r_a$ such that $\phi_a(x, v_i)$ is true relative to $G \cup Q_i$. If $\phi_a(x, v_i)$ is true relative to $\mathcal{W}$, then halt and output v_i, otherwise there is a $u_i \in (\mathcal{W} \cap Y_n) \setminus Q_i$ such that it is the first number in which it is queried in computation $\phi_a(x, v_i)$ relative to the $\mathcal{W}$ such that $u_i \in \mathcal{W}$, but $u \notin Q_i$. Define $Q_{i+1} = Q_i \cup \{u_i\}$ and repeat this procedure.

First, note that in every iteration, this procedure indeed finds a v such that relative to $G \cup Q_i$, $\phi_a(x, v)$ holds, because in that case we can find a condition $p_i \subset q \in \mathcal{P}_K$ such that $G \cup Q_i \subseteq q^{-1}(1)$ and hence q forces that $(n^{r_a} + r_a, \phi_a(x, y))$ is not a TFNP problem (note that if $Y_n \cap \mathcal{W} = \varnothing$, then we should find actually the solution of the problem relative to $\mathcal{W}$ in the first iteration, hence the construction of the previous conditions that makes sure some proof systems are not nonuniformly p-optimal would not cause a problem in finding such a q), hence after some iterations f will find a solution of this TFNP problem relative to $\mathcal{W}$. If we prove that the number of iterations are polynomial in $|x|$, then we are done. Suppose after l'th iteration we find the solution. This means that $|Q_l| = l - 1$. Let $l' = l - 1$. Note that for every $j < l$, u_j can be described by the code of poly time relation $\phi_a(x, y)$, x, $G \cup Q_j$ and a $e \log_2 |x|$ bit string which it it shows the order number of u_j among queries of $\phi_a(x, v_j)$, hence Q_l can be described by a string of length $l'(e \log_2 |x|) + O(n \log_2 n) + 2|x| + O(1)$ (Note that G has at most $n + \log_2 n + \log_2 \log_2 n + ...$ of strings of length at most $\log_2 n$, hence it can be described by a string of length $O(n \log_2 n)$ bits). Let p be the concatenation of all y's from $\llcorner\langle i, y\rangle\lrcorner \in Y_n \setminus Q_l$ according to the order on i's, hence $|p| = n(2^n l')$. Note that Z_n can be described using p by inserting the second component of members of Q_l in places that the first component refer to, hence by the fact that $C(Q_l) \leq l'(e\log_2|x|) + O(n\log_2 n) + 2|x| + O(1)$, we have:

$$n2^n \leq C(Z_n) \leq n(2^n l') + 2l'(e\log_2|x|) + O(n\log_2 n) + 4|x| + O(1).$$

This implies $l'(n2e\log_2|x|) \leq O(n\log_2 n) + 4|x| + O(1)$. Note that by definition of n, $4|x|^{2e} < 2^n$, hence $2 + 2e\log_2|x| < n$ and this implies $n2e\log_2|x| > 2$, hence $2l' \leq O(n\log_2 n) + 4|x| + O(1)$ which means $l \leq O(4|x|2e\log_2(4|x|^{2e})) + 2|x| + O(1)$ and this completes the proof. ■

It is worth mentioning that the forcing notion that used in [14] is a finite condition forcing, but the forcing notion $\mathcal{P}_K$ permits us to have conditions with an infinite domain. Note that we essentially use this property of $\mathcal{P}_K$ in our construction. We do not know whether (nonuniform) p-optimal proof systems for TAUT exists relative to the original oracle that defined in [14]. Note that the existence of oracles $\mathcal{V}$ and $\mathcal{W}$ imply several separations between conjectures of figure 1. The following corollary shows several independence (not all of the separations) of the conjectures of the branches in the figure 1.

Corollary 5.3 *Define the following sets:*

1. $A = \{\mathsf{CON}, \mathsf{CON}^{\mathsf{N}}\}$,
2. $B = \{\mathsf{SAT}_c, \mathsf{TFNP}_c, \mathsf{DisjCoNP}_c\}$.

Then for every conjecture $Q \in A$ and every conjecture $Q' \in B$, Q and Q' do not imply each other in relativized worlds.

Proof. Follows from theorems 5.1 and 5.2. ■

Acknowledgment

We are indebted to Pavel Pudlák for many invaluable discussions that we have had about this work. We are also grateful to him for his careful readings of the drafts of this paper, his useful comments and suggestions about it and also pointing out many small errors which leads to improvements of presentation. We also thank Michael Rathjen for answering our question about realizability and introducing the reference [13] to us. This research was partially supported by the ERC Advanced Grant 339691 (FEALORA).

References

[1] P. Pudlák, *Incompleteness in finite domain*, Bulletin of Symbolic Logic 23(4), 405-441 (2018)

[2] J. Krajíček, P. Pudlák, *Propositional proof systems, the consistency of first order theories and the complexity of computations*, Journal of Symbolic Logic 54(3), 1063-1079 (1989)

[3] M. Ajtai, *The complexity of the Pigeonhole Principle*, Combinatorica 14(4), 417-433 (1994)

[4] S.R. Buss, *Bounded Arithmetic*, Bibliopolis, Naples (1986)

[5] D. Johnson, C. Papadimitriou, M. Yannakakis, *How easy is local search?*, Journal of Computer and System Sciences 37(1), 79-100 (1988)

[6] A.A. Razborov, *On provably disjoint NP-pairs*, ECCC Technical Report TR94-006 (1994)

[7] P. Hájek, P. Pudlák, *Metamathematics of first order arithmetic*, Springer-Verlag/ASL Perspectives in Logic (1993)

[8] P. Pudlák, *Logical Foundations of Mathematics and Computational Complexity, a gentle introduction*, Springer Monographs in Mathematics, Springer-Verlag (2013)

[9] J. Messner, J. Torán, *Optimal proof systems for propositional logic and complete sets*, Lecture Notes in Computer Science, 477487 (1998)

[10] S. Ben-David, A. Gringauze, *On the Existence of Propositional Proof Systems and Oracle-relativized Propositional Logic*, ECCC Technical Report TR98-021 (1998)

[11] C. Glaßer, A. L. Selman, S. Sengupta, L. Zhang, *Disjoint NP-pairs*, SIAM Journal of Computing, 33(6), 1369-1416 (2004)

[12] A.S. Troelstra, D. van Dalen, *Constructivism in Mathematics*, Volume I, North Holland, Amsterdam, (1988)

[13] M. Rathjen, *Realizability for constructive Zermelo-Fraenkel set theory*, Logic Colloquium 2003, Lecture Notes in Logic 24, 282-314 (2006)

[14] Harry Buhrman, Lance Fortnow, Michal Koucký, John D. Rogers, Nikolay Vereshchagin, *Does the Polynomial Hierarchy Collapse if Onto Functions are Invertible?*, Theory of Computing Systems 46, 143-156 (2010)

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

[16] Sam Buss, Valentine Kabanets, Antonina Kolokolova, and Michal Koucký, *Expander Construction in VNC1*, Innovations in Theoretical Computer Science, (2017)

[17] Søren Riis, *Count(q) versus the pigeon-hole principle*, Archive for Mathematical Logic, 36(3), 157-188 (1997)