On the pigeonhole and the modular counting principles over the bounded arithmetic V^0

Eitetsu Ken,
The Graduate School of Mathematical Sciences,
The University of Tokyo

Abstract

The theorem of Ajtai ([1], improved by [11] and [12]), which shows a superpolynomial lower bound for AC^0-Frege proofs of the pigeonhole principle, was a significant breakthrough of proof complexity and has been inspiring many other important works considering the strengths of modular counting principles and the pigeonhole principle. In terms of bounded arithmetics, the theorem implies that the pigeonhole principle is independent from the bounded arithmetic V^0. Along the stream of researches, [7] gave the following conjectures and showed some sufficient conditions to prove them:

- $V^0 + UCP^{l,d}_k \nvdash injPHP^{n+1}_n$.
- For any prime number p other than 2, $V^0 + oddtown_k \nvdash Count^p_n$.
- For any integer $p \geq 2$, $V^0 + FIE_k \nvdash Count^p_n$.

Here, $injPHP^{n+1}_n$ is a formalization of the pigeonhole principle for injections, $UCP^{l,d}_k$ is the uniform counting principle defined in [7], $Count^p_n$ is the modular counting principle mod p, $oddtown_k$ is a formalization of oddtown theorem, and FIE_k is a formalization of Fisher's inequality.

In this article, we give a summary of the work of [7], supplement both technical parts and motivations of it, and propose the future perspective.

1 Keywords

Proof complexity, AC^0-Frege system, bounded arithmetic, V^0, Ajtai's theorem, Nullstellensatz proof system, pigeonhole principle, modular counting principle, uniform counting principle, general counting principle, oddtown theorem, Fisher's inequality.

2 Introduction

Ajtai's discovery ([1]) of $V^0 \nvdash ontoPHP^{n+1}_n$, where $ontoPHP^{n+1}_n$ is a Σ^B_0-formalization of the statement "there does not exist a bijection between $(n+1)$ pigeons and n holes," was a significant breakthrough in proof complexity. The techniques which were later formalized in [11] as *k-evaluation* and *switching lemma* have been utilized to further works to compare the relative strengths of various types of counting principles (e.g. [2] and [3]). Along the course of the researches, [7][1] gave the following conjectures and showed some sufficient conditions to prove them:

- $V^0 + UCP_k^{l,d} \nvdash injPHP_n^{n+1}$.
- For any integer $p \geq 2$ which is not a power of 2,$V^0 + oddtown_k \nvdash Count_n^p$.
- For any integer $p \geq 2$, $V^0 + FIE_k \nvdash Count_n^p$.

Here, $injPHP_n^{n+1}$ is a formalization of the pigeonhole principle for injections, $UCP_k^{l,d}$ is the uniform counting principle defined in [7], $Count_n^p$ is the modular counting principle mod p, $oddtown_k$ is a formalization of oddtown theorem, and FIE_k is a formalization of Fisher's inequality.

In this article, we give a summary of the work of [7], supplement both technical parts and motivations of it, and propose the future perspective.

To be concrete, the article is organized as follows. In section 3, we prepare the basic notions and notations which we need. In section 4, we summarize the main parts of [7] with some supplements. In section 5, we discuss the outlook of the future research.

3 Preliminaries

Throughout this paper, p and q denote natural numbers. The cardinality of a finite set S is denoted by $\#S$. We prioritize the readability and often use natural abbreviations to express logical formulae. We assume that the reader is familiar with the basics of bounded arithmetics and Frege systems (such as the concepts treated in [6]). Unless stated otherwise, we follow the convention of [6].

As propositional connectives, we use only $\bigvee$ and $\neg$. We assume $\bigvee$ has unbounded arity. When the arity is small, we also use $\vee$ to denote $\bigvee$. We define an abbreviation $\bigwedge$ by

$$\bigwedge_{i=1}^{k} \varphi_i := \neg \bigvee_{i=1}^{k} \neg\varphi_i.$$

When the arity of $\bigwedge$ is small, we also use $\wedge$ to denote it. We give the operators $\bigvee$ and $\bigwedge$ precedence over $\vee$ and $\wedge$ as for the order of application.

Example 1. $\bigwedge_i \varphi_i \vee \bigwedge_j \psi_j$ means $(\bigwedge_i \varphi_i) \vee (\bigwedge_j \psi_j)$.

We also define an abbreviation $\to$ by

$$(\varphi \to \psi) := \neg\varphi \vee \psi.$$

For a set S of propositional variables, an *S-formula* means a propositional formula whose propositional variables are among S. For a set $S = \bigcup_{j=1}^{k} \{s_i^j\}_{i \in I_j}$ of propositional variables

[1] For the latest revised version, see [8].

where each s_i^j is distinct, an S-formula ψ, and a family $\{\varphi_i^j\}_{i\in I_j}$ $(j = 1, \dots, k)$ of propositional formulae,

$$\psi[\varphi_i^1/s_i^1, \cdots, \varphi_i^k/s_i^k]$$

denotes the formula obtained by substituting each φ_i^j for s_i^j simultaneously.

It is well-known that a Σ_0^B $\mathcal{L}_A^2$-formula $\varphi(x_1, \dots, x_k, R_1, \dots, R_l)$ can be translated into a family $\{\varphi[n_1, \dots, n_k, m_1, \dots, m_l]\}_{n_1,\dots,n_k,m_1,\dots,m_l\in\mathbb{N}}$ of propositional formulae (see Theorem VII 2.3 in [6]).

Now, we define several formulae which express so-called "counting principle."

Definition 2. For each $p \geq 2$, let $Count^p(n, X)$ be an $\mathcal{L}_A^2$-formula as follows (intuitively, it says for $n \not\equiv 0 \pmod p$, $[n]$ cannot be p-partitioned):

$$\begin{aligned} Count^p(n, X) := \neg p|n \to \neg((&\forall e \in X.(e < (n+1)^p \to Code(e, n)) \\ &\wedge (\forall k \in [n].\exists e \in X.k \in^* e) \\ &\wedge (\forall e, e' \in X.\neg(e \perp e'))) \end{aligned}$$

Here, $p|n$ is a Σ_0^B formula expressing p divides n. $[n]$ denotes the set $\{1, \dots, n\}$, and we code a p-subset $e = \{e_1 < \cdots < e_p\}$ of $[n]$ by the number $\sum_{i=1}^p e_i(n+1)^{p-i}$, and $Code(e, n)$ is a natural Σ_0^B-predicate saying "e is a code of p-subset of n." The elementship relation $\in^*$ is expressed by a natural Σ_0^B-predicate. $e \perp e'$ means "$e \neq e'$ and $e \cap e' \neq \emptyset$," and it is also expressed by a natural Σ_0^B-predicate.

We also define the propositional formula $Count_n^p$ as in [9]:

$$Count_n^p := \begin{cases} \neg(& \bigwedge_{k\in[n]} \bigvee_{e:k\in e\in[n]^p} r_e \wedge \\ & \bigwedge_{e,e'\in[n]^p:e\perp e'} (\neg r_e \vee \neg r_{e'})) \quad (\text{if } n \not\equiv 0 \pmod p) \\ & 1 \quad (\text{otherwise}) \end{cases}$$

Here, $[n]^p$ denotes the set of all p-subsets of $[n]$, and $\{r_e\}_{e\in[n]^p}$ is a family of distinct propositional variables.

Convention 3. It is easy to see that we may assume $|X| = (n+1)^p$ in $Count^p(n, X)$ over V^0. Furthermore, with suitable identification of propositional variables, $Count^p(x, X)[n, (n+1)^p]$ is equivalent to $Count_n^p$ over AC^0-Frege system modulo polynomial-sized proofs. Thus we often abuse the notation and write $Count_n^p$ for $Count^p(n, X)$.

Definition 4. The Σ_0^B $\mathcal{L}_A^2$-formula $ontoPHP(m, n, R)$ is a natural expression of the statement "If $m > n$, then R does not give a graph of a bijection between $[m]$ and $[n]$," in a similar way as $Count^p(n, X)$. Similarly, the Σ_0^B $\mathcal{L}_A^2$-formula $injPHP(m, n, R)$ is a natural expression of the statement "If $m > n$, then R does not give a graph of an injection from $[m]$ to $[n]$."

We also define the propositional formulae $ontoPHP_n^m$ and $injPHP_n^m$ by

$$ontoPHP_n^m := \begin{cases} \neg(& \bigwedge_{i\in[m]} \bigvee_{j\in[n]} r_{ij} \wedge \bigwedge_{i\neq i'\in[m]} \bigwedge_{j\in[n]} (\neg r_{ij} \vee \neg r_{i'j}) \\ & \wedge \bigwedge_{j\in[n]} \bigvee_{i\in[m]} r_{ij} \\ & \wedge \bigwedge_{j\neq j'\in[n]} \bigwedge_{i\in[m]} (\neg r_{ij} \vee \neg r_{ij'})) \quad (\text{if } m > n) \\ & 1 \quad (\text{otherwise}) \end{cases}$$

and

$$injPHP_n^m := \begin{cases} \neg(& \bigwedge_{i\in[m]} \bigvee_{j\in[n]} r_{ij} \wedge \bigwedge_{i\neq i'\in[m]} \bigwedge_{j\in[n]} (\neg r_{ij} \vee \neg r_{i'j}) \\ & \wedge \bigwedge_{j\neq j'\in[n]} \bigwedge_{i\in[m]} (\neg r_{ij} \vee \neg r_{ij'})) \quad (\text{if } m > n) \\ & 1 \quad (\text{otherwise}) \end{cases}$$

With reasons similar to the one stated in Convention 3, we abuse the notations and use $ontoPHP_n^m$ to denote $ontoPHP(m, n, R)$ and $injPHP_n^m$ to denote $injPHP(m, n, R)$.

The following are well-known:

Theorem 5 ([1], improved by [11] and [12])**.**

$$V^0 \nvdash ontoPHP_n^{n+1}.$$

Here, we follow the following convention.

Convention 6. For Σ_0^B-formulae $\psi_1, \ldots, \psi_l$ and φ, we write

$$V^0 + \psi_1 + \cdots + \psi_l \vdash \varphi$$

to express the fact that the theory $V^0 \cup \{\forall\forall\psi_i \mid i \in [l]\}$ implies $\forall\forall\varphi$. Here, $\forall\forall$ means the universal closure.

We use different parameters to express concrete $\vec{\psi}$ and φ in order to avoid the confusion. We also use letters p, q for fixed parameters of formulae (which is not universally quantified in the theory). For example,

$$V^0 + Count_k^p \nvdash Count_n^q$$

means

$$V^0 + \forall k, X. Count^p(k, X) \nvdash \forall n, X.\ Count^q(n, X),$$

while $V^0 \nvdash UCP_n^{l,d}$ means $V^0 \nvdash \forall l, d, n, R.\ UCP(l, d, n, R)$ (for the definition of $UCP_n^{l,d}$ and $UCP(l, d, n, R)$, see Definition 12).

In the former example, note that we have used the different variables k, n in order to avoid confusions on the dependency of variables.

Theorem 7 ([2])**.** For $p, q \geq 2$, $V^0 + Count_k^p \vdash Count_n^q$ if and only if $\exists N \in \mathbb{N}.\ q \mid p^N$.

Theorem 8 ([3])**.** For any $p \geq 2$, $V^0 + Count_k^p \nvdash injPHP_n^{n+1}$.

Also, the following is a corollary of the arguments given in [9]:

Theorem 9 (essentially in [9])**.** For all $p \geq 2$, $V^0 + injPHP_k^{k+1} \nvdash Count_n^p$.

Remark 10. Note that the exact statement Theorem 12.5.7 in [9] shows is

$$V^0 + ontoPHP_k^{k+1} \nvdash Count_n^p.$$

However, with a slight change of the argument, it is easy to see that Theorem 9 actually holds.

In the proof of Theorem 7 and 8, Nullstellensatz proofs (which is written shortly as "NS-proofs") play an essential role in the arguments. The notion is also utilized in [7], so we set up our terminology on NS-proofs and end this section.

Definition 11. Let R be a commutative ring, and $\mathcal{F}$ be a set of multivariate R-polynomials. For multivariate R-polynomials g_1, g_2 and h_f $(f \in \mathcal{F})$, $\{h_f\}_{f\in\mathcal{F}}$ *is a NS-proof of $g_1 = g_2$ from $\mathcal{F}$* if and only if

$$g_1 - g_2 = \sum_{f\in\mathcal{F}} h_f f.$$

The *degree* of a NS-proof $\{h_f\}_{f\in\mathcal{F}}$ is defined by $\max_{f\in\mathcal{F}} \deg(h_f)$. Here, we adopt the convention; $\deg 0 := -\infty$.

4 A summary of [7] with some supplements and remarks

In this section, we give a summary of the main works of [7] and supplement some technical parts and intuitions.

4.1 $UCP_k^{l,d}$ v.s. $injPHP_n^{n+1}$

The direct motivation of [7] is Theorem 8. It is tried to make the result uniform with respect to p. In order to formalize the problem, the following "uniform" version of counting principles is defined:

Definition 12. $UCP(l, d, n, R)$ (which stands for *Uniform Counting Principle*) is an $\mathcal{L}_A^2$ formula defined as follows:

$$\begin{aligned}
&(d \geq 1 \wedge \neg d|n) \to \\
\neg[&\forall i \in [l].(\forall j \in [d].\exists e \in [n].R(i,j,e) \vee \forall j \in [d].\neg\exists e \in [n].R(i,j,e)) \\
&\wedge \forall (i,j) \in [l] \times [d].\forall e \neq e' \in [n](\neg R(i,j,e) \vee \neg R(i,j,e')) \\
&\wedge \forall (i,j) \neq (i',j') \in [l] \times [d].\forall e \in [n].(\neg R(i,j,e) \vee \neg R(i',j',e)) \\
&\wedge \forall e \in [n].\exists (i,j) \in [l] \times [d].R(i,j,e)]
\end{aligned}$$

The propositional formula $UCP_n^{l,d}$ is defined as follows:

$$UCP_n^{l,d} := \begin{cases} \neg[\quad \bigwedge_{i=1}^{l} \left(\left(\bigwedge_{j=1}^{d} \bigvee_{e\in[n]} r_{i,j,e} \right) \vee \left(\bigwedge_{j=1}^{d} \neg \bigvee_{e\in[n]} r_{i,j,e} \right) \right) \\ \quad\quad \wedge \bigwedge_{(i,j)\in[l]\times[d]} \bigwedge_{e\neq e'\in[n]} (\neg r_{i,j,e} \vee \neg r_{i,j,e'}) \\ \quad\quad \wedge \bigwedge_{(i,j)\neq(i',j')\in[l]\times[d]} \bigwedge_{e\in[n]} (\neg r_{i,j,e} \vee \neg r_{i',j',e}) \\ \quad\quad \wedge \bigwedge_{e\in[n]} \bigvee_{(i,j)\in[l]\times[d]} r_{i,j,e}] \quad (\text{if } n \not\equiv 0 \pmod{d},\ d \geq 1) \\ \quad\quad 1 \quad (\text{otherwise}) \end{cases}$$

As in the previous definitions, we abuse the notation and use $UCP_n^{l,d}$ to express $UCP(l, d, n, R)$.

Intuitively, $UCP_n^{l,d}$ states "if $n \not\equiv 0 \pmod{d}$, then there does not exist a family $\{S_i\}_{i\in[l]}$ which consists of d-sets and emptysets which give a partition of $[n]$." Each variable $r_{i,j,e}$ reads "the j-th element of S_i is e."

We observe the following:

Proposition 13. 1. For any $p \geq 2$, $V^0 + UCP_k^{l,d} \vdash Count_n^p$.

2. $V^0 + UCP_k^{l,d} \vdash ontoPHP_n^m$.

Hence, $UCP_n^{l,d}$ is indeed a generalization of counting principles. Seeing theorem 8, [7] conjectured the following:

Conjecture 1. For any integer $c \geq 1$,

$$F_c + UCP_k^{l,d} \nvdash_{poly(n)} injPHP_n^{n+1}.$$

Here, for a family $\{\alpha_{\vec{k}}\}_{\vec{k}\in\mathbb{N}}$ of propositional formulae, $F_c + \alpha_{\vec{k}}$ is the fragment of Frege system allowing the formulae with depth $\leq c$ only and admitting $\{\alpha_{\vec{k}}\}_{\vec{k}}$ as an axiom scheme. Furthermore, $P \vdash_{poly(n)} \varphi_n$ means each φ_n has a $poly(n)$-sized P-proof.

If this conjecture is true, then it follows that $V^0 + UCP_k^{l,d} \nvdash injPHP_n^{n+1}$ by the witnessing theorem and the translation theorem. By Proposition 13, we can regard the statement as a "uniform" version of Theorem 8.

In [7], the notions *$injPHP$-tree* and *k-evaluations using $injPHP$-trees* are defined, and a sufficient condition to prove Conjecture 1 is shown.

Definition 14. Let D and R be disjoint sets. A *partial injection from D to R* is a set ρ which satisfies the following:

1. Each $x \in \rho$ is either a 2-set having one element from D and one element from R, or a singleton contained in R (in the former case, if $x = \{i, j\}$ where $i \in D$ and $j \in R$, then we use a tuple $\langle i, j\rangle$ to denote x, In the latter case, if $x = \{j\}$ where $j \in R$, then we use 1-tuple $\langle j\rangle$ to denote x).

2. Each pair $x \neq x' \in \rho$ are disjoint.

The 2-sets in a partial injection ρ gives a partial bijection from D to R. We denote it by ρ_{bij}. Also, we set $\rho_{sing} := \rho \setminus \rho_{bij}$.

We define $v(\rho) := \bigcup_{x\in\rho} x$, $\mathrm{dom}(\rho) := v(\rho) \cap D$, and $\mathrm{ran}(\rho) := v(\rho) \cap R$.

For two partial injections ρ and τ from D to R,

1. $\rho || \tau$ if and only if $\rho \cup \tau$ is again a partial injection.

2. $\rho \perp \tau$ if and only if $\rho||\tau$ does not hold. In other words, there exist $x \in \rho$ and $y \in \tau$ such that $x \neq y$ and $x \cap y \neq \emptyset$.

3. $\sigma\tau := \sigma \cup \tau$.

In the following, if there is no problem, we identify domains having the same size n, and denote them D_n. Similarly, we identify ranges R having the same size n, and denote them R_n. We also assume that for every pair m and n, D_m and R_n are mutually disjoint.

Definition 15. For each $m > n$, $\mathcal{M}_n^m$ denotes the set of all partial injections from D_m to R_n.

Definition 16. Let D and R be disjoint finite sets. *$injPHP$-tree over* (D, R) is a vertex-labelled and edge-labelled rooted tree defined inductively as follows:

1. The tree whose only vertex is its root and has no labels is an $injPHP$-tree over (D, R).
2. If the root is labelled by "$i \mapsto ?$" having $|R|$ children and each of its edges corresponding to each label "$\langle i, j\rangle$" $(j \in R)$, and the subtree which the child under the edge labelled by "$\langle i, j\rangle$" induces is an $injPHP$-tree over $(D \setminus \{i\}, R \setminus \{j\})$, then the whole labelled tree is again an $injPHP$-tree over (D, R).
3. If the root is labelled by "$? \mapsto j$" having $(|D| + 1)$ children and each of its edges corresponding to each label "$\langle i, j\rangle$" $(i \in D)$ and "$\langle j\rangle$," and the subtree which the child under the edge indexed by $\langle i, j\rangle$ induces is an $injPHP$-tree over $(D \setminus \{i\}, R \setminus \{j\})$ while the subtree which the the child under the edge labelled by "$\langle j\rangle$" induces is an $injPHP$-tree over $(D, R \setminus \{j\})$, then the whole tree is again an $injPHP$-tree over (D, R).

For an $injPHP$-tree T, we denote *the height* (the maximum number of edges in its branches) of T by $height(T)$ and the set of its branches by $br(T)$.

The pair $(T, L \colon br(T) \to S)$ is called a *labelled $injPHP$-tree with label set S*. For each label $s \in S$, we set $br_s(T) := L^{-1}(s)$.

Convention 17. When T is an $injPHP$-tree over (D, R), each branch $b \in br(T)$ naturally gives a partial injection, which is the collection of labels of edges contained in b. We often abuse the notation and use b to denote the partial injection given by b.

Definition 18. Let Γ be a subformula closed set of $\{r_{ij}\}_{i \in D_m, j \in R_n}$-formulae $(m > n)$. A *k-evaluation (using $injPHP$-trees) of* Γ is a map $T_\cdot \colon \varphi \in \Gamma \mapsto T_\varphi$ satisfying the following:

1. Each T_φ is a labelled $injPHP$-tree over (D_m, R_n) with label set $\{0, 1\}$.
2. T_0 is the $injPHP$-tree with height 0, whose only branch is labeled by 0.
3. T_1 is the $injPHP$-tree with height 0, whose only branch is labeled by 1.
4. $T_{r_{ij}}$ is the $injPHP$-tree over (D_m, R_n) with height 1, whose label of the root is $i \mapsto ?$ and $br_1(T_{r_{ij}}) = \{\langle i, j\rangle\}$.
5. $T_{\neg\varphi} = T_\varphi^c$, that is, $T_{\neg\varphi}$ is obtained from T_φ by flipping the labels 0 and 1.
6. $T_{\bigvee_{i \in I} \varphi_i}$ (where each φ_i does not begin from $\vee$) represents $\bigcup_{i \in I} br_1(T_{\varphi_i})$. Here, we say a $\{0, 1\}$-labelled $injPHP$-tree T represents a set $\mathcal{F}$ of partial injections if and only if the following hold:
   (a) For each $b \in br_1(T)$, there exists a $\sigma \in \mathcal{F}$ such that $\sigma \subset b$.

(b) For each $b \in br_0(T)$, every $\sigma \in \mathcal{F}$ satisfies $\sigma \perp b$.

Theorem 19. Let $f\colon \mathbb{N} \to \mathbb{N}$ be a function satisfying $n < f(n) \leq n^{O(1)}$. Suppose $(\pi_n)_{n\geq 1}$ be a sequence of Frege-proofs such that π_n proves $injPHP_n^{f(n)}$ using $UCP_k^{l,d}$ as an axiom scheme.

Then there cannot be a sequence $(T^n)_{n\geq 1}$ satisfying the following: each T^n is an $o(n)$-evaluation using $injPHP$-trees over $(D_{f(n)}, R_n)$ of Γ_n, where Γ_n is the set of all subformulae appearing in π_n.

Roughly saying, an $injPHP$-tree is a kind of decision tree, and a k-evaluation using $injPHP$-trees is a kind of model of propositional logic, where k is a complexity measure of the model. The theorem can be read that any Frege-proof of $injPHP_n^{f(n)}$ using $UCP_k^{l,d}$ cannot have a simple model.

Hence, we obtain the following;

Corollary 20. Assume $F_c + UCP_k^{l,d} \vdash_{poly(n)} injPHP_n^{n+1}$ is witnessed by AC^0-Frege proofs $(\pi_n)_{n\geq 1}$. Suppose there are partial injections $(\rho_n)_{n\geq 1}$ satisfying

- For each n, $\rho_n \in \mathcal{M}_n^{n+1}$.
- $n - \#\operatorname{ran}(\rho_n) \to \infty$ $(n \to \infty)$.
- There exist $o(n - \#\operatorname{ran}(\rho_n))$-evaluations $(T^n)_{n\geq 1}$ of Γ_n^ρ, where Γ_n is the all subformulae appearing in π_n.

Then we obtain a contradiction.

The condition above is an analogue of the switching lemma used in a standard proof of Ajtai's theorem (see Lemma 15.2.2 and the section 15.7 in [10] for reference and the historical remarks). It seems the proof of that this condition holds is beyond the current proof techniques. The difficulty is relevant to that of the famous open problem; does $V^0 \vdash injPHP_n^{2n}$ hold? For future perspectives, see section 5.

On the other hand, there is a natural generalization of counting principles which also implies $injPHP_n^{n+1}$.

Definition 21. $GCP(P, Q_1, Q_2, R_1, R_2, M_0, M_1, M_2)$ (which stands for *Generalized Counting Principle*) is a Σ_0^B $\mathcal{L}_A^2$-formula expressing the following statement: bounded sets

$$P, Q_1, Q_2, R_1, R_2, M_0, M_1, M_2$$

cannot satisfy the conjunction of following properties:

1. M_0 codes a bijection between $(P \times Q_1) \sqcup R_1$ and $(P \times Q_2) \sqcup R_2$.
2. M_1 is an injection from R_1 to R_2 such that some element $a \in R_2$ is out of its range.
3. M_2 is an injection from R_2 to P such that some element $b \in P$ is out of its range.

Remark 22. We can consider the propositional translation of GCP as well as the previous examples $UCP_n^{l,d}$, $Count_n^p$, etc. However, we do not write it down here because we do not use it this time.

It is easy to see that:

Proposition 23. 1. $V^0 + GCP \vdash UCP_n^{l,d}$.

2. $V^0 + GCP \vdash injPHP_n^{n+1}$.

It is natural to ask:

Question 1. 1. Does the following hold?: $V^0 + UCP_k^{l,d} \vdash GCP$.

2. Is there any other combinatorial principle than GCP which also implies $injPHP_n^{n+1}$ and some of $Count_n^p$?

If the conjecture 1 is true, then the answer to the question 1 is no (since GCP implies $injPHP_n^{n+1}$).

As for question 2, [7] considered oddtown theorem.

4.2 On the strength of oddtown theorem

Oddtown theorem is a combinatorial principle stating that there cannot be $(n+1)$-orthogonal normal vectors in $\mathbb{F}_2^n$. In other words, (regarding each $v \in \mathbb{F}_2^n$ as the characteristic vector of a subset $S \subset [n]$) there cannot be a family $(S_i)_{i\in[n+1]}$ satisfying the following:

- Each S_i has an odd cardinality.
- Each $S_i \cap S_{i'}$ $(i < i')$ has an even cardinality.

Historically, oddtown theorem and Fisher's inequality (introduced in Section 4.3) have been candidates for statements which are easy to prove in extended Frege system but not in Frege system ([4]). However, we still do not know the exact strengths of the principles.

[7] first showed that a natural formalization of oddtown theorem over V^0 is stronger than several combinatorial principles related to counting.

Definition 24. Define the Σ_0^B $\mathcal{L}_A^2$-formula $oddtown(n, P, Q, R, S)$ as follows:

$$\begin{aligned}
&\neg[\forall i \in [n+1].\forall j \in [n].(S(i,j) \leftrightarrow Q(i,j) \vee \exists e \in [n]^2.(j \in^* e \wedge P(i,e)) \\
&\quad \wedge \forall i \in [n+1].\exists j \in [n].Q(i,j) \\
&\quad \wedge \forall i \in [n+1].\forall j \neq j' \in [n].(\neg Q(i,j) \vee \neg Q(i,j')) \\
&\quad \wedge \forall i \in [n+1].\forall j \in [n].\forall e \in [n]^2(j \in^* e \to \neg Q(i,j) \vee \neg P(i,e)) \\
&\quad \wedge \forall i \in [n+1].\forall e \neq e' \in [n]^2(e \cap e' \neq \emptyset \to \neg P(i,e) \vee \neg P(i,e')) \\
&\quad \wedge \forall i < i' \in [n+1].\forall j \in [n].(S(i,j) \wedge S(i',j) \leftrightarrow \exists e \in [n]^2(j \in^* e \wedge R(i,i',e))) \\
&\quad \wedge \forall i < i' \in [n+1].\forall e \neq e' \in [n]^2.(e \cap e' \neq \emptyset \to \neg R(i,i',e) \vee \neg R(i,i',e'))]
\end{aligned}$$

Intuitively, S above gives $S_i := \{j \in [n] \mid S(i,j)\}$, P gives a 2-partition of each S_i leaving one element, which is specified by Q, and R gives a 2-partition of each $S_i \cap S_{i'}$ $(i < i')$.

Definition 25. Define the propositional formula $oddtown_n$ as follows:

$$oddtown_n := \begin{cases} \quad 1 \quad (n=0) \\ \neg[\ \bigwedge_{i\in[n+1]}\bigwedge_{j\in[n]}(\neg s_{ij}\vee q_{ij}\vee\bigvee_{e:j\in e\in[n]^2} p_{ie}) \\ \quad\wedge\bigwedge_{i\in[n+1]}\bigwedge_{j\in[n]}(s_{ij}\vee\neg q_{ij}) \\ \quad\wedge\bigwedge_{i\in[n+1]}\bigwedge_{j\in[n]}\bigwedge_{e:j\in e\in[n]^2}(s_{ij}\vee\neg p_{ie}) \\ \quad\wedge\bigwedge_{i\in[n+1]}\bigvee_{j\in[n]} q_{ij} \\ \quad\wedge\bigwedge_{i\in[n+1]}\bigwedge_{j<j'\in[n]}(\neg q_{ij}\vee\neg q_{ij'}) \\ \quad\wedge\bigwedge_{i\in[n+1]}\bigwedge_{j\in[n]}\bigwedge_{e:j\in e\in[n]^2}(\neg q_{ij}\vee\neg p_{ie}) \\ \quad\wedge\bigwedge_{i\in[n+1]}\bigwedge_{e,e'\in[n]^2:e\perp e'}(\neg p_{ie}\vee\neg p_{ie'}) \\ \quad\wedge\bigwedge_{i<i'\in[n+1]}\bigwedge_{j\in[n]}(\neg s_{ij}\vee\neg s_{i'j}\vee\bigvee_{e:j\in e\in[n]^2} r_{ii'e}) \\ \quad\wedge\bigwedge_{i<i'\in[n+1]}\bigwedge_{j\in[n]}\bigwedge_{e:j\in e\in[n]^2}(s_{ij}\vee\neg r_{ii'e}) \\ \quad\wedge\bigwedge_{i<i'\in[n+1]}\bigwedge_{j\in[n]}\bigwedge_{e:j\in e\in[n]^2}(s_{i'j}\vee\neg r_{ii'e}) \\ \quad\wedge\bigwedge_{i<i'\in[n+1]}\bigwedge_{e,e'\in[n]^2:e\perp e'}(\neg r_{ii'e}\vee\neg r_{ii'e'})] \quad (n\geq 1) \end{cases}$$

By a reason similar to that of Convention 3, we abuse the notation and write $oddtown_n$ to express $oddtown(n, P, Q, R, S)$, too. It quickly turns out that:

Proposition 26. 1. $V^0 + oddtown_k \vdash injPHP^{n+1}_n$.

2. $V^0 + oddtown_k \vdash Count^2_n$.

By theorem 8 and 9, we obtain

Corollary 27.

$$V^0 + injPHP^{k+1}_k \nvdash oddtown_n,$$
$$V^0 + Count^2_k \nvdash oddtown_n.$$

This rases the following natural problems:

Question 2. 1. $V^0 + injPHP^{k+1}_k + Count^2_k \vdash oddtown_n$? How about $V^0 + GCP \vdash oddtown_n$?

2. $V^0 + oddtown_k \vdash Count^p_n$ for which p?

[7] tackled the item 2.

From Proposition 26 and Theorem 7, it is easy to see:

Corollary 28. If p is a power of 2, $V^0 + oddtown_k \vdash Count^p_n$.

[7] conjectured that the converse of this corollary holds. Furthermore, [7] conjectured the following:

Conjecture 2. For each $d \in \mathbb{N}$ and a prime $p \neq 2$, $F_d + oddtown_k \nvdash_{poly(n)} Count^p_n$.

Using Theorem 7, it is easy to see that Conjecture 2 implies the converse of Corollary 28. [7] gave a sufficient condition to prove Conjecture 2:

Theorem 29. *Let $p \in \mathbb{N}$ be a prime other than 2. Suppose $F_d + oddtown_k \vdash_{poly(n)} Count^p_n$. Then there exists a constant $\epsilon > 0$ such that for large enough $n \not\equiv 0 \pmod{p}$, there exists $m \in \mathbb{N}$ and a family $(f_{ij})_{i\in[m+1],j\in[m]}$ of $\mathbb{F}_2$-polynomials such that:*

1. *$m \leq n^{O(1)}$.*
2. *For each $i \in [m+1]$, there exists a NS-proof over $\mathbb{F}_2$ of $\sum_{j\in[m]} f_{ij} + 1 = 0$ from $\neg Count^p_{n^\epsilon}$ with degree $\leq O(\log(n))$ (here, we round n^ϵ to the nearest integer which is not a multiple of p).*
3. *For each $i \neq i' \in [m+1]$, there exists a NS-proof over $\mathbb{F}_2$ of $\sum_{j\in[m]} f_{ij}f_{i'j} = 0$ from $\neg Count^p_{n^\epsilon}$ with degree $\leq O(\log(n))$.*

Here, $\neg Count^p_M$ (where $M \not\equiv 0 \pmod{p}$) means the following system of polynomials:

$$\sum_{e:j\in e\in[M]^p} x_e - 1, x_e x_{e'}, x_e^2 - x_e$$
$$(j \in [M], e, e' \in [M]^p, e \perp e')$$

Hence, if we can prove that such ϵ does not exist, then the Conjecture 2 is true.

Roughly saying, the theorem states the following; if $V^0 + oddtown_k \vdash Count^p_n$, then there exists a constant $\epsilon > 0$ such that for each n, we can construct a vector of $n^{O(1)}$ many $\mathbb{F}_2$-polynomials whose violating oddtown condition can be verified by a NS-proof from $\neg Count^p_{n^\epsilon}$ over $\mathbb{F}_2$ with degree $\leq O(\log(n))$.

4.3 On the strength of Fisher's inequality

When we discuss whether the condition given in Theorem 29 actually holds or not, it is natural to also consider the $\mathbb{K}$-analogue of the condition, where $\mathbb{K}$ is an arbitrary field other than $\mathbb{F}_2$. The next combinatoial principle (see Remark 31 for the informal meaning) relates to a condition which has a similar form to the analogue.

Definition 30 (slightly modified from the version given in [7] [2])**.** We define the Σ^B_0 $\mathcal{L}^2_A$ formula

[2] see Remark 31

$FIE(n, S, R)$ as follows:

$$\begin{array}{l}
\quad FIE(n, S, R) := \\
\neg[\forall i \in [n+1] \exists j \in [n] S(i, j) \\
\wedge \forall i_1 < i_2 \in [n+1] \exists j \in [n]((S(i_1, j) \wedge \neg S(i_2, j)) \vee (\neg S(i_1, j) \wedge S(i_2, j))) \\
\wedge \forall i_1 < i_2 \in [n+1] \forall i'_1 < i'_2 \in [n+1] \forall j \in [n] \\
\quad (\neg S(i_1, j) \vee \neg S(i_2, j) \vee \exists j' \in [n] R(i_1, i_2, i'_1, i'_2, j, j')) \\
\wedge \forall i_1 < i_2 \in [n+1] \forall i'_1 < i'_2 \in [n+1] \forall j' \in [n] \\
\quad (\neg S(i'_1, j) \vee \neg S(i'_2, j) \vee \exists j \in [n] R(i_1, i_2, i'_1, i'_2, j, j')) \\
\wedge \forall i_1 < i_2 \in [n+1] \forall i'_1 < i'_2 \in [n+1] \forall j, j' \in [n] \\
\quad (\neg R(i_1, i_2, i'_1, i'_2, j, j') \vee S(i_1, j)) \\
\wedge \forall i_1 < i_2 \in [n+1] \forall i'_1 < i'_2 \in [n+1] \forall j, j' \in [n] \\
\quad (\neg R(i_1, i_2, i'_1, i'_2, j, j') \vee S(i_2, j)) \\
\wedge \forall i_1 < i_2 \in [n+1] \forall i'_1 < i'_2 \in [n+1] \forall j, j' \in [n] \\
\quad (\neg R(i_1, i_2, i'_1, i'_2, j, j') \vee S(i'_1, j')) \\
\wedge \forall i_1 < i_2 \in [n+1] \forall i'_1 < i'_2 \in [n+1] \forall j, j' \in [n] \\
\quad (\neg R(i_1, i_2, i'_1, i'_2, j, j') \vee S(i'_2, j')) \\
\wedge \forall i_1 < i_2 \in [n+1] \forall i'_1 < i'_2 \in [n+1] \forall j \in [n] \forall j' \neq j'' \in [n] \\
\quad (\neg R(i_1, i_2, i'_1, i'_2, j, j') \vee \neg R(i_1, i_2, i'_1, i'_2, j, j'')) \\
\wedge \forall i_1 < i_2 \in [n+1] \forall i'_1 < i'_2 \in [n+1] \forall j' \in [n] \forall j \neq \widetilde{j} \in [n] \\
\quad (\neg R(i_1, i_2, i'_1, i'_2, j, j') \vee \neg R(i_1, i_2, i'_1, i'_2, \widetilde{j}, j'))]
\end{array}$$

Furthermore, we define the propositional formula FIE_n as follows:

$$\begin{aligned}
FIE_n :=\neg(& \bigwedge_{i\in[n+1]} \bigvee_{j\in[n]} s_{ij} \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigvee_{j\in[n]} ((s_{i_1j} \wedge \neg s_{i_2j}) \vee (\neg s_{i_1j} \wedge s_{i_2j})) \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigwedge_{i'_1<i'_2\in[n+1]} \bigwedge_{j\in[n]} (\neg s_{i_1j} \vee \neg s_{i_2j} \vee \bigvee_{j'\in[n]} r^{i_1,i_2,i'_1,i'_2}_{j,j'}) \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigwedge_{i'_1<i'_2\in[n+1]} \bigwedge_{j'\in[n]} (\neg s_{i'_1j} \vee \neg s_{i'_2j} \vee \bigvee_{j\in[n]} r^{i_1,i_2,i'_1,i'_2}_{j,j'}) \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigwedge_{i'_1<i'_2\in[n+1]} \bigwedge_{j,j'\in[n]} (\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee s_{i_1j}) \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigwedge_{i'_1<i'_2\in[n+1]} \bigwedge_{j,j'\in[n]} (\neg r^{i_1,i_2,i'_1,i'_2\in[n+1]}_{j,j'} \vee s_{i_2j}) \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigwedge_{i'_1<i'_2\in[n+1]} \bigwedge_{j,j'\in[n]} (\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee s_{i'_1j'}) \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigwedge_{i'_1<i'_2\in[n+1]} \bigwedge_{j,j'\in[n]} (\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee s_{i'_2j'}) \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigwedge_{i'_1<i'_2\in[n+1]} \bigwedge_{j\in[n]} \bigwedge_{j'\neq j''\in[n]} (\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee \neg r^{i_1,i_2,i'_1,i'_2}_{j,j''}) \\
\wedge & \bigwedge_{i_1<i_2\in[n+1]} \bigwedge_{i'_1<i'_2\in[n+1]} \bigwedge_{j'\in[n]} \bigwedge_{j\neq\widetilde{j}\in[n]} (\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee \neg r^{i_1,i_2,i'_1,i'_2}_{\widetilde{j},j'}))
\end{aligned}$$

Remark 31. The above formulae are formalizations of Fisher's inequality: there does not exist a family $\{S_i\}_{i\in[n+1]}$ satisfying the following:

- For each i, $\emptyset \neq S_i \subset [n]$.
- For each $i_1 < i_2$, $S_{i_1} \neq S_{i_2}$.
- For each $i_1 < i_2$ and $i'_1 < i'_2$, $\#(S_{i_1} \cap S_{i_2}) = \#(S_{i'_1} \cap S_{i'_2})$.

In the definition of $FIE(n, S, R)$, S intuitively gives a family $\{S_i\}_{i\in[n+1]}$, and R gives a family of bijections

$$\{R^{i_1,i_2,i'_1,i'_2} \colon S_{i_1} \cap S_{i_2} \to S_{i'_1} \cap S_{i'_2}\}_{i_1<i_2 \& i'_1<i'_2}.$$

Note that the condition $\emptyset \neq S_i$ is added to the version given in [7] to make the statement valid in the standard model (if we did not impose the condition, $\{\emptyset, \{1\}, \ldots, \{n\}\}$ would give a counterexample).

It is easy to see that FIE_n is a generalization of the pigeonhole principle.

Proposition 32. $V^0 + FIE_k \vdash injPHP_n^{n+1}$. Hence, for each $p \geq 2$, $V^0 + Count_k^p \nvdash FIE_n$.

It is natural to ask; which p satisfies $V^0 + FIE_k \vdash Count_n^p$?
As for the question, [7] gave the following conjecture:

Conjecture 3. For any $p \geq 2$, $F_c + FIE_k \nvdash_{poly(n)} Count_n^p$. In particular, $V^0 + FIE_k \nvdash Count_n^p$.

We give a slightly modified version of a sufficient condition to prove Conjecture 3 in [7], whose change is along that of the formalization of Fisher's inequality given in Definition 30. We may interpret the following theorem in a similar way as Theorem 29; roughly saying, the theorem states the following; if $V^0 + FIE_k \vdash Count_n^p$, then there exists a constant $\epsilon > 0$ such that for each n, we can construct a vector of $n^{O(1)}$ many $\mathbb{K}$-polynomials whose violating Fisher's inequality can be verified by a NS-proof from $\neg Count_{n^\epsilon}^p$ over $\mathbb{K}$ with degree $\leq O(\log(n))$ (a_{ij} and $b_{i_1 i_2 j}$ work as witnesses of $S_i \neq \emptyset$ and $S_{i_1} \neq S_{i_2}$ in Remark 31).

Theorem 33. Let $\mathbb{K}$ be a field. Suppose $F_d + FIE_k \vdash_{poly(n)} Count_n^p$. Then there exists a constant $\epsilon > 0$ such that for large enough $n \not\equiv 0 \pmod p$, there exists $m \in \mathbb{N}$ and families $(f_{ij})_{i \in [m+1], j \in [m]}$, $(a_{ij})_{i \in [m+1], j \in [m]}$ and $(b_{ii'j})_{i < i' \in [m+1], j \in [m]}$ of $\mathbb{K}$-polynomials satisfying the following:

1. $m \leq n^{O(1)}$.
2. For each $i_1 < i_2 \in [m+1]$ and $i_1' < i_2' \in [m+1]$, there exists a NS-proof of
$$\sum_{j=1}^{m} f_{i_1 j} f_{i_2 j} = \sum_{j=1}^{m} f_{i_1' j} f_{i_2' j}$$
from $\neg Count_{n^\epsilon}^p$ over $\mathbb{K}$ with degree $\leq O(\log(n))$ (note that we round n^ϵ to the nearest integer which is not a multiple of p).
3. For $i \in [m+1]$, there exists a NS-proof of $a_{ij}(1 - f_{ij}) = 0$ from $\neg Count_{n^\epsilon}^p$ over $\mathbb{K}$ with degree $\leq O(\log(n))$.
4. For $i \in [m+1]$, there exists a NS-proof of $\sum_{j=1}^{m} a_{ij} = 1$ from $\neg Count_{n^\epsilon}^p$ over $\mathbb{K}$ with degree $\leq O(\log(n))$.
5. For $i < i' \in [m+1]$ and $j \in [m]$, there exist NS-proofs of $b_{ii'j} f_{ij} f_{i'j} = 0$ and $b_{ii'j}(1 - f_{ij})(1 - f_{i'j}) = 0$ from $\neg Count_{n^\epsilon}^p$ over $\mathbb{K}$ with degree $\leq O(\log(n))$.
6. For each $i < i' \in [m+1]$, there exists a NS-proof of $\sum_{j=1}^{m} b_{ii'j} = 1$ from $\neg Count_{n^\epsilon}^p$ over $\mathbb{K}$ with degree $\leq O(\log(n))$.

Since the conditions 3 and 4 are newly added to the ones given in [7], we give a full proof of the theorem just for sure.

Proof. We adopt the notations in [7]. For readability, we assume $p = 3$. Let proofs $(\pi_n)_{n \in \mathbb{N}}$ witness
$$F_d + FIE_k \vdash_{poly(n)} Count_n^3.$$

Let Γ_n be the set of subformulae of π_n. Apply the switching lemma for 3-tree (cf. Lemma 15.2.2 in [10]), and obtain a constant $\epsilon > 0$ and a restriction ρ_n leaving n^ϵ elements of the universe $[n]$ such that there exists an $O(\log n)$-evaluation T^n of Γ_n^ρ. We fix a large enough $n \not\equiv 0 \pmod p$, and suppress scripts n of T^n, ρ_n, etc. $(Count_n^3)^\rho$ (which can be identified with $Count_{n^\epsilon}^3$) satisfies $T \not\models (Count_n^3)^\rho$ (here, $T \models \varphi$ means $br(T_\varphi) = br_1(T_\varphi)$). Soundness with respect to $\models$ (cf. Lemma 15.1.7 in [10]) gives that some instance

$$I := FIE_m[\sigma_{ij}/s_{ij}, \varphi_{j,j'}^{i_1,i_2,i_1',i_2'}/r_{j,j'}^{i_1,i_2,i_1',i_2'}]$$

satisfies $T \not\models I$. With an additional restriction, we may assume that $br_0(T_I) = br(T_I)$.

We obtain the following :

1. Let $T_i := T_{\bigvee_{j\in[m]}\sigma_{ij}}$. Since

   $$T \models \bigvee_{j\in[m]} \sigma_{ij},$$

   each $b \in br(T_i)$ has at least one $j_b \in [m]$ and $b' \in br_1(T_{\sigma_{ij_b}})$ such that $b' \subset b$. We relabel each branch $b \in br(T_i)$ with $\langle j_b \rangle$ and obtain a labelled $injPHP$-tree $\widetilde{T}_i$.

2. Let $T_{i_1,i_2} := T_{\bigvee_{j\in[m]}((\sigma_{i_1 j}\wedge\neg\sigma_{i_2 j})\vee(\neg\sigma_{i_1 j}\wedge\sigma_{i_2 j}))}$. Since

   $$T \models \bigvee_{j\in[m]} ((\sigma_{i_1 j} \wedge \neg\sigma_{i_2 j}) \vee (\neg\sigma_{i_1 j} \wedge \sigma_{i_2 j})),$$

   each $b \in br(T_{i_1,i_2})$ has at least one j_b satisfying one of the following :

   (a) For all $b' \in br_0(T_{\sigma_{i_1 j_b}}) \cup br_1(T_{\sigma_{i_2 j_b}})$, $b \perp b'$.

   (b) For all $b' \in br_1(T_{\sigma_{i_1 j_b}}) \cup br_0(T_{\sigma_{i_2 j_b}})$, $b \perp b'$.

   We relabel each branch $b \in br(T_{i_1,i_2})$ with $\langle j_b \rangle$ and obtain a labelled $injPHP$-tree $\widetilde{T}_{i_1,i_2}$.

3. Let $T_{1,j}^{i_1,i_2,i_1',i_2'} := T_{\neg\sigma_{i_1 j}\vee\neg\sigma_{i_2 j}\vee\bigvee_{j'\in[m]}\varphi_{j,j'}^{i_1,i_2,i_1',i_2'}}$. Each $b \in br(T_{1,j}^{i_1,i_2,i_1',i_2'})$ is an extension of some element of $br_0(T_{\sigma_{i_1 j}}), br_0(T_{\sigma_{i_2 j}}), \bigcup_{j'} br_1(T_{\varphi_{j,j'}^{i_1,i_2,i_1',i_2'}})$. If b is an extension of an element of $br_1(T_{\varphi_{j,j'}^{i_1,i_2,i_1',i_2'}})$, such j' is unique.

4. Let $T_{2,j'}^{i_1,i_2,i_1',i_2'} := T_{\neg\sigma_{i_1' j}\vee\neg\sigma_{i_2' j}\vee\bigvee_{j\in[m]}\varphi_{j,j'}^{i_1,i_2,i_1',i_2'}}$. Each $b \in br(T_{2,j'}^{i_1,i_2,i_1',i_2'})$ is an extension of an element of $br_0(T_{\sigma_{i_1' j'}}), br_0(T_{\sigma_{i_2' j'}}), \bigcup_j br_1(T_{r_{j,j'}^{i_1,i_2,i_1',i_2'}})$. If b is an extension of an element of $br_1(T_{r_{j,j'}^{i_1,i_2,i_1',i_2'}})$, such j is unique.

Now, we set

$$
\begin{aligned}
f_{ij} &:= \sum_{\alpha \in br_1(T_{\sigma_{ij}})} x_\alpha, \\
a_{ij} &:= \sum_{\alpha \in br_{\langle j \rangle}(\widetilde{T}_i)} x_\alpha \\
b_{i_1 i_2 j} &:= \sum_{\alpha \in br_{\langle j \rangle}(\widetilde{T}_{i_1,i_2})} x_\alpha. \\
&(i \in [m+1], j \in [m])
\end{aligned}
$$

Clearly, $m \leq n^{O(1)}$.

We show that each of the following has a NS-proof from $\neg Count^3_{n^\epsilon}$ over $\mathbb{K}$ with $O(\log(n))$-degree :

$$\sum_{j=1}^{m} a_{ij} = 1, \tag{1}$$

$$\sum_{j=1}^{m} b_{i_1 i_2 j} = 1, \tag{2}$$

$$\sum_{j=1}^{m} f_{i_1 j} f_{i_2 j} = \sum_{j=1}^{m} f_{i'_1 j} f_{i_2 j'}, \tag{3}$$

$$a_{ij}(1 - f_{ij}) = 0, \tag{4}$$

$$b_{i_1 i_2 j} f_{i_1 j} f_{i_2 j} = 0, \tag{5}$$

$$b_{i_1 i_2 j}(1 - f_{i_1 j})(1 - f_{i_2 j}) = 0. \tag{6}$$

$$(i, i_1, i_2, i'_1, i'_2 \in [m+1] \& i_1 < i_2 \& i'_1 < i'_2 \& j \in [m])$$

(1): Since the left-hand side is the sum of all brances of the 3-pratition tree $\widetilde{T}_i$.

(2): Since the left-hand side is the sum of all brances of the 3-pratition tree $\widetilde{T}_{i_1,i_2}$.

(3): We first define $A_{i_1,i_2,j} := T_{\sigma_{i_1 j}} * T_{\sigma_{i_2 j}}$ $(i_1, i_2 \in [m+1], j \in [m], i_1 < i_2)$. Let $B_{i_1,i_2,j}$ be the set of all branches $b \in A_{i_1,i_2,j}$ having the form

$$b = cd^c \quad (c \in br_1(T_{\sigma_{i_1 j}}), d \in br_1(T_{\sigma_{i_2 j}})).$$

It is easy to construct a NS-proof of

$$f_{i_1 j} f_{i_2 j} = \sum_{b \in B_{i_1,i_2,j}} x_b \tag{7}$$

from $\neg Count^3_{n^\epsilon}$ over $\mathbb{K}$ with degree $\leq O(\log(n))$.

Now, fix $i_1, i_2, i'_1, i'_2 \in [m+1]$ such that $i_1 < i_2$ and $i'_1 < i'_2$. For each $j \in [m]$, consider the trees

$$R_j := A_{i_1,i_2,j} * \sum_{b \in B_{i_1,i_2,j}} (T_{1,j}^{i_1,i_2,i'_1,i'_2})^b$$
$$R'_j := A_{i'_1,i'_2,j} * \sum_{b \in B_{i'_1,i'_2,j}} (T_{2,j}^{i_1,i_2,i'_1,i'_2})^b.$$

For each $r = bd^b$ ($b \in B_{i_1,i_2,j}$, $d \in br(T_{1,j}^{i_1,i_2,i'_1,i'_2})$), since $d||b$, there exists a unique j'_r such that d is an extension of some $c \in br_1(T_{\varphi^{i_1,i_2,i'_1,i'_2}_{j,j'_r}})$. Let $B_j \subset br(R_j)$ be the set of all branches having the above form.

Similarly, for each $r' = bd^b$ ($b \in B_{i'_1,i'_2,j}$, $d \in br(T_{2,j}^{i_1,i_2,i'_1,i'_2})$), since $d||b$, there exists a unique $\widehat{j}_{r'}$ such that d is an extension of some $c \in br_1(T_{\varphi^{i_1,i_2,i'_1,i'_2}_{\widehat{j}_{r'},j}})$. Let $B'_j \subset br(R'_j)$ be the set of all branches having the above form.

Now, we define

$$\begin{aligned} T_{j,j'} := (((T_{\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee s_{i_1 j}} * T_{\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee s_{i_2 j}}) * \\ T_{\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee s_{i'_1 j'}}) * T_{\neg r^{i_1,i_2,i'_1,i'_2}_{j,j'} \vee s_{i'_2 j'}}). \end{aligned}$$

for each $j \neq j' \in [m]$. Using these trees, we define

$$S_j := R_j * \sum_{r \in B_j} (T_{j,j'_r} * \sum_{t \in br(T_{j,j'_r})} (R'_{j'_r})^t)^r,$$
$$S'_j := R'_j * \sum_{r' \in B'_j} (T_{\widehat{j}_{r'},j} * \sum_{t \in br(T_{\widehat{j}_{r'},j})} (R_{\widehat{j}_{r'}})^t)^{r'}.$$

Label each branch $b \in br(S_j)$ as follows:

- If b extends some $r \in B_j$, then label b with $\langle j, j'_r \rangle$.
- Otherwise, label b with the symbol $\perp$.

Similarly, we label each branch $b' \in br(S'_j)$ as follows:

- If b extends some $r' \in B'_j$, then label b with $\langle \widehat{j}_{r'}, j \rangle$.
- Otherwise, label b with the symbol $\perp$.

It is easy to see that for each j, j', $br_{\langle j,j' \rangle}(S_j) = br_{\langle j,j' \rangle}(S'_{j'})$. Hence,

$$\sum_{j,j' \in [m]} \sum_{\alpha \in br_{\langle j,j' \rangle}(S_j)} x_\alpha = \sum_{j,j' \in [m]} \sum_{\beta \in br_{\langle j,j' \rangle}(S'_{j'})} x_\beta$$

Furthermore, it is easy to see that the following have NS-proofs from $\neg Count^3_{n^\epsilon}$ over $\mathbb{K}$ with $\leq O(\log(n))$-degree:

$$\sum_{j'\in[m]}\sum_{\alpha\in br_{\langle j,j'\rangle}(S_j)} x_\alpha = \sum_{b\in B_{i_1,i_2,j}} x_b \quad (j\in[m]),$$

$$\sum_{j\in[m]}\sum_{\beta\in br_{\langle j,j'\rangle}(S'_{j'})} x_\beta = \sum_{b\in B_{i'_1,i'_2,j'}} x_b \quad (j'\in[m]).$$

Hence, combined with (7), they give a NS-proof of $\sum_j f_{i_1j}f_{i_2j} = \sum_{j'} f_{i'_1}f_{i'_2}$ satisfying the required conditions.

(4): It follows similarly as (5) and (6) below.

(5): $b_{i_1i_2j}f_{i_1j}f_{i_2j} = 0$ follows easily from $\neg Count^3_{n^\epsilon}$ since each $\alpha \in br_{\langle j\rangle}(\widetilde{T}_{i_1,i_2})$ satisfies $\alpha \perp b$ for all $b \in B_{i_1,i_2,j}$.

(6): Note that we have NS-proofs of the following:

$$f_{i_1j} + \sum_{\beta\in br_0(T_{\sigma_{i_1j}})} x_\beta = 1,$$

$$f_{i_2j} + \sum_{\beta\in br_0(T_{\sigma_{i_2j}})} x_\beta = 1.$$

$$(j\in[m])$$

Hence, $b_{i_1i_2j}(1-f_{i_1j})(1-f_{i_2j}) = 0$ follows easily from $\neg Count^3_{n^\epsilon}$ by a similar reason as the previous item.

■

5 Future perspectives

In this section, we discuss future perspectives of the three conjectures above.

First, we note that the proof of Theorem 19 uses the uniform (with respect to the coefficient field) linear degree lower bound for NS-proofs of $injPHP^{f(n)}_n$ shown in [13], which seems to be a natural approach.

Next, Conjecture 1 is interesting on its own right; it casts the question on the difference between identifying the set size by division (using partitions) and doing it by ordering (using injections).

It also should be noted that if Conjecture 1 is true, then in particular,

$$V^0 + ontoPHP^k_l \nvdash injPHP^{n+1}_n. \tag{8}$$

The situation is interesting since the models of V^0 in which $injPHP^{n+1}_n$ is violated given so far (such as in [1] and [3]) actually violates $ontoPHP^k_l$. Therefore, the proof technique utilized to solve the problem (8) above may lead another breakthrough in proof complexity. The merit of approaching the problem (8) is that it seems to be easier than other important open problems of this field such as

- $V^0 \vdash injPHP^{2n}_n$? and
- $V^0(2) \vdash injPHP^{n+1}_n$?

The pigeonhole principle to be violated in (8) is more similar to the known violated ones than $injPHP^{2n}_n$, that is, the number of pigeons and that of holes are closer. Furthermore, over V^0, the problem (8) compares simple Σ^B_0 statements while "$V^0(2) \vdash injPHP^{n+1}_n$? " compares a Σ^B_1 one and a Σ^B_0 one.

As for Conjecture 2, a natural approach to prove the sufficient condition given in Theorem 29 is to utilize an appropriate version of "design" given in [5] and [3]. In order to achieve it, the bottleneck is the condition 3 of Theorem 29. We would like to construct a mapping from the set of low-degree monomials to $\mathbb{F}_2$ (which can be naturally extended to $\mathbb{F}_2$-module homomorphisms from the set of low-degree polynomials to $\mathbb{F}_2$) which is compatible with the polynomially many equations

$$\sum_{j\in[m]} f_{ij}f_{i'j} + 1 = 0 \quad (i \neq i' \in [m+1]).$$

(If it succeeds, then we can derive the contradiction from the usual oddtown theorem). It seems that the treatment of multiplication is difficult. The difficulty may be related to that of constructing a model of a given extended NS-proof (see [5] and section 15.6 of [10] for reference). In other words, the solution to Conjecture 2 may include the tips to give a superpolynomial lower bound of $F_d(2)$-proofs.

As for Conjecture 3, it is important to note that the condition given in Theorem 33 admits arbitrary field $\mathbb{K}$. Hence, although the difficulty is similar as Conjecture 2, it may be more approachable to tackle Conjecture 3.

Acknowledgements

The author is grateful to Toshiyasu Arai for helpful discussions and his patient support. The author also thanks to Jan Krajíček for his valuable comments.

This work was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

References

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

[2] Beame, P., Impagliazzo, R., Krajíček, J., Pitassi, T. & Pudlak, P. Lower bounds on Hilbert's Nullstellensatz and propositional proofs, *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994), 794-806.

[3] Beame, P., & Riis, S. More on the relative strength of counting principles, in *Proof Complexity and Feasible Arithmetics*, P. Beame, & S. Buss (Eds.), DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol.39, American Mathematical Society, Providence, RI (1998), 13-35.

[4] Bonet, M., Buss, S., & Pitassi, T. Are there hard examples for Frege systems?, in *Feasible Mathematics II*, Progress in Computer Science and Applied Logic, 13, P. Clote, & J.B. Remmel (Eds.), Birkhäuser Boston, Boston, MA (1995), 30-56.

[5] Buss, S., Impagliazzo, R., Krajíček, J., Pudlák, P., Razborov, A. A., & Sgall, J. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting, *Computational Complexity*, *vol.6*, *no.3* (1996), 256-298.

[6] Cook, S., & Nguyen, P. *Logical foundations of proof complexity*, Perspectives in Logic. Cambridge University Press, New York, NY (2010).

[7] Ken, E. (2022), On some Σ_0^B-generalizations of the pigeonhole and the modular counting principles over V^0, Graduate School of Mathematical Sciences, the University of Tokyo, master's thesis.

[8] Ken, E. (2022), On some Σ_0^B-generalizations of the pigeonhole and the modular counting principles over V^0 (preprint), arXiv:2203.10237

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

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

[11] Krajíček, J., Pudlák, P., & Woods, A. An exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, *Random Structures and Algorithms*, *vol. 7*, *no. 1* (1995), 15-39.

[12] Pitassi, T., Beame, P., & Impagliazzo, R. Exponential lower bounds for the pigeonhole principle, *Computational Complexity*, *vol. 3*, *no.2* (1993), 97-140.

[13] Razborov, A, A. Lower bounds for the polynomial calculus, *Computational Complexity*, *vol. 7*, *no. 4* (1998), 291-324.

The Graduate School of Mathematical Sciences,
The University of Tokyo
Tokyo 153-8914
JAPAN
Email-address: `yeongcheol-kwon@g.ecc.u-tokyo.ac.jp`

東京大学　数理科学研究科　権　英哲