On some $\Sigma_0^B$-formulae generalizing counting principles over $V^0$

Eitetsu Ken$^1$

July 16, 2024

$^1$email: yeongcheol-kwon@g.ecc.u-tokyo.ac.jp
Abstract

We formalize various counting principles and compare their strengths over $V^0$. In particular, we conjecture the following mutual independence between:

- a uniform version of modular counting principles and the pigeonhole principle for injections,
- a version of the oddtown theorem and modular counting principles of modulus $p$, where $p$ is any natural number which is not a power of 2,
- and a version of Fisher’s inequality and modular counting principles.

Then, we give sufficient conditions to prove them. We give a variation of the notion of $PHP$-tree and $k$-evaluation to show that any Frege proof of the pigeonhole principle for injections admitting the uniform counting principle as an axiom scheme cannot have $o(n)$-evaluations. As for the remaining two, we utilize well-known notions of $p$-tree and $k$-evaluation and reduce the problems to the existence of certain families of polynomials witnessing violations of the corresponding combinatorial principles with low-degree Nullstellensatz proofs from the violation of the modular counting principle in concern.
1 Introduction

Ajtai’s discovery ([2]) of $V^0 \not\vdash \text{ontoPHP}_{n+1}^n$, where $\text{ontoPHP}_{n+1}^n$ is a 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 technique, which was later formalized in [14] as $k$-evaluation and switching lemma, has been utilized to further works in the area such as the comparison between various types of counting principles (such as [3] and [4]). In the course of the works, it turned out that degree lower bounds of Nullstellensatz proofs are essential when one would like to give lower bounds for the lengths of proofs from constant depth Frege system equipped with $\{\text{Count}_k^n\}_{1 \leq k \in \mathbb{N}}$ (i.e., the modular counting principle mod $p$) as an axiom scheme. One of the most important open problems in the current proof complexity is whether $V^0(p) \not\vdash \text{injPHP}_{n+1}^n$ or not (here, $\text{injPHP}_{n+1}^n$ denotes the pigeonhole principle for injections). This problem is interesting because it would deepen our understanding of how hard it is to count a set (recall that $\text{VTC}^0 \vdash \text{injPHP}_{n+1}^n$ and $V^0(p) \vdash \text{Count}_n^n$). Furthermore, if the problem is solved for composite $p$, it would give us tips to solve the separation problem $\text{AC}^0(p)$ versus $\text{TC}^0$. As for this problem, [17] made considerable progress. The paper gave good degree lower bounds for polynomial calculus proofs of $\text{injPHP}_{n+1}^m$ ($m > n$), which does not depend on the specific coefficient field.

This paper aims to connect the result of [17] to a superpolynomial lower bound for the proof length of $\text{injPHP}_{n+1}^m$ from $\text{AC}^0$-Frege system equipped with Uniform Counting Principle, which can be seen as a uniform version of infinite formulae $\{\text{Count}_n^n\}_{p,n}$, as an axiom scheme. Tackling the issue, we obtain natural and exciting open problems. We also consider some of them, too.

The detailed content and the organization of the article are as follows.

First, in §2 as the preliminary, we define three types of (first-order and propositional) formulae, which at first glance seem to be generalized versions of modular counting principles (which do not fix the modulus). We name them as:

1. Modular Pigeonhole Principle $\text{modPHP}_{n,m}^d$.
2. Uniform Counting Principle $\text{UCP}_{n,m}^d$.
3. Generalized Counting Principle $\text{GCP}$.

Then, we compare the relative strength of these versions over $V^0$ and also develop some independence results over $V^0$. It immediately turns out that

- $V^0 + \text{ontoPHP}_{n+1}^d \vdash \text{modPHP}_{k,m}^d$, and
- $V^0 + \text{modPHP}_{k,m}^d \vdash \text{ontoPHP}_{n+1}^d$.

(For the precise meaning of the statements, see §2)

Therefore, we see $\text{modPHP}_{n,m}^d$ is actually not appropriate to be called a generalized version of modular counting principles because it cannot imply them.

On the other hand, we observe that
• For any natural number $p \geq 2$, $V^0 + UCP_{k,m}^l \vdash Count_p^n$.
• $V^0 + UCP_{k,m}^l \vdash ontoPHP_{n+1}^n$.
• $V^0 + GCP \vdash UCP_{n,m}$.
• $V^0 + GCP \vdash injPHP_{n+1}^n$.

Hence, we see $UCP_{n,m}$ and $GCP$ can be seen as generalizations of counting principles. In the latter sections, we tackle natural questions arising from the observations above. Towards them, in §2 we review the Nullstellensatz proof system.

In §3 we consider the problem: $V^0 + UCP_{k,m}^l \vdash injPHP_{n+1}^n$? The author conjectures $V^0 + UCP_{k,m}^l \nvdash injPHP_{n+1}^n$, and gives a sufficient condition to prove it. We define suitable analogues of PHP-tree and $k$-evaluation in the proof of Ajtai’s theorem given in [13], and show that if an $h$-evaluation using $injPHP$-trees exists for a Frege proof of $injPHP_{n+1}^n$ admitting $UCP_{k,m}^l$ as an axiom scheme, $h$ cannot be of order $o(n)$. Our main work is manipulating the trees that connect the order of $h$ with the degrees of Nullstellensatz proofs of it.

In §4 we consider a “more natural” combinatorial principle than GCP that implies both $injPHP_{n+1}^n$ and $Count_p^n$ for some $p$. Namely, we consider the (propositional and first-order) formulae $oddtown_n$, which formalize the the odd-town theorem. We observe:

• $V^0 + oddtown_k \vdash Count_p^n$ for $p = 2^k$.
• $V^0 + oddtown_k \vdash injPHP_{n+1}^n$.

The author conjectures $V^0 + oddtown_k \nvdash Count_p^n$ for any prime $p \neq 2$, and gives a sufficient condition to prove it. Roughly speaking, the statement is as follows; 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 Nullstellensatz proofs from $\neg Count_p^n$ with degree $O(1)$.

In §5 we consider the (propositional and first-order) formulae $FIE_n$ which formalize Fisher’s inequality. We observe

• $V^0 + FIE_k \vdash injPHP_{n+1}^n$.

On the other hand, the author conjectures $V^0 + FIE_k \nvdash Count_p^n$ for any $p \geq 2$, and gives a sufficient condition whose form is similar to the previous one to prove it.

2 Preliminaries

2.1 Setup of bounded arithmetic and counting principles

Throughout this paper, $p$ and $q$ denote natural numbers. The cardinality of a finite set $S$ is denoted by $\#S$. We prioritize readability and often use natural
abbreviations to express logical formulae. We assume the reader is familiar with the basics of bounded arithmetics and Frege systems (such as the concepts treated in [8]). Unless stated otherwise, we follow the conventions of [8].

We basically use the parenthesis (, ) to denote tuples, but when there are several tuples of different types or in different universes, we also use ⟨, ⟩ for readability. In particular, in §5, we often label edges and leaves of a tree by tuples. In that case, we use ⟨, ⟩.

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

\[
\land_{i=1}^{k} \varphi_i := \neg \lor_{i=1}^{k} \neg \varphi_i.
\]

When the arity of \( \land \) is small, we also use \( \wedge \) to denote it. We give the operators \( \lor \) and \( \land \) precedence over \( \vee \) and \( \wedge \) as the order of application.

Example 1. \( \land_{i} \varphi_i \lor \land_{j} \psi_j \) means \( (\land_{i} \varphi_i) \lor (\land_{j} \psi_j) \).

We also define an abbreviation \( \rightarrow \) by

\[
(\varphi \rightarrow \psi) := \neg \varphi \lor \psi.
\]

For a set \( S \) of propositional variables, an \( S \)-formula means a propositional formula whose propositional variables are among \( S \). For a set \( S = \{s_j^i \mid 1 \leq j \leq k, i \in I_j \} \) of propositional variables where each \( s_j^i \) is distinct, an \( S \)-formula \( \psi \), and a family \( \{\varphi_i^j\}_{i \in I_j} \) of propositional formulae,

\[
\psi[\varphi_i^1/s_1^1, \ldots, \varphi_i^k/s_k^1]
\]

denotes the formula obtained by substituting each \( \varphi_i^j \) for \( s_j^i \) simultaneously.

It is well-known that a \( \Sigma^B_0 \) \( L^2_A \)-formula \( \varphi(x_1, \ldots, x_k, R_1, \ldots, R_l) \) can be translated into a family \( \{\varphi[n_1, \ldots, n_k, m_1, \ldots, m_l] \}_{n_1, \ldots, n_k, m_1, \ldots, m_l \in \mathbb{N}} \) of propositional formulae. (See Theorem VII 2.3 in [8].)

Now, we define several formulae which express the so-called “counting principle.”

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

\[
\text{Count}^p(n, X) := \neg p \mid n \rightarrow -\left( (\forall k \in [n]. \exists e \in [n]^{(p)}. (e \in X \land k \in ^* e)) \right) \\
\land \left( (\forall e, e' \in [n]^{(p)}. \neg (e \in X \land e' \in X \land e \perp e')) \right)
\]

Here,
• $p \mid n$ is a $\Sigma^B_0$ formula expressing “$p$ divides $n$.”
• $[n]$ denotes the set $\{1, \ldots, n\}$.

We code a $p$-subset 
\[ e = \{e_1 < \ldots < e_p\} \]
of $[n]$ by the number 
\[ \sum_{i=1}^{p} e_i (n+1)^{p-i}. \]

• $[n]^{(p)}$ denotes the $\Sigma^B_0$-definable set of all the codes of the $p$-subsets of $[n]$. Note that each member in $[n]^{(p)}$ is less than, say, $(n+1)^p$.

• The elementship relation $\in^*$ is expressed by a natural $\Sigma^B_0$-predicate. We often write it $\in$, too.

• $e \perp e'$ means 
\[ e \neq e' \text{ and } e \cap e' \neq \emptyset, \]
and it is also expressed by a natural $\Sigma^B_0$-predicate.

We also define the propositional formula $\text{Count}_n^p$ as in [12]:
\[
\text{Count}_n^p := \begin{cases} 
1 & \text{if } p \mid n \\
\neg \left( \bigwedge_{k \in [n]} \bigvee_{e \in [n]^{(p)}} r_e \land \bigwedge_{e, e' \in [n]^{(p)} : e \perp e'} (\neg r_e \lor \neg r_{e'}) \right) & \text{otherwise}
\end{cases}
\]

Here, $\{r_e\}_{e \in [n]^{(p)}}$ is a family of distinct propositional variables.

**Convention 3.** With suitable identification of propositional variables, $\text{Count}^p(x, X)[n, (n+1)^p]$ is equivalent to $\text{Count}_n^p$ over $\text{AC}^0$-Frege system modulo polynomial-sized proofs. Thus we often abuse the notation and write $\text{Count}_n^p$ for $\text{Count}^p(n, X)$.

**Definition 4.** The $\Sigma^B_0 \mathcal{L}^A_2$-formula $\text{ontoPHP}(m, n, R)$ 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 $\text{Count}^p(n, X)$. Similarly, the $\Sigma^B_0 \mathcal{L}^A_2$-formula $\text{injPHP}(m, n, R)$ 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 $\text{ontoPHP}_n^m$ and $\text{injPHP}_n^m$ by
\[
\text{ontoPHP}_n^m := \begin{cases} 
\neg \left( \bigwedge_{i \in [m]} \bigvee_{j \in [n]} r_{ij} \land \bigwedge_{i \neq i' \in [m]} \bigwedge_{j \in [n]} (\neg r_{ij} \lor \neg r_{i'j}) \right) & \text{if } m > n \\
1 & \text{otherwise}
\end{cases}
\]
and
\[
\text{injPHP}_n^m := \begin{cases} 
\neg \left( \bigwedge_{i \in [m]} \bigvee_{j \in [n]} r_{ij} \land \bigwedge_{i \neq i' \in [m]} \bigwedge_{j \neq j' \in [n]} (\neg r_{ij} \lor \neg r_{i'j'}) \right) & \text{if } m > n \\
1 & \text{otherwise}
\end{cases}
\]
With reasons similar to the one stated in Convention 3, we abuse the notations and use \( \text{ontoPHP}^m_n \) to denote \( \text{ontoPHP}(m,n,R) \) and \( \text{injPHP}^m_n \) to denote \( \text{injPHP}(m,n,R) \).

The following are well-known:

**Theorem 5** ([2], improved by [14] and [16]).

\[ V^0 \not\vdash \text{ontoPHP}^n_{n+1}. \]

Here, we adopt the following convention.

**Convention 6.** For \( \Sigma^B_0 \)-formulae \( \psi_1, \ldots, \psi_l \) and \( \varphi \), we write

\[ V^0 + \psi_1 + \cdots + \psi_l \vdash \varphi \]

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

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

\[ V^0 + \text{Count}_k^p \not\vdash \text{Count}_n^q \]

means

\[ V^0 + \forall k, X. \text{Count}_k^p(k,X) \not\vdash \forall n, X. \text{Count}_n^q(n,X), \]

while

\[ V^0 \not\vdash \text{UCP}_n^{l,d} \]

means

\[ V^0 \not\vdash \forall l, d, n, R. \text{UCP}(l,d,n,R) \]

(for the definition of \( \text{UCP}_n^{l,d} \) and \( \text{UCP}(l,d,n,R) \), see Definition 13).

In the former example, note that we have used the different variables \( k, n \) to avoid confusion about the variables’ dependencies.

**Theorem 7** ([3]). For \( p, q \geq 2 \), \( V^0 + \text{Count}_k^p \vdash \text{Count}_n^q \) if and only if \( \exists N \in \mathbb{N}. q \mid p^N \).

**Theorem 8** ([4]). For any \( p \geq 2 \), \( V^0 + \text{Count}_k^p \not\vdash \text{injPHP}_n^{k+1} \).

Also, the following is a corollary of the arguments given in [12]:

**Theorem 9** (essentially in [12]). For all \( p \geq 2 \), \( V^0 + \text{injPHP}_k^{k+1} \not\vdash \text{Count}_n^p \).

**Remark 10.** Note that the exact statement Theorem 12.5.7 in [12] shows is

\[ V^0 + \text{ontoPHP}_k^{k+1} \not\vdash \text{Count}_n^p \]

for each fixed \( p \geq 2 \). However, with a slight change of the argument, it is easy to see that Theorem 8 actually holds.
From now on, we consider several seemingly generalized versions of \( \text{Count}^n_r \), which do not fix the modulus \( p \), and evaluate their strengths. Naively, the generalized counting principle should be a statement like: “For any \( d \geq 2 \) and \( n \in \mathbb{N} \), if \( d \) does not divide \( n \), then \( n \) cannot be partitioned into \( d \)-sets.” The following is one of the straightforward formalizations of this statement:

**Definition 11.** The \( \mathcal{L}^2_0 \)-formula \( \text{modPHP}(d, m, n, R) \) is a natural formalization of the statement “If \( m \not\equiv n \pmod{d} \), then \( R \) does not give the graph of a bijection between \([m]\) and \([n]\),” We also define the propositional formulae \( \text{modPHP}^{d,m}_n \) as follows:

\[
\text{modPHP}^{d,m}_n := \begin{cases} 
\text{same as the case of } m > n \text{ in the definition of } \text{ontoPHP}^m_n & (m \not\equiv n \pmod{d}) \\
1 & \text{(otherwise)}
\end{cases}
\]

With a similar reason as the one given in Convention 3, we abuse the notation and use \( \text{modPHP}^{d,m}_n \) to denote \( \text{modPHP}(d, n, R) \).

Intuitively, \( \text{modPHP}^{d,m}_n \) expresses “if \( n \not\equiv m \pmod{d} \) and \( m = ds + r \) \((0 \leq r < d)\), then there does not exist a family \( \{S_i\}_{i \in [g]} \) of \( d \)-sets and an \( r \)-set \( S_0 \) which give a partition of \([n]\).” However, it does not imply even \( \text{Count}^2_n \):

**Proposition 12.** The following hold:

1. \( V^0 + \text{ontoPHP}^{L,L}_k \vdash \text{modPHP}^{d,m}_k \).
2. \( V^0 + \text{modPHP}^{d,m}_k \vdash \text{ontoPHP}^{L,L}_k \).

In particular, for any \( p \geq 2 \), \( V^0 + \text{modPHP}^{d,m}_k \not\vdash \text{Count}^p_n \).

**Proof.** As for 1 argue in \( V^0 \) as follows: assume \( m \not\equiv k \pmod{d} \), and \( R \) gives a bijection between \([m]\) and \([k]\). It easily follows that \( m \not\equiv k \), and hence \( R \) or \( R^{-1} \) violates \( \text{ontoPHP}^m_k \) or \( \text{ontoPHP}^{m}_k \).

As for 2 argue in \( V^0 \) as follows: suppose \( L > l \) and \( R \) gives a bijection between \([L]\) and \([l]\). Then \( R \) violates \( \text{modPHP}^{L,L}_l \).

The last part follows from Theorem 9.

Therefore, \( \text{modPHP}^{d,m}_n \) is actually not a generalization of counting principles over \( V^0 \).

Next, we consider the following version:

**Definition 13.** \( \text{UCP}(l, d, n, R) \) (which stands for Uniform Counting Principle) is an \( \mathcal{L}^2_A \) formula defined as follows:

\[
(d \geq 1 \land \lnot d \mid n) \to \forall i \in [l],(\forall j \in [d], \exists e \in [n], R(i, j, e) \lor \forall j \in [d], \exists e \in [n], R(i, j, e)) \\
\land \forall (i, j) \in [l] \times [d], \forall e \neq e' \in [n], (\neg R(i, j, e) \lor R(i, j, e') \lor \neg R(i, j, e')) \\
\land \forall (i, j) \neq (i', j') \in [l] \times [d], \forall e \in [n], (\neg R(i, j, e) \lor R(i', j', e')) \\
\land \forall e \in [n], \exists (i, j) \in [l] \times [d], R(i, j, e)
\]

6
The propositional formula $UCP_{n}^{l,d}$ is defined as follows:

$$UCP_{n}^{l,d} := \begin{cases} 
\neg \left( \bigwedge_{i=1}^{l} \left( \bigwedge_{j=1}^{d} \forall \varepsilon \in [n] \ r_{i,j,\varepsilon} \right) \lor \left( \bigwedge_{j=1}^{d} \neg \forall \varepsilon \in [n] \ r_{i,j,\varepsilon} \right) \right) \\
\bigwedge_{(i,j) \in [l] \times [d]} \bigwedge_{\varepsilon \neq \varepsilon'} \bigwedge_{\varepsilon' \in [n]} \left( \neg r_{i,j,\varepsilon} \lor \neg r_{i,j,\varepsilon'} \right) \\
\bigwedge_{(i,j) \neq (i',j')} \bigwedge_{\varepsilon \in [n]} \left( \neg r_{i,j,\varepsilon} \lor \neg r_{i',j',\varepsilon} \right) \\
\bigwedge_{\varepsilon \in [n]} \bigwedge_{(i,j) \in [l] \times [d]} \left( r_{i,j,\varepsilon} \right) \quad \text{(if } n \neq 0 \text{ (mod } d) \text{, } d \geq 1) \\
1 \quad \text{(otherwise)}
\end{cases}$$

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 $n \equiv 0$ (mod $d$), 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 $r_{i,j,\varepsilon}$ reads “the $j$-th element of $S_{i}$ is $\varepsilon$.”

We observe the following:

**Proposition 14.** $VTC^{0} \vdash UCP_{k}^{l,d}$.

For a detailed treatment of the bounded arithmetic $VTC^{0}$, see §IX.3 of [8].

**Proof Sketch.** Work in $VTC^{0}$. Suppose a bounded set $R$ violates $UCP_{k}^{l,d}$, that is:

- $k \equiv 0$ (mod $d$).
- $[k]$ is partitioned into $\{S_{i}\}_{i \in [l]}$, where $S_{i} = \{e \in [k] \mid \exists j \in [d]. R(i, j, e)\}$.
- Each $S_{i}$ is either empty or $[d]$-set. In the latter case, it is witnessed by the bijection $B_{i} := \{(j, e) \mid R(i, j, e)\}$.

Crucial properties of $VTC^{0}$ we use are:

1. There is a $\Sigma_{0}^{B}$-definable function $\# S$, which counts the cardinality of the input bounded set $S$.

2. $VTC^{0}$ proves the following: if a bounded set $M$ codes a bijection between two bounded sets $A$ and $B$, then $\# A = \# B$.

Armed with these, we can derive a contradiction in the following way: we consider the cardinality of $S = \{(i, j, e) \in [l] \times [d] \times [k] \mid R(i, j, e)\}$. We can show that $\# S_{i}$ is 0 if it is empty and $d$ otherwise. In the latter case, we use the item 2 above. Furthermore, by induction on $i \in [l]$, we see that $\# \bigcup_{i' \leq i} S_{i'} \equiv 0$ (mod $d$). Considering the case $i = l$, we have $\# S \equiv 0$ (mod $d$).

On the other hand, there is a $\Sigma_{0}^{B}$-definable bijection between $S$ and $[k]$:

$$S \rightarrow [k]; \ (i, j, e) \mapsto e.$$ 

The fact that the above map is a bijection follows immediately from the assumption on $R$. Hence, using the item 2 again, we have $\# S = k \neq 0$ (mod $d$), a contradiction. ■
Proposition 15. The following hold:

1. For any \( p \geq 2 \), \( V^0 + UCP_{k}^{l,d} \vdash Count_{n}^{p} \).

2. \( V^0 + UCP_{k}^{l,d} \vdash ontoPHP_{m}^{n} \).

Proof. As for 1, argue in \( V^0 \) as follows: suppose \( n \not\equiv 0 \pmod{p} \), and \( R \) gives a \( p \)-partition of \([n]\). Set the family \( \{S_{r}\}_{r \in [(n+1)p]} \) by:

\[
S_{r} := \begin{cases} 
\text{the set coded by } r & \text{ (if } r \in R) \\
\emptyset & \text{ (otherwise)}
\end{cases}
\]

Then \( \{S_{r}\}_{r \in [(n+1)p]} \) indeed violates \( UCP_{n}^{(n+1)p} \).

As for 2, argue in \( V^0 \) as follows: suppose \( m > n \) and \( R \) gives a bijection between \([m]\) and \([n]\). Then, \( \{[n]\} \) violates \( UCP_{n}^{l,m} \).

Hence, \( UCP_{n}^{l,d} \) is indeed a generalization of counting principles. It is natural to ask

Question 1. Does the following hold?:

\[
V^0 + UCP_{k}^{l,d} \vdash injPHP_{n+1}^{n},
\]

or, at least,

\[
V^0 + ontoPHP_{m}^{m} \vdash injPHP_{n+1}^{n}.
\]

In view of theorem 8, the author conjectures the answer to the problem is no. We tackle this issue in section 3.

Here, we consider one more generalization of counting principles (which relates to the above problem):

Definition 16. \( GCP(P, Q_1, Q_2, R_1, R_2, M_0, M_1, M_2) \) (which stands for Generalized Counting Principle) is a \( \Sigma_{0}^{L_{A}^{2}} \)-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 the 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 17. 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 are not using it at this time.
It is easy to see that:

**Proposition 18.** $\text{VTC}^0 \vdash \text{GCP}$.

*Proof Sketch.* Analogously with Proposition 14, we can derive an arithmetical contradiction in number sort by applying $#$ to the bounded sets listed in the definition of $\text{GCP}$ and their products.

**Proposition 19.**

1. $V^0 + \text{GCP} \vdash UCP^{l,d}$.
2. $V^0 + \text{GCP} \vdash injPHP^{n+1}$.

*Proof.* Work in $V^0 + \text{GCP}$.

We first prove $UCP^{l,d}$. Suppose $n \not\equiv 0 \pmod{d}$, and $\{S_i\}_{i \in [l]}$ is a family consisting of $d$-sets and emptysets, and $[n] = \bigsqcup_{i \in [l]} S_i$. Set

$$Q := \{i \in [l] \mid S_i \neq \emptyset\}.$$

Then the partition gives a bijection between $[n]$ and $Q \times [d] \sqcup \emptyset$.

On the other hand, since $n \not\equiv 0 \pmod{d}$, we can write $n = ds + r$ where $1 \leq r < d$. This gives a natural bijection between $[n]$ and $[d] \times [s] \sqcup [r]$.

Using $\Sigma^B_d$-COMP (cf. Definition V.1.2 in [8]), it is straightforward to construct proper injections from $\emptyset$ to $[r]$ and from $[r]$ to $[d]$. Thus, $\text{GCP}$ is violated, which is a contradiction.

We next prove $injPHP^{n+1}$. Suppose $R$ gives an injection from $[n+1]$ to $[n]$. Then, there is a natural bijection between $[n]$ and $[n+1] \times [1] \sqcup ([n] \setminus \text{ran } R)$.

On the other hand, there is a natural bijection between $[n]$ and $[n+1] \times \emptyset \sqcup [n]$.

It is easy to construct proper injections from $[n] \setminus \text{ran } R$ to $[n]$, and from $[n]$ to $[n+1]$. Thus, $\text{GCP}$ is violated, which is a contradiction.

It is natural to ask:

**Question 2.**

1. Does the following hold: $V^0 + UCP^{l,d} \vdash \text{GCP}$?
2. Is there any other combinatorial principle than $\text{GCP}$ which also implies $injPHP^{n+1}$ and some of $Count^n$?

On the item 1, the author conjectures the answer is no (since $\text{GCP}$ implies $injPHP^{n+1}$).

As for the item 2, we consider the oddtown theorem in §4.

### 2.2 Nullstellensatz proof system

In the analysis of this paper, Nullstellensatz proofs (written shortly as “$NS$-proofs”) play an essential role in the arguments. We set up our terminology on $NS$-proofs and review degree lower bounds for $injPHP$. 

9
Definition 20. Let $A$ be a (commutative) ring, and $\mathcal{F}$ be a set of multivariate $A$-polynomials. For multivariate polynomials $g_1$, $g_2$ and $h_f$ ($f \in \mathcal{F}$) over $A$, \( \{h_f\}_{f \in \mathcal{F}} \) is a NS-proof of $g_1 = g_2$ from $\mathcal{F}$ over $A$ if and only if
\[
g_1 - g_2 = \sum_{f \in \mathcal{F}} h_f f.
\]
Especially, for $a \in A \setminus \{0\}$, a NS-proof of $a = 0$ from $\mathcal{F}$ is called a NS-refutation of $\mathcal{F}$.

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

We are particularly interested in the following family of polynomials, which is another representation of the pigeonhole principle:

Definition 21. Let $M, m \in \mathbb{N}$, and $M > m$. Given a ring $A$, we define $\neg \text{injPHP}^M_m[A]$ as the family of the following multivariate polynomials over $A$:

\begin{align*}
x_{ij}^2 - x_{ij} & \quad (i \in [M], j \in [m]), \\
x_{ij}x_{ij'} & \quad (i \in [M], j \neq j' \in [m]), \\
x_{ij}x_{i'j} & \quad (i \neq i' \in [M], j \in [m]), \\
\sum_{j=1}^m x_{ij} - 1 & \quad (i \in [M]),
\end{align*}

(each $x_{ij}$ is distinct.)

Furthermore, we define $\neg \text{inj}^*\text{PHP}^M_m[A]$ as the family of the following multivariate polynomials over $A$:

\begin{align*}
x_{ij}^2 - x_{ij}, u_{ij}^2 - u_j & \quad (i \in [M], j \in [m]), \\
x_{ij}x_{ij'} & \quad (i \in [M], j \neq j' \in [m]), \\
x_{ij}x_{i'j} & \quad (i \neq i' \in [M], j \in [m]), \\
\sum_{j=1}^m x_{ij} - 1 & \quad (i \in [M]), \\
\sum_{i=1}^M x_{ij} + u_j - 1 & \quad (j \in [m])
\end{align*}

($x_{ij}$ and $u_j$ are distinct indeterminates).

Remark 22. It is easy to see that $\neg \text{injPHP}^M_m[A]$ is not satisfiable in $A$ if $A$ is a field; the system is a paraphrase of the pigeonhole principle since $x^2 - x = 0$ implies $x = 0, 1$ in a field. This unsatisfiability of $\neg \text{injPHP}^M_m[A]$ is extended to the case when $A$ is a general nontrivial ring since there always exists a ring homomorphism from $A$ to a field, and all the coefficients of the polynomials in $\neg \text{injPHP}^M_m[A]$ are among $0, \pm 1$. 

10
Furthermore, if $A$ is nontrivial, then $\neg \text{injPHP}_m^M[A]$ always has a $\textup{NS}$-refutation over $A$. Indeed, the unit of $A$ generates a subring of $A$ which is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$ ($m \geq 2$). $\neg \text{injPHP}_m^M[\mathbb{Z}]$ has a $\textup{NS}$-refutation over $\mathbb{Z}$ since we have a $\textup{NS}$-refutation over $\mathbb{Q}$. We know that $\neg \text{injPHP}_m^M[\mathbb{Z}/m\mathbb{Z}]$ has a $\textup{NS}$-refutation over $\mathbb{Z}/m\mathbb{Z}$ when $m$ is prime. For composite $m$, taking a prime divisor $p$ of it, we have an embedding of $\mathbb{Z}/p\mathbb{Z}$ into $\mathbb{Z}/m\mathbb{Z}$ as additive groups. Since all the coefficients of the polynomials in $\neg \text{injPHP}_m^M[\mathbb{Z}/m\mathbb{Z}]$ are among $0, \pm 1$, we can transform a $\textup{NS}$-refutation $\langle h_f \rangle_f$ over $\mathbb{Z}/p\mathbb{Z}$ to a $\textup{NS}$-refutation over $\mathbb{Z}/m\mathbb{Z}$ by simply mapping each coefficient of $h_f$ by the embedding.

Note that Nullstellensatz proof system is not always complete for general coefficient rings. See the appendix of [7] for details.

We have introduced $\neg \text{injPHP}_m^M[A]$ since it makes the translation of $\text{injPHP}$-trees into $\textup{NS}$-refutations in the proof of Theorem 53 simpler, although it is an easy observation that $\neg \text{injPHP}_m^M$ and $\neg \text{injPHP}_m^*$ are equivalent in the sense of degree of $\textup{NS}$-refutation:

**Proposition 23.** Let $A$ be a ring. For $M, m, d \in \mathbb{N}$ with $M > m$, the following are equivalent:

1. $\neg \text{injPHP}_m^M[A]$ has a $\textup{NS}$-refutation over $A$ of degree $\leq d$.
2. $\neg \text{injPHP}_m^*[A]$ has a $\textup{NS}$-refutation over $A$ of degree $\leq d$.

**Proof.** $\text{1} \Rightarrow \text{2}$ follows from $\neg \text{injPHP}_m^M[A] \subseteq \neg \text{injPHP}_m^*[A]$ as families of polynomials.

We consider the converse. Suppose $\neg \text{injPHP}_m^*[A]$ has a $\textup{NS}$-refutation of degree $\leq d$. Applying the substitution $u_j := 1 - \sum_{i=1}^M x_{ij} \ (j \in [m])$, we obtain a $\textup{NS}$-refutation of

$$
\neg \text{injPHP}_m^M \cup \left\{ \left(1 - \sum_{i=1}^M x_{ij}\right)^2 - \left(1 - \sum_{i=1}^M x_{ij}\right) \ | \ j \in [m] \right\}
$$

over $A$ without increasing the degree. Furthermore,

$$
\left(1 - \sum_{i=1}^M x_{ij}\right)^2 - \left(1 - \sum_{i=1}^M x_{ij}\right) = \sum_{i=1}^M (x_{ij}^2 - x_{ij}) + \sum_{i \neq i' \in [M]} x_{ij}x_{i'j}.
$$

Hence, we obtain a $\textup{NS}$-refutation of $\neg \text{injPHP}_m^M[A]$ over $A$ without increasing the degree.

As for the case when $A$ is a field, the following powerful degree lower-bound is well-known:

**Theorem 24 ([17]).** Let $M, m \in \mathbb{N}$ and $M > m$. Assume $A$ is a field. There is no $\textup{PC}$-refutation of $\neg \text{injPHP}_m^M[A]$ over $A$ with degree $\leq m/2$. In particular, there is no $\textup{NS}$ refutation of $\neg \text{injPHP}_m^M[A]$ over $A$ with degree $\leq m/2$. 

11
Here, \( PC \) stands for “Polynomial Calculus.” For the precise treatment of the formal system, see §6.2 of [13].

Towards the discussion in §3, we want to generalize the above degree lower bound for \( A = \mathbb{Z}/n\mathbb{Z} \), where \( n \) is a general integer satisfying \( n \geq 2 \). Precisely speaking, taking a closer look at the proof of Theorem 24, we can obtain the following generalization:

**Corollary 25** (essentially by [17]). Let \( A \) be a finite nontrivial commutative ring. Let \( M, m \in \mathbb{N} \) satisfy \( M > m \). Then there is no \( NS \)-refutation of \( injPHP^M_m[A] \) of degree \( \leq \frac{m}{2} \).

We give a proof for completeness. Below, we follow the presentation of §16.2 in [13]. Fix \( M > m \) and a finite nontrivial commutative ring \( A \) in the rest of this section.

Let \( Maps \) be the set of partial bijections from \([M]\) to \([m]\). For each \( \alpha \in Maps \), set \( x_\alpha := \prod_{i \in \text{dom}(\alpha)} x_{\alpha(i)} \). In particular, \( x_\emptyset := 1 \). Let \( \hat{S} := A[\bar{x}]/I \), where \( I \) is the ideal generated by the polynomials (1), (2), (3) in \( injPHP^M_m[A] \). For \( f \in A[\bar{x}] \), \( \hat{f} \) denotes the quotient of \( f \) in \( \hat{S} \). Furthermore, for a subset \( U \subseteq A[\bar{x}] \), set

\[
\hat{U} := \{ \hat{f} \in \hat{S} \mid f \in U \}.
\]

**Definition 26.** For a parameter \( t \leq m \), define:

\[
Maps_t := \{ \alpha \in Maps \mid \#\alpha \leq t \};
\]

\[
S_t := \{ f \mid f \in A[\bar{x}], \deg(f) \leq t \};
\]

\[
T_t := \{ x_\alpha \mid \alpha \in Maps_t \}.
\]

Note that:

**Proposition 27.** For \( t \leq m \),

1. \( \hat{S}_t \) is a free \( A \)-module of finite rank.

2. \( \hat{T}_t \) is a basis of \( \hat{S}_t \), and \( \#T_t = \#\hat{T}_t \).

**Proof.** The first item follows from the second item. We can show the second item as follows. The fact that \( \hat{T}_t \) generates \( \hat{S}_t \) straightforwardly follows from the definition of \( I \) above. We show that \( \hat{T}_t \) is \( A \)-linearly independent and \( \#T_t = \#\hat{T}_t \).

Suppose not. Then we have

\[
\sum_{\alpha \in Maps_t} c_\alpha x_\alpha \in I
\]

for some \( \{ c_\alpha \}_{\alpha \in Maps_t} \subseteq A \) such that \( c_\alpha \neq 0 \) for at least one \( \alpha \). Take a minimal \( \alpha_0 \) of such, and consider the following substitution:

\[
x_{ij} \mapsto \begin{cases} 
1 & \text{(if } \alpha_0(i) = j) \\
0 & \text{(otherwise)}.
\end{cases}
\]
Then every element in $I$ is evaluated to 0, and $c_\alpha x_\alpha$ is evaluated to:

\[
\begin{cases}
c_{\alpha_0} & \text{(if } \alpha = \alpha_0) \\
0 & \text{(otherwise)}.
\end{cases}
\]

because of the minimality of $\alpha_0$. Thus we have $c_{\alpha_0} = 0$, a contradiction. ■

We aim to show that no $a \in A \setminus \{0\}$ is in $O_t$ ($t \leq m/2$) below.

**Definition 28.** For $t \leq m$, let $O_t$ be the set of $f \in A[\bar{x}]$ such that $f$ has a degree $\leq t$ PC-proof from $\text{injPHP}_m^M[A]$.

Towards it, the following notion is useful to describe the rewriting procedure of polynomials in concern:

**Definition 29.** Let $\alpha \in Maps$. A pigeon dance of $\alpha$ is the following non-deterministic process:

- Take the first (i.e. the smallest) pigeon $i_1 \in \text{dom}(\alpha)$ and move it to any unoccupied hole $j$ such that $j > \alpha(i_1)$.
- Then take the second smallest pigeon $i_2 \in \text{dom}(\alpha)$ and move it to any currently unoccupied hole larger than $\alpha(i_2)$, etc., as long as this is possible.

We say pigeon dance is defined on $\alpha$ if this process can be completed for all the pigeons in $\text{dom}(\alpha)$.

**Definition 30.** Let $Maps^*$ be the set of all partial maps $\alpha : [M] \to [m] \cup \{0\}$ such that $\alpha$ is injective outside $\alpha^{-1}(0)$. The partial bijection $\alpha \restriction_{\alpha^{-1}(\downarrow M)}$ is denoted by $\alpha^-$.

For $\alpha \in Maps^*$, extend the notation $x_\alpha$ as follows:

\[x_\alpha := x_{\alpha^-} \times \prod_{i : \alpha(i) = 0} \left(\sum_{j=1}^{m} x_{ij} - 1\right)\]

Note that $x_\alpha$ is no longer a monomial in general. We consider the following subsets of $S_t$:

**Definition 31.** For $t \leq m$, define:

1. $B_t \subseteq S_t$ as the set of all $x_\alpha \in Maps^*$ such that $\#\alpha \leq t$ and a pigeon dance is defined on $\alpha^-$. 
2. $C_t := B_t \setminus T_t$ and $\Delta_t := B_t \cap T_t$, that is, $\Delta_t$ consists of the monomials $x_\alpha$ for $\alpha \in Maps_t$ such that a pigeon dance is defined on $\alpha$.

Now, Corollary 25 is an immediate consequence of the following lemma since $1 \in \Delta_t$:
Lemma 32. For $t \leq m/2$,

$$\hat{S}_t = \hat{O}_t \oplus A\hat{\Delta}_t, \quad \hat{O}_t = A\hat{C}_t$$

as $A$-modules. In particular, any non-zero scalar in $A$ does not belong to $O_t$.

Proof. First, we show that $\hat{B}_t = \hat{C}_t \cup \hat{\Delta}_t$ spans $\hat{S}_t$. For the monomials

$$x_\gamma = x_{i_1,j_1} \cdots x_{i_k,j_k} \quad \text{and} \quad x_\delta = x_{u_1,v_1} \cdots x_{u_l,v_l} \quad (i_1 < \cdots < i_k \& u_1 < \cdots < u_l)$$

from $T_t$, define a partial ordering $x_\gamma \preceq x_\delta$ by the condition that:

- either $k < l$, or $k = l$ and for the largest $w$ such that $j_w \neq v_w$ it holds that $j_w < v_w$.

Claim 33. The monomial $x_\gamma$ can be expressed as

$$\hat{x}_\gamma = \sum_{x_\alpha \in X} c_\alpha \hat{x}_\alpha + \sum_{x_\beta \in Y} c_\beta \hat{x}_\beta$$

in $\hat{S}$ for some $X \subseteq C_t$ and $Y \subseteq \Delta_t$, and non-zero coefficients $c_\alpha$’s from $A$. (Note that $X \cap Y = \emptyset$ by definition of $C_t$ and $\Delta_t$.) Further, for all $x_\alpha \in X$ and $x_\beta \in Y$, $\text{dom}(\alpha) \cup \text{dom}(\beta) \subseteq \text{dom}(\gamma)$.

We may assume $i_1 < \cdots < i_k$ in $x_\gamma$ above and also $x_\gamma \notin \Delta_t$. We use induction on $\preceq$. Assume the claim holds for all terms $\preceq$-smaller than $x_\gamma$. In the following, we omit the symbol $(\hat{\cdot})$ representing the quotient map for readability. In $\hat{S}$, rewrite $x_\gamma$ as

$$x_{i_2,j_2} \cdots x_{i_k,j_k} - \sum_{j_1' < j_1} x_{i_1,j_1'} \cdots x_{i_k,j_k} - \sum_{j_1' > j_1 \text{ and } j_1' \notin \{j_2, \ldots, j_k\}} x_{i_1,j_1'} \cdots x_{i_k,j_k}$$

$$+ \left( \sum_{j=1}^m x_{i_1,j} - 1 \right) x_{i_2,j_2} \cdots x_{i_k,j_k}.$$

The first term and the terms in the first summation are all $\preceq$-smaller than $x_\gamma$, and their domain is included in $\text{dom}(\gamma)$. Thus, the statement for them follows by the induction hypothesis. Moreover, the statement for the first term implies that for the last term. Note that $x_\alpha \in B_{t-1}$ implies $\left( \sum_{j=1}^m x_{i_1,j} - 1 \right) x_\alpha \in AB_t + I$.

The collection of all the terms in the second summation can be interpreted as describing all possible moves of $i_1$ in the attempted pigeon dance of $\gamma$. To simulate other steps in all possible pigeon dances, rewrite each of these terms analogously using (4) for $i_2$, and so on. We have assumed $x_\gamma \notin \Delta_t$ that the pigeon dance cannot be completed. Therefore, the rewriting procedure must eventually produce only terms $\preceq$-smaller than $x_\gamma$. This completes the proof of Claim 33.
Next, we establish the linear independence of $\hat{B}_t = \hat{C}_t \cup \hat{\Delta}_t$. It suffices to show
\[
\#B_t \leq \#T_t = \#\hat{T}_t
\]
since $\hat{B}_t$ spans $\hat{S}_t$, $\hat{T}_t$ is its basis, $\#\hat{B}_t \leq \#B_t$, and $A$ is finite. Note that $\#\hat{B}_t = \#B_t = \#T_t$ follows.

Towards the above inequality, consider another procedure minimal pigeon dance, which is described as follows: given $\alpha \in \text{Maps}^*$, it is defined by the following instructions:

1. Put $\alpha_1 := \alpha$.
2. For $i = 1, \ldots, M$, if $i \in \text{dom}(\alpha_i)$, move it to the smallest free hole $j > \alpha_i(i)$ and let $\alpha_{i+1}$ be the resulting map. If $i \notin \text{dom}(\alpha_i)$, do nothing and put $\alpha_{i+1} := \alpha_i$.
3. $D(\alpha)$ is the result of this process applied to $\alpha$.

The following claims are purely combinatorial results on minimal pigeon dance, and the coefficient ring $A$ does not matter, so we state them without proof. See the proof of Lemma 16.2.2 in [13] for concrete proofs.

Claim 34. For all $t \leq m/2$, $D$ is defined on the whole of $B_t$.

Claim 35. $D$ is an injective map from $B_t$ into $T_t$ for $t \leq m/2$.

Claim 35 implies $\#B_t \leq \#T_t$.

It remains to show that $\hat{C}_t$ is a basis of $\hat{O}_t$. We already know that $\hat{C}_t$ is $A$-linearly independent, so we focus on proving $\hat{C}_t$ spans $\hat{O}_t$. Clearly $C_t \subseteq O_t$ and $AC_t$ contains all the axioms [14] in injPHP$^M_m[A]$ and is closed under the addition rule of $PC$. For the closure of the space under the multiplication rule, assume that $x_{\alpha} \in C_t$, $s = \deg(x_{\alpha}) < t$.

It suffices to show that $x_{ij}x_{\alpha} \in AC_{s+1} + I$, which implies $\hat{f}x_{\alpha} \in A\hat{C}_t$ for each monomial $f$ with $\deg(f) + \deg(x_{\alpha}) \leq t$ by induction on $\deg(f)$ and for each $f \in A[\bar{x}]$ with $\deg(f) + \deg(x_{\alpha}) \leq t$ since $A\hat{C}_t$ is closed under addition and scalar product. We use induction on $s$. By the definition of $C_t$, we can write $x_{\alpha} = x_{\beta}(1 - \sum_{j=1}^{m} x_{i'j})$ for some $i' \in [M]$. As $\deg(x_{\beta}) < \deg(x_{\alpha}) = s$, $x_{ij}x_{\beta} \in AB_s + I$ by Claim 33 if $x_{\beta} \in T_{s-1}$ and by induction hypothesis if $x_{\beta} \in C_{s-1}$. Note that the degree does not increase. Multiplying $(1 - \sum_{j=1}^{m} x_{i'j})$, we have $x_{ij}x_{\alpha} \in AC_{s+1} + I$.

3 On Question [1]

As for Question [1], the author conjectures the following:
Conjecture 1.

\[ F_c + UCP_{k,d} \not\vdash_{\text{poly}(n)} \text{injPHP}_n^{n+1}. \]

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

If this conjecture is true, then it follows that \( V_0 + UCP_{l,d} \not\vdash \text{injPHP}_n^{n+1} \) by the witnessing theorem and the translation theorem. In this section, we provide a sufficient condition to prove this conjecture. Our strategy is to adapt the proof technique of Ajtai’s theorem to the situation. We define \( \text{injPHP}_k \)-tree and a \( k \)-evaluation using \( \text{injPHP}_k \)-tree, and show that a Frege-proof of \( \text{injPHP}_n^{n+1} \) admitting \( UCP_{k,d} \) as an axiom scheme cannot have \( o(n) \)-evaluation. Taking the contrapositive, we obtain our sufficient condition.

We start with introducing the following notions:

**Definition 36.** Let \( D \) and \( R \) be disjoint sets. A partial injection from \( D \) to \( R \) is a set \( \rho \) 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 \( j \in R \), 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 \( \rho \) give a partial bijection from \( D \) to \( R \). We denote it by \( \rho_{\text{bij}} \). Also, we set \( \rho_{\text{sing}} := \rho \setminus \rho_{\text{bij}} \).

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

For two partial injections \( \rho \) and \( \tau \) from \( D \) to \( R \),

1. \( \rho \parallel \tau \) if and only if \( \rho \cup \tau \) is again a partial injection.

2. \( \rho \perp \tau \) if and only if \( \rho \parallel \tau \) 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. \( \sigma \tau := \sigma \cup \tau \).

Now, we introduce an analogy of PHP-trees in this context:

**Definition 37.** Let \( D \) and \( R \) be disjoint finite sets. An injPHP-tree over \((D,R)\) is a vertex-labeled and edge-labeled 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 labeled by “$i \mapsto ?$” having $\#R$ children and each of its edges corresponding to each label “$(i, j)$” ($j \in R$), and the subtree which the child under the edge labeled by “$(i, j)$” induces is an $injPHP$-tree over $(D \setminus \{i\}, R \setminus \{j\})$, then the whole labeled tree is again an $injPHP$-tree over $(D, R)$.

3. If the root is labeled by “? $\mapsto j$” having $(\#D + 1)$ children and each of its edges corresponding to each label “$(i, j)$” ($i \in D$) and “$(j)$,” and the subtree which the child under the edge indexed by $(i, j)$ induces is an $injPHP$-tree over $(D \setminus \{i\}, R \setminus \{j\})$ while the subtree which the child under the edge labeled by “$(j)$” 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 $\text{height}(T)$ and the set of its branches by $\text{br}(T)$.

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

**Convention 38.** When $T$ is an $injPHP$-tree over $(D, R)$, each branch $b \in \text{br}(T)$ 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 $b$.

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 assume $D_m$ and $R_n$ are disjoint for any $m, n \in \mathbb{N}$.

**Definition 39.** For $m > n$, $\mathcal{M}_n^m$ denotes the set of all partial injections from $D_m$ to $R_n$.

**Definition 40.** Let $\rho \in \mathcal{M}_n^m$ ($m > n$). Let $T$ be an $injPHP$-tree over $(D_m, R_n)$. We define the restriction $T^\rho$ as the $injPHP$-tree over $(D_m \setminus \text{dom}(\rho), R_n \setminus \text{ran}(\rho))$ obtained from $T$ by deleting the edges with label incompatible with $\rho$, contracting the edges whose label are contained in $\rho$ (we leave the label of the child), and taking the connected component including the root of the tree.

In particular, we are interested in shallow $injPHP$-trees. The main reason is the following Lemma 42.

**Definition 41.** For $\tau \in \mathcal{M}_n^m$ such that $\tau || \rho$, we set

$$\tau^\rho := \tau \setminus \rho.$$  

**Lemma 42.** Let $T$ be an $injPHP$-tree and $\rho \in \mathcal{M}_n^m$ ($m > n$). If $\text{height}(T) \leq n - \#\rho$, then the map

$$\{b \in \text{br}(T) \mid b || \rho\} \to \text{br}(T^\rho); \ b \mapsto b^\rho$$

is bijective.
Proof. First, we observe that $b^\rho \in br(T^\rho)$ if $b \in br(T)$ satisfies $b||\rho$. Indeed, no edge in $b$ is deleted by the restriction with $\rho$ since $b||\rho$, although some edges in $b$ may be contracted.

Next, we see the above map $b \mapsto b^\rho$ is injective. Indeed, if $b \neq b' \in br(T)$, $b||\rho$, and $b'||\rho$, then $b \nparallel b'$. Let $\pi \in b$ and $\pi' \in b'$ witness $b \nparallel b'$, that is, one of the following holds:

- $\pi = \langle i, j \rangle$, $\pi' = \langle i, j' \rangle$, and $j \neq j'$.
- $\pi = \langle i, j \rangle$, $\pi' = \langle i', j \rangle$, and $i \neq i'$.
- $\{\pi, \pi'\} = \{(i, j), (j)\}.$

Since $b||\rho$ and $b'||\rho$, we have $\pi', \pi \notin \rho$, and therefore $\pi \in b^\rho$ and $\pi' \in (b')^\rho$ follow. It implies $b^\rho \nparallel (b')^\rho$.

Lastly, we show that $b \mapsto b^\rho$ is surjective. Let $r \in br(T^\rho)$. By definition of $T^\rho$, there exists a vertex $v$ of $T$ such that $a||\rho$ and $r = a^\rho$, where $a$ is the partial injection induced by the path from the root to $v$ in $T$. Let $v$ be the most distant from the root among such. It suffices to show that $v$ is actually a leaf of $T$, and therefore $a \in br(T)$. Suppose $v$ is not a leaf of $T$. If $h$ is the height of $v$, then $h < n - \#\rho$ by assumption. It implies $\#a + \#\rho < n$. Hence, whatever the label of $v$ is, there exists an edge from $v$ whose label is compatible with $\rho$, contradicting the maximality of $v$.

Definition 43. In the setting of the previous Lemma, we denote the inverse mapping by:

$$br(T^\rho) \to \{b \in br(T) \mid b||\rho\}; \quad r \mapsto r^{-\rho}.$$ 

Definition 44. Let $\rho \in M_n^m$ ($m > n$). For $\{r_{ij}\}_{i \in D_m, j \in R_n}$-propositional formula $\varphi$ (by a natural identification of variables, we regard each variable $r_{ij}$ is utilized to construct the propositional formula $injPHP_n^m$), we define the restriction $\varphi^\rho$ by applying $\varphi$ the following partial assignment: for each $i \in [m]$ and $j \in [n]$,

$$r_{ij} \mapsto \begin{cases} 1 & (\text{if } \langle i, j \rangle \in \rho) \\ 0 & (\text{if } \{\langle i, j \rangle\} \nparallel \rho) \\ r_{ij} & (\text{otherwise}) \end{cases}$$

For a set $\Gamma$ of $\{r_{ij}\}_{i \in D_m, j \in R_n}$-propositional formulae, define

$$\Gamma^\rho := \{\varphi^\rho \mid \varphi \in \Gamma\}.$$ 

Example 45. Let $\rho \in M_n^m$ ($m > n$). Then, by suitable change of variables, $(injPHP_n^m)^\rho$ is equivalent to $injPHP_n^{m-\#\text{dom(}\rho\})$ (over $AC^0$-Frege system, mod poly$(m, n)$-sized proofs).

Definition 46. Let $m > n$. Let $T$ be an $injPHP$-tree over $(D_m, R_n)$ with height $h$. Given a set $S \subseteq br(T)$ and a family $(T_b)_{b \in br(T)}$ of $injPHP$-trees
where each $T_b$ is over $(D_m \setminus \text{dom}(b), R_n \setminus \text{ran}(b))$, we define the concatenated tree

$$T * \sum_{b \in S} T_b$$

as follows: for each $b \in S$, concatenate $T_b$ under $b$ in $T$ identifying the leaf of $b$ and the root of $T_b$ (and leaving the label of the root of $T_b$).

For two $injPHP$-trees $T$ and $U$ over $(D_m, R_n)$, we define

$$T * U := T * \sum_{b \in \text{br}(T)} U^b.$$

**Lemma 47.** In the setting of the previous Definition, the following map is a bijection:

$$\{(b, b') \mid b \in S, b' \in \text{br}(T_b)\} \cup (\text{br}(T) \setminus S) \to \text{br} \left( \sum_{b \in S} T_b \right):$$

\[
\begin{align*}
(b, b') & \mapsto bb' \\
\hat{b} & \mapsto \hat{b}
\end{align*}
\]

**Proof.** Clear. \(\blacksquare\)

**Definition 48.** Let $\Gamma$ 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 $\Gamma$ is a map

$$T : \varphi \in \Gamma \mapsto T_\varphi$$

satisfying the following:

1. Each $T_\varphi$ is a labeled $injPHP$-tree over $(D_m, R_n)$ with label set \{0, 1\} and height \(\leq k\).
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 $\text{br}_1(T_{r_{ij}}) = \{(i, j)\}$.
5. $T_{\neg \varphi} = T_{\neg \varphi}'$, that is, $T_{\neg \varphi}$ is obtained from $T_\varphi$ by flipping the labels 0 and 1.
6. $T_{\bigvee_{i \in I} \varphi_i}$ (where each $\varphi_i$ does not begin from $\lor$) represents $\bigcup_{i \in I} \text{br}_1(T_{\varphi_i})$. Here, we say a \{0, 1\}-labeled $injPHP$-tree $T$ represents a set $\mathcal{F}$ of partial injections if and only if the following hold:

(a) For each $b \in \text{br}_1(T)$, there exists a $\sigma \in \mathcal{F}$ such that $\sigma \subseteq b$.
(b) For each $b \in \text{br}_0(T)$, every $\sigma \in \mathcal{F}$ satisfies $\sigma \perp b$.  

19
Example 49. Given a list $F = \{\sigma_1, \ldots, \sigma_N\}$, where $\sigma_1, \ldots, \sigma_N$ are partial injections from $D$ to $R$, we define the $\{0, 1\}$-labeled $injPHP$-tree $T_F$ over $(D, R)$ inductively as follows:

1. If $F$ is empty, $T_F := T_0$.
2. If some $\sigma_i$ is an empty map, $T_F := T_1$.
3. Otherwise, ask where to go for each $v \in v(\sigma_1)$. Let $T$ be the obtained $injPHP$-tree.
4. For each branch $b \in br(T)$, consider $F^b$ below:
   $$F^b := \{\sigma^b_i \mid v(b) \in v(\sigma_i)\}.$$

   Construct $T_{F^b}$ over $(D \setminus \text{dom}(b), R \setminus \text{ran}(b))$ inductively, and set
   $$T_F := T \ast \sum_{b \in br(T)} T_{F^b}.$$ 

$T_F$ clearly represents $F$ (we regard $F$ as a set here).

Definition 50. Let $T = (S, L)$ be a labeled $injPHP$-tree over $(D_m, R_n) \ (m > n)$. Let $\rho \in \mathcal{M}_m^n$ and assume $\text{height}(T) \leq n - \#\rho$. Then the restricted labeled $injPHP$-tree $T^\rho = (S', L')$ is defined as follows:

$$S' := S^\rho, \quad L'(r) := L(r^\rho).$$

Example 51. If a $\{0, 1\}$-labeled $injPHP$-tree $T$ over $(D_m, R_n) \ (m > n)$ represents $F$, $\rho \in \mathcal{M}_m^n$, and $\text{height}(T) \leq n - \#\rho$, then $T^\rho$ represents $F^\rho$. Indeed, for $r \in br_1(T^\rho)$, there exists $\sigma \in F$ such that $\sigma \subseteq r^\rho$. Hence $\sigma \parallel \rho$ and it gives $\sigma^\rho \subseteq F^\rho$, $\sigma^\rho \subseteq b^\rho$. On the other hand, for $r \in br_0(T^\rho)$, each $\sigma \in F$ satisfies $\sigma \perp r^\rho$. Therefore, for all $\sigma$ such that $\sigma \parallel \rho, \sigma^\rho \perp (r^\rho)^\rho = r \rho$ holds.

Proposition 52. Let $T$ be a $k$-evaluation of a subformula-closed set $\Gamma$ of $\{r_{ij}\}_{i \in \mathbb{N}, j \in \mathbb{N}}$-formulae ($m > n$), $\rho \in \mathcal{M}_m^n$, $k \leq n - \#\rho$.

Consider
$$U_\varphi := (T_\varphi)^\rho.$$ 

Note that the RHS is the restricted labeled $injPHP$-tree.

$U_\varphi$ is an $injPHP$-tree over $(D_m \setminus \text{dom}(\rho), R_n \setminus \text{ran}(\rho))$, which can be regarded as $(D_{m - \# \text{dom}(\rho)}, R_{n - \# \text{ran}(\rho)})$. In particular, we can regard $U_\varphi$ as a $k$-evaluation of $\Gamma^\rho$ of $\{r_{ij}\}_{i \in \mathbb{N}, j \in \mathbb{N}}$-formulae.

Proof. Clear. \hfill \blacksquare

Theorem 53. Let $f : \mathbb{N} \rightarrow \mathbb{N}$ 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 $\pi_n$ proves $injPHP^f(n)$ using $UCP^\varnothing_0$ 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 of $\Gamma_n$ using $injPHP$-trees over $(D_{f(n)}, R_n)$, where $\Gamma_n$ is the set of all subformulae appearing in $\pi_n$. 

20
Proof. Suppose otherwise. There exist $o(n)$-evaluations $T^n$ of $\Gamma_n$. Fix a large enough $n$, and we suppress the superscript $n$ of $T^n$, and denote it simply by $T$.

For $\varphi \in \Gamma_n$, define

$$T \models \varphi : \iff br_1(T_{\varphi}) = br(T_{\varphi}).$$

Then, we can show the following claims analogously with Lemma 15.1.7 and Lemma 15.1.6 in [13]:

**Claim 54.** There exists a constant $c > 0$, depending only on the formalization of the Frege system we use, such that the following holds: if $\varphi$ is derived from $\psi_1, \ldots, \psi_k \in \pi_n$ by a Frege rule in $\pi_n$, $\forall i \in [k].T \models \psi_i$, and $\forall i \in [k].\text{height}(T_{\varphi}) \leq n/c$, then $T \models \varphi$.

**Claim 55.** $br_1(T_{injPHP_n^{[\pi(n)]}}) = \emptyset$. In particular, $T \not\models injPHP_n^{[\pi(n)]}$.

Also, the following fact is useful:

**Claim 56.**

$$T \models \bigwedge_{i=1}^L \varphi_i \implies \forall i \in [L]. T \models \varphi_i.$$  

**Proof of the claim.** The hypothesis means

$$T \models \neg \bigvee_{i=1}^L \neg \varphi_i,$$

that is,

$$br_0(T_{\bigvee_{i=1}^L \neg \varphi_i}) = br(T_{\bigvee_{i=1}^L \neg \varphi_i}).$$

Therefore, for each $b \in br(T_{\bigvee_{i=1}^L \neg \varphi_i})$ and $r \in \text{br}_1(T_{\neg \varphi_i})$, $b \perp r$ holds. Now, assume some $br_0(T_{\varphi_i})$ is nonempty, and $r_0$ be one of its elements. Since

$$\#r_0 \leq o(n) \quad \text{and} \quad \text{height}(T_{\bigwedge_{i=1}^L \neg \varphi_i}) \leq o(n),$$

there exists a branch $b \in br(T_{\bigwedge_{i=1}^L \neg \varphi_i})$ such that $b || r_0$, which is a contradiction. 

Therefore, there exists an instance

$$I = UCP_{k,d}^{[\psi_{i,j,e}]} \in \pi_n$$

such that $T \not\models I$. Hence, $k \not\equiv 0 \pmod{d}$. By restricting the formulae and $T$ by some $\rho \in \text{br}_0(T_i)$, we obtain the proof $\pi^n_\rho$ of $(injPHP^{[\pi(n)]})^\rho$ and the $o(n)$-evaluation $T^\rho$ of $\Gamma^n_\rho$ (note that $\#\rho \leq o(n)$, hence $T^\rho$ is well-defined). Therefore,
we may assume that \( \text{br}_0(T_I) = \text{br}(T_I) \).

Let

\[
S_{i,j,e} := T_{\psi_{i,j,e}},
S_e := T_{\forall (i,j) \in [l] \times [d] \psi_{i,j,e}},
S_{i,j} := T_{\forall e \in [k] \psi_{i,j,e}},
P_i := T_{\neg \forall e \in [k] \psi_{i,j,e}},
N_i := T_{\forall e \in [d] \forall e \in [k] \psi_{i,j,e}},
U_i := T_{(\neg \forall e \in [d] \neg \forall e \in [k] \psi_{i,j,e}) \lor (\neg \forall e \in [d] \forall e \in [k] \psi_{i,j,e})}.
\]

(i \in [l], j \in [d], e \in [k])

Since \( \text{br}_0(T_I) = \text{br}(T_I) \), we observe the following facts:

1. For each \( e \in [k] \), \( T \models \forall (i,j) \in [l] \times [d] \psi_{i,j,e} \), that is, every \( b \in \text{br}(S_e) \) has \((i,j) \in [l] \times [d] \) and \( b' \in \text{br}_1(S_{i,j,e}) \) such that \( b' \subseteq b \).

2. For each \( e \in [k] \) and \((i,j) \neq (i',j') \in [l] \times [d] \), every pair of branches \( b \in \text{br}_1(S_{i,j,e}) \) and \( b' \in \text{br}_1(S_{i',j',e}) \) satisfies \( b \perp b' \).

3. For each \( e \neq e' \in [k] \) and \((i,j) \in [l] \times [d] \), each \( b \in \text{br}_1(S_{i,j,e}) \) and \( b' \in \text{br}_1(S_{i,j,e'}) \) satisfies \( b \perp b' \).

4. For each \( i \in [l] \), \( T \models (\neg \forall e \in [d] \forall e \in [k] \psi_{i,j,e}) \lor (\neg \forall e \in [d] \forall e \in [k] \psi_{i,j,e}) \), that is, every \( b \in \text{br}(U_i) \) is an extension of some \( b' \in \text{br}_1(P_i) \) or some \( b' \in \text{br}_1(N_i) \). In the former case, \( b \) is incompatible with every \( b'' \in \bigcup_j \text{br}_0(S_{i,j}) \). In the latter case, \( b \) is incompatible with every \( b'' \in \bigcup_j \text{br}_1(S_{i,j,e}) \). Therefore, the two cases are mutually disjoint. Indeed, if \( b \) satisfies the both cases, then take \( b' \in \text{br}(S_{i,j}) \) such that \( b \parallel b' \) (which exists since \( \#b \) and \( \text{height}(S_{i,j}) \) are both \( o(n) \)). It follows that \( b' \in \text{br}_1(S_{i,j}) \), and therefore \( b' \) is an extension of some \( b'' \in \bigcup_e \text{br}_1(S_{i,j,e}) \), which contradicts the observation of the latter case.

With the observations above, we construct labeled \( \text{injPHP} \)-trees \((X_{i,j})_{(i,j) \in [l] \times [d]} \) and \((Y_{e})_{e \in [k]} \) as follows

- We define \( Y_e \) for fixed \( e \) first. Consider \( S_e \). By observation \([\text{i}][\text{and}][\text{ii}] \) and each \( b \in \text{br}(S_e) \) has a unique \((i_b,j_b) \in [l] \times [d] \) such that \( b \) is an extension of some \( b' \in \text{br}_1(S_{i_b,j_b,e}) \). Consider the tree

\[
S_e \ast \sum_{b \in \text{br}(S_e)} (U_{i_b} \ast S_{i_b,j_b})^b
\]

(here, we have concatenated the trees, ignoring their labels).

Label each branch extending \( b \in \text{br}(S_e) \) with \((i_b, j_b, e) \). Let \( Y_e \) be the resulting labeled \( \text{injPHP} \)-tree. Note that \( \text{height}(Y_e) \) is still \( o(n) \).

22
• Next, we define $X_{i,j}$ for fixed $(i,j) \in [l] \times [d]$. Consider $U_i$. Let $B \subseteq br(U_i)$ be the set of all $b \in br(U_i)$ satisfying the former case of observation $4$. Consider the tree $\tilde{X}_{i,j} := U_i \ast \sum_{b \in B} S^b_{i,j}$. Each branch $b \in br(\tilde{X}_{i,j})$ satisfies one of the following:

1. $\tilde{b} \in br(U_i) \setminus B$.

2. Otherwise, by Lemma $12$ we can decompose $\tilde{b} = bs^b$ ($b \in B, s \in br(S_{i,j})$). Since $b$ is an extension of some $b' \in br_1(P^c)$, we have $br_1(S^b_{i,j}) = br(S^b_{i,j})$. It implies $s \in br_1(S_{i,j})$. Therefore, by observation $3$ each $s^b \in br(S^b_{i,j})$ has a unique $e_s^b \in [k]$ such that $s$ extends some $e''_s^b \in br_1(S_{i,j,e^c})$.

Let $\tilde{B}$ be the all branches of $\tilde{X}_{i,j}$ satisfying the second item. We define

$$\hat{X}_{i,j} := \tilde{X}_{i,j} \ast \sum_{b \in \tilde{B}} (S^b_{i,j})^b.$$  

We label each branch $b \in br(\hat{X}_{i,j})$ as follows and define $X_{i,j}$ to be the obtained labeled $injPHP$-tree.

1. If $b \in br(U_i) \setminus B$, then label it with the symbol $\bot$.

2. Otherwise, there exists a unique $\tilde{b} \in \tilde{B}$ such that $\tilde{b} \subseteq b$. Label the branch $b$ with $(i,j,e^b)$.

By observation $3$ we see that $(X_{i,j})_{i \in [l], j \in [d]}$ and $(Y_e)_{e \in [k]}$ satisfy the following:

• For each $ibr_{\bot}(X_{i,1}) = \cdots = br_{\bot}(X_{i,d})$.

• For each $i,j,e$, $br_{(i,j,e)}(X_{i,j}) = br_{(i,j,e)}(Y_e)$ (as sets of partial injections).

The second item is justified as follows. By Lemma $12$ Lemma $47$ and the definitions of $Y_e$ and $X_{i,j}$, the following are bijections for each $i,j,e$:

$$\left\{ (b, \beta, s) \in br(S_e) \times br(U_i) \times br(S_{i,j}) \mid \exists b' \in br_1(S_{i,j,e}).(b' \subseteq b), \beta || s, b || s \right\}$$

$\rightarrow br_{(i,j,e)}(Y_e); (b, \beta, s) \mapsto b(\beta s)$. 

$$\left\{ (\beta, s, b) \in br(U_i) \times br(S_{i,j}) \times br(S_e) \mid \exists b' \in br_1(P^c_i).\tilde{b} \subseteq \beta, \exists b'' \in br_1(S_{i,j,e}).(b'' \subseteq s), \beta || s, b || s \right\}$$

$\rightarrow br_{(i,j,e)}(X_{i,j}); (\beta, s, b) \mapsto (\beta s)b$.

Hence, in order to see $br_{(i,j,e)}(X_{i,j}) = br_{(i,j,e)}(Y_e)$, it suffices to show the following: let $\beta \in br(U_i), s \in br(S_{i,j}), b \in br(S_e)$. If $\beta || s$ and $\beta s || b$, then the following are equivalent:
1. There exists \( b' \in br_1(S_{i,j,e}) \) such that \( b' \subseteq b \).

2. \( \beta \) is an extension of some \( \hat{b} \in br_1(P_i) \), and \( s \) is an extension of some \( b'' \in br_1(S_{i,j,e}) \).

We consider \([1] \Rightarrow [2]\) first. Suppose \( \beta \) is not an extension of any \( \hat{b} \in br_1(P_i) \), \( \beta \in br(U_i) \), so it must be an extension of some \( r \in br_1(N_i) = br_0(N_i) \) by observation \([4]\) above. Thus we have \( r \perp b' \), and therefore \( \beta \perp b \), contradicting the assumption \( \beta \in [b] \). Hence, \( \beta \) is an extension of some \( \hat{b} \in br_1(P_i) = br_0(P_i) \).

Then, by observation \([1]\) and the assumption \( \beta \in [s] \), we have \( s \in br_1(S_{i,j}) \), which means \( s \) is an extension of some \( b'' \in br_1(S_{i,j,e}) \). This finishes the proof of \([1] \Rightarrow [2]\).

Next, we consider the converse. By observation \([1]\) there exist \( i' \), \( j' \) and \( b' \in br(S_{i',j',e}) \) such that \( b' \subseteq b \). Then we have \( b' \parallel [s] \) since \( b \in [s] \) follows from \( \beta \in [b] \). By observation \([2]\) \( (i, j) = (i', j') \) and \( b'' \parallel b'' \) follows. Since \( b'' \in br_1(S_{i,j,e}) \) by assumption, we have the converse.

Now, we construct a low-degree \( NS \)-refutation of \( \neg inj^{*}PHP^{f(n)-\# dom(\rho)}_{n-\# ran(\rho)} \).

By the properties of \( (X_{i,j})_{e \in [i,j] \in [d]} \) and \( (Y_{e,c})_{c \in [k]} \), the following holds:

\[
\sum_{(i,j) \in [i] \times [d]} \sum_{\alpha \in br(X_{i,j})} x_\alpha = \sum_{e \in [k]} \sum_{\beta \in br(Y_e)} x_\beta \pmod{d}.
\]

(Here, for a partial injection \( \rho \), \( x_\rho := (\prod_{(p,h) \in p_{bij}} x_{p,h})(\prod_{(h) \in p_{bij}, u_h}) \).

It is easy to see that for any \( \text{injPHP-tree } T \) over \( (D_M, R_m, \rho) \), \( \sum_{\alpha \in br(T)} x_\alpha = 1 \) has a \( NS \)-refutation from \( \neg inj^{*}PHP^{f(n)-\# dom(\rho)}_{n-\# ran(\rho)} \) with degree \( \leq \text{height}(T) \). Hence, we obtain a \( NS \)-proof of \( k = 0 \) from \( \neg inj^{*}PHP^{f(n)-\# dom(\rho)}_{n-\# ran(\rho)} \) over \( \mathbb{Z}/d\mathbb{Z} \) with degree \( o(n) \). Since \( k \neq 0 \pmod{d} \), it is a \( NS \)-refutation of \( \neg inj^{*}PHP^{f(n)-\# dom(\rho)}_{n-\# ran(\rho)} \) over \( \mathbb{Z}/d\mathbb{Z} \) with degree \( o(n) \). However, it contradicts Proposition \([2]\) and Corollary \([5]\).

Setting \( f(n) := n + 1 \) and taking the contrapositive of Theorem \([5]\), we obtain that an analogue of switching lemma for \( injPHP \)-trees suffices to prove Conjecture \([4]\).

**Corollary 57.** Assume \( F_c + UCP^{f,d}_{k} \vdash_{\text{poly}(n)} \text{injPHP}^{n+1} \) is witnessed by \( AC^{0} \)-proofs \((\rho_n)_{n \geq 1} \). Suppose there are partial injections \((\rho_n)_{n \geq 1}\) satisfying

- For each \( n, \rho_n \in M^{n+1}_n \).
- \( n - \# \text{ran}(\rho_n) \to \infty \) \((n \to \infty)\).
- There exist \( o(n - \# \text{ran}(\rho_n)) \)-evaluations \((T^n)_{n \geq 1} \) of \( \Gamma^n \), where \( \Gamma_n \) is the all subformula appearing in \( \pi_n \).

Then, we obtain a contradiction.
Note that an analog of switching lemma would give how to construct such $\rho_n$ above.

**Remark 58.** It will be good if we can prove such an analog for $injPHP$-trees; in that case, we can apply the previous theorem and prove that Conjecture 1 is valid. However, it seems implementing this approach is beyond the current proof techniques. The difficulty is relevant to that of the famous open problem: does $V^0 \vdash injPHP^{2n}_n$ hold?

### 4 On the strength of the oddtown theorem

The oddtown theorem is a combinatorial principle stating that there cannot be $n + 1$ orthogonal normal vectors in $F^n_q$. In other words, (regarding each $v \in F^n_q$ as the characteristic vector of a subset $S \subseteq [n]$) 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, the oddtown theorem and Fisher’s inequality (introduced in §5) were proposed as candidates for statements that are easy to prove in the extended Frege system but not in the Frege system ([6]). Standard proofs of them use linear-algebra methods, such as evaluating the number of linearly independent vectors of a given linear space, which do not seem easy to formalize in the bounded arithmetic $VNC^1$ (corresponding to polynomial-sized Frege proofs), and this was why they and some other combinatorial principles were presented as above candidates.

Actually, around the time [6] was published, a linear-algebra-free proof of Fisher’s inequality was already discovered, and I did not know it. See §5 for details and acknowledgment.

On the other hand, upper bounds of linear algebra methods were also given in a series of works. [18] and [19] gave natural bounded arithmetics $\mathbf{LA}$ and $\mathbf{LAP}$ capable of formalizing elementary arguments in linear algebra, formalized the matrix determinant by Berkowitz algorithm [5], and showed the following:

- Cayley-Hamilton, co-factor expansion, and an axiomatic definition of determinants (multi-linear, alternating, and $\det(I) = 1$ for unit matrices $I$) are equivalent over $\mathbf{LAP}$.
- Multiplicativity of determinants implies all above in $\mathbf{LAP}$.

[10] and [20] were recent breakthroughs in the area.

[10] gave a short proof of multiplicativity of determinants of $F$-matrices in the proof system $P_c(F)$, which manipulates arithmetical circuits, for general coefficient fields $F$. The results and the arguments in [10] also imply multiplicativity of determinant for $\mathbb{Z}$-matrices (or, equivalently, $\mathbb{Q}$-rational matrices) has quasipolynomial-sized Frege proofs. See the introduction of [10] for details.
carefully formalized the argument for $\mathbb{Z}$-matrices in $\text{VNC}^2$. Using the result of [20], we can show that $\text{VNC}^2$ proves the oddtown theorem, and therefore propositional translations have quasipolynomial-sized Frege proofs. See Proposition 61.

However, there is still room to investigate the precise strengths of the oddtown theorem and Fisher’s inequality in terms of bounded reverse mathematics. In this section, we focus on lower bounds for the oddtown theorem. We observe that a natural formalization of the oddtown theorem over $V^0$ is stronger than several combinatorial principles related to counting. Then, we try to analyze the relation between the oddtown theorem and $\text{Count}_n^p$ for $p$, which is not a 2-power.

**Definition 59.** Define the $\Sigma^B_0 \land \forall^A_0$-formula $\text{oddtown}(n, P, Q, R, S)$ as follows:

\[
\neg[\forall i \in [n+1].\forall j \in [n].(S(i, j) \leftrightarrow Q(i, j) \lor \exists e \in [n]^{(2)}(j \in^* e \land P(i, e)))
\land \forall i \in [n+1].\exists j \in [n].Q(i, j)]
\land \forall i \in [n+1].\forall j \neq j' \in [n].(\neg Q(i, j) \lor \neg Q(i, j'))
\land \forall i \in [n+1].\forall j \in [n].\forall e \in [n]^{(2)}(j \in^* e \to \neg Q(i, j) \lor \neg P(i, e))
\land \forall i \in [n+1].\forall e \neq e' \in [n]^{(2)}(e \cap e' \neq \emptyset \to \neg P(i, e) \lor \neg P(i, e'))
\land \forall i < i' \in [n+1].\forall j \in [n].(S(i, j) \land S(i', j) \leftrightarrow \exists e \in [n]^{(2)}(j \in^* e \land R(i, i', e)))
\land \forall i < i' \in [n+1].\forall e \neq e' \in [n]^{(2)}(e \cap e' \neq \emptyset \to \neg R(i, i', e) \lor \neg R(i, i', e'))
\]

Intuitively, $S$ above gives sets $S_i := \{ j \in [n] \mid S(i, j) \}$. $P$ 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 60.** Define the propositional formula $\text{oddtown}_n$ as follows:

\[
\text{oddtown}_n := \begin{cases} 
1 & (n = 0) \\
\neg[ \land_{i \in [n+1]} \land_{j \in [n]} \neg s_{ij} \lor q_{ij} \lor \land_{e,j \in [n]^{(2)}} p_{ie} \\
\land_{i \in [n+1]} \land_{j \in [n]} \neg s_{ij} \lor q_{ij} \\
\land_{i \in [n+1]} \land_{j \in [n]} \land_{e,j \in [n]^{(2)}} s_{ij} \lor \neg p_{ie} \\
\land_{i \in [n+1]} \land_{j \in [n]} q_{ij} \\
\land_{i \in [n+1]} \land_{j < j' \in [n]} \neg q_{ij} \lor \neg q_{ij'} \\
\land_{i \in [n+1]} \land_{j \in [n]} \land_{e,j \in [n]^{(2)}} s_{ij} \lor \neg p_{ie} \\
\land_{i \in [n+1]} \land_{e,j \in [n]^{(2)}} \neg p_{ie} \lor \neg p_{ie'} \\
\land_{i < i' \in [n+1]} \land_{j \in [n]} s_{ij} \lor \neg s_{ij} \lor \land_{e,j \in [n]^{(2)}} r_{ii'e} \\
\land_{i < i' \in [n+1]} \land_{j \in [n]} \land_{e,j \in [n]^{(2)}} s_{ij} \lor \neg r_{ii'e} \\
\land_{i < i' \in [n+1]} \land_{j \in [n]} \land_{e,j \in [n]^{(2)}} \neg r_{ii'e} \lor \neg r_{ii'e} \\
\land_{i < i' \in [n+1]} \land_{e,j \in [n]^{(2)}} \neg r_{ii'e} \lor \neg r_{ii'e} \end{cases} (n \geq 1)
\]

By a reason similar to that of Convention 83 we abuse the notation and write $\text{oddtown}_n$ to express $\text{oddtown}(n, P, Q, R, S)$, too.

We first observe an upper bound of the strength of $\text{oddtown}_n$:
Proposition 61. [A corollary of [20]]

\[ \text{VNC}^2 \vdash \text{oaddtown}(n, P, Q, R, S). \]

For the definition of \( \text{VNC}^2 \), see [8].

Proof Sketch. [20] showed that there exists a \( \Sigma^B_1 \)-definition \( \text{det}(A) = N \) of the matrix determinant, where both \( A \) and \( N \) are of set-sort, \( N \) is meant to be a binary representation of an integer, and \( A \) is meant to code a square matrix with integer coefficients, where each coefficient is represented by a binary expression, such that \( \text{VNC}^2 \) proves:

- Let \( A \) and \( B \) be strings coding square matrices with integer coefficients of the same size \((k \times k)\). Then \( \text{det}(A) \text{det}(B) = \text{det}(AB) \).
- \( \text{det}(A) \) can be computed by co-factor expansion concerning any row or column.

Focusing on the last digit of the integers involved, we can see that there exists a \( \Sigma^B_1 \)-definition \( \text{det}_{F_2}(A) = b \), where \( b \in \{0, 1\} \), and \( A \) is of set-sort, meant to code a square matrix with \( F_2 \)-coefficients satisfying the above two items.

Armed with this, we work in \( \text{VNC}^2 \) and show \( \text{oaddtown}_n \) as follows. Towards a contradiction, suppose \( n, P, Q, R, S \) violate \( \text{oaddtown}(n, P, Q, R, S) \). Let \( M \) be an \( F_2 \) matrix of size \((n + 1) \times n\) given by

\[
M_{ij} := \begin{cases} 
1 & \text{(if } S(i, j) \text{ holds)} \\
0 & \text{(otherwise)} 
\end{cases}
\]

Since \( \text{oaddtown}(n, P, Q, R, S) \) is violated, we have \( MM^t = I_{n+1} \) as \( F_2 \)-matrices, where \( I_{n+1} \) is a unit matrix of size \((n + 1) \times (n + 1)\). Note that \( \text{VNC}^2 \) is an extension of \( \text{VTC}^0 \) and can count cardinalities of bounded sets, which is sufficient to prove \( MM^t = I_{n+1} \). Consider the matrix \( A \) obtained by padding \( M \) by a zero column vector. \( A \) is of size \((n + 1) \times (n + 1)\), and \( AA^t = I_{n+1} \).

Taking determinants of both sides and applying multiplicativity of determinants, we have \( \text{det}_{F_2}(A) \text{det}_{F_2}(A^t) = \text{det}_{F_2}(I_{n+1}) \). However, \( A \) has a zero column vector, and \( A^t \) has a zero row vector. Therefore, by co-factor expansions, we have \( \text{det}_{F_2}(A) = \text{det}_{F_2}(A^t) = 0 \). On the other hand, it is elementary to see \( \text{det}_{F_2}(I_{n+1}) = 1 \), a contradiction. ■

Corollary 62. There exist \( 2^{O((\log n)^2)} \)-sized Frege proofs of \( \text{oaddtown}_n \).

Now, we focus on the lower bounds of the strength of \( \text{oaddtown}_n \). We start with the following simple observations:

Proposition 63. 1. \( V^0 + \text{oaddtown}_k \vdash \text{injPHP}_{n+1}^n \).

2. \( V^0 + \text{oaddtown}_k \vdash \text{Count}_n^2 \).
Proof. We first prove 1. Argue in $V^0$. We prove the contrapositive. Suppose there exists an injection $f : [n + 1] \to [n]$. Define

$$S_i := \{f(i)\}.$$

Then it violates oddtown$_n$.

We next prove 2. Argue in $V^0$. We prove the contrapositive. Suppose $[2n+1]$ is partitioned by 2-sets. Let $R$ be the 2-partition. Then setting $S_i := [2n+1] \ (i \in [2n+2])$, we can violate oddtown$^{2n+2}_n$ since $[2n+1] \cap [2n+1]$ can be 2-partitioned by $R$ while $[2n+1] \backslash \{2n+1\}$ has a natural 2-partition.

Remark 64. Observing the proof above, one may think that we might obtain another interesting formalization of the oddtown theorem imposing $\{S_i\}_{i \in [n+1]}$ to be a family of distinct sets. Let oddtown$'$ be this version. It turns out that:

1. $V^0 + \text{oddtown}_k \vdash \text{oddtown}'_n$.
2. $V^0 + \text{oddtown}'_k + \text{Count}^2_k \vdash \text{oddtown}_n$.
3. $V^0 + \text{oddtown}'_k \vdash \text{Count}^2_n$.

Hence, oddtown$_n$ and oddtown$'$$_n$ have the same strength over $V^0$.

The proof of the remark. The item 1 is clear.

We show the item 2. Work in $V^0 + \text{oddtown}'_k + \text{Count}^2_k$. Assume $\{S_i\}_{i=1}^{n+1}$ (where $S_i \subseteq [n]$) violates oddtown$_n$. Since each $S_i \cap S_{i'} (i < i')$ is 2-partitioned, it follows that $S_i \neq S_{i'}$. Indeed, if $S_i = S_{i'} =: S$, then both $S$ and $S \backslash \{s_0\}$ ($s_0 \in S$) is 2-partitioned by the hypothesis. Consider a straightforward bijection:

$$[2n-1] \cong ([n] \backslash S) \sqcup ([n] \backslash S) \sqcup S \sqcup (S \backslash \{s_0\}).$$

The right-hand side gives a natural 2-partition using those of $S$ and $S \backslash \{s_0\}$, and it induces a 2-partition of the left-hand side, which violates Count$^2_{n-1}$. Hence, it follows that each $S_i$ is distinct. However, it contradicts oddtown$'$$_n$. This shows the item 2.

Lastly, we show the item 3. Argue in $V^0$. Assume $R$ is a 2-partition of $[2n+1]$. Note that $R$ has a natural linear ordering induced by that of whole numbers. Define $\{S_i\}_{i=1}^{2n+2}$ as follows: it is easy to see that $R$ has at least four elements. Take distinct $r_1, r_2, r_3 \in R$. For each $i = 1, \ldots, 2n+1$, take the unique $j$ such that $\{i, j\} \in R$. Then,

Case 1. If $i < j$, set $S_i := [2n+1] \backslash \{i, j\}$.

Case 2. If $i > j$, set $S_i := [2n+1] \backslash \{(i, j) \cup s_i\}$, where $s_i$ is the successor of $\{i, j\}$ in $R$. If there is none (i.e. $\{i, j\} = \max R$), let $s_i$ be $\min R$. 28
Furthermore, we define $S_{2n+2} := [2n + 1] \setminus (r_1 \cup r_2 \cup r_3)$.

Now, we see that $\{S_i\}_{i=1}^{2n+2}$ violates $oddtown_{2n+2}$. Indeed, the $S_i$ are distinct, we can take natural 2-partitions leaving one element for each $S_i$, and we can obtain 2-partitions for each $S_i \cap S_j$ ($i < j$) removing at most five elements from $R$.

By theorem 8 and 9, we obtain

**Corollary 65.**

\[
V^0 + injPHP^{k+1}_k \not\vdash oddtown_n, \\
V^0 + Count^2_k \not\vdash oddtown_n.
\]

This raises the following natural problems:

**Question 3.**
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 $p$?

The author cannot answer these questions for now. However, we tackle the item 2 in the rest of this section.

By Proposition 63 and Theorem 7, it is easy to see:

**Corollary 66.** If $p$ is a power of 2, $V^0 + oddtown_k \vdash Count^p_n$.

The author conjectures that the converse of this corollary holds. Furthermore, the author conjectures the following:

**Conjecture 2.** For each $d \in \mathbb{N}$ and a prime $p \neq 2$,

\[
F_d + oddtown_k \not\vdash_{poly(n)} Count^p_n.
\]

Using Theorem 7 it is easy to see that Conjecture 2 implies the converse of Corollary 66. We give a sufficient condition to prove Conjecture 2:

**Theorem 67.** Let $p \in \mathbb{N}$ be a prime other than 2. Suppose

\[
F_d + oddtown_k \vdash_{poly(n)} Count^p_n.
\]

Then, for any large enough $n \not\equiv 0 \pmod{p}$, there exist $m = n^{O(1)}$ and a family $(f_{ij})_{i \in [m+1], j \in [m]}$ of polynomials over $\mathbb{F}_2$ such that the following equalities have NS-proofs over $\mathbb{F}_2$ from $\lnot Count^p_n$ with degree $O(1)$:

\[
\sum_{j \in [m]} f_{ij} = 1 \quad (i \in [m+1])
\]

\[
\sum_{j \in [m]} f_{ij} f_{i'j} = 0 \quad (i \neq i' \in [m+1])
\]
Here, $\neg \text{Count}_n^p$ (where $n \not\equiv 0 \pmod{p}$) means the following system of polynomials:

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

$(j \in [n] & e, e' \in [n]^{(p)} & e \perp e')$

Hence, if we can prove a non-constant degree lower bound for NS-proofs for the above system of equations, then Conjecture 2 is true.

Before the proof, we present a strategy for obtaining the constant degree bound above. We assume the basics of partial $p$-partitions, $p$-trees, and $k$-evaluations using $p$-trees. See section 15.5 in [13] for references. We also use the notations $br(T), T \models \varphi, T \ast \sum_{b \in S} T_b$, etc. as the straightforward analogous meanings to the ones given in [13].

The power of the notion comes from the following so-called switching lemma:

**Theorem 68** (Lemma 12.3.11 in [12]. Essentially by [14], [16].) Let $p \geq 2$. Then there exists a constant $c$ satisfying the following: let $H_1, \ldots, H_N$ be families of partial $p$-partitions of $[pn + r]$, where $0 \leq r < p$. Assume that $\#H_i \leq t \leq s$ for every $i \in [N]$, and

$$\frac{w^s}{t \cdot (n - w)^{c^s}} > N,$$

(5)

where $w \leq n$. Then there is a partial $p$-partition $\rho$ with $\#\rho = w$, such that for every $i \in [N]$ there exists a $p$-tree with height at most $p \cdot s$ representing $H_i^\rho$.

**Remark 69.** In the book [12], $r = 1$ is assumed, but the proof is straightforwardly extended to treat general $r < p$ since $p$ is a fixed constant here.

**Remark 70.** In the book [12], the notion $k$-complete system is used instead of $p$-trees, and therefore the precise definition of $k$-evaluation in it is different from the one given in [13]. However, the proof of Lemma 12.3.11 in [12] essentially constructs canonical $p$-trees $T_i$ representing $H_i$’s under “good” restrictions, and $br(T_i)$’s are the $k$-complete systems argued in [12]. In other words, an inequality corresponding to (5) can be extracted from the proof of Theorem 15.2.2 in [13].

The intertwine between several terminologies and notions is concisely mentioned in §4.4 of [1].

In particular, when $N = n^{O(1)}$, choosing a parameter $0 < \epsilon < 1/c$ and putting $w := n - n^\epsilon$, we can satisfy the inequality (5) by choosing sufficiently large $t = s = O(1)$. Applying Theorem 68 constantly many times, we obtain the following:

**Corollary 71.** [A counterpart of Theorem 12.4.3 in [12] when $\#\Gamma$ is just $n^{O(1)}$]

Let $e, d \geq 1$. Then, for sufficiently small $\epsilon > 0$, there exists a constant $k > 0$ satisfying the following:
• For sufficiently large $n$, if $\Gamma$ is a set of formulae of depth $\leq d$ whose variables are those used in $\text{Count}_{pn+r}^p$ $(0 \leq r < p)$, closed under the subformulae, and with size $\#\Gamma \leq n^\varepsilon$, then there is a partial $p$-partition $\rho$ with size $n - n^\varepsilon$ such that there exists a $k$-evaluation of $\Gamma^\rho$.

Here, $n^\varepsilon$ is rounded to an integer in an appropriate way.

Now, we move on to the proof of Theorem 67.

**Proof of Theorem 67** In this proof, we assume $p = 3$ for readability. Let proofs $(\pi_l)_{l \in \mathbb{N}}$ witness $F_d + \text{oddtown}_k \vdash_{\text{poly}(l)} \text{Count}^3_l$.

We focus on $l \not\equiv 0 \pmod{3}$. Let $l = 3n + r$ $(0 < r < 3)$. Let $\Gamma_l$ be the all subformulae appearing in $\pi_l$. Apply Corollary 71 for 3-trees, and obtain $\varepsilon > 0$ and a partial 3-partition $\rho$ with size $n^\varepsilon$ such that there exists an $O(1)$-evaluation $T$ of $\Gamma_l^\rho$, where $l$ is sufficiently large. Note that $(\text{Count}^3_l)^\rho$ can be identified as $\text{Count}_{3n^\varepsilon + r}^3$.

It suffices to construct $(f_{ij})$ in the claim for these sufficiently large $3n^\varepsilon + r$ instead of general $l$. Indeed, given sufficiently large integer $N \not\equiv 0 \pmod{3}$, take an integer $n$ satisfying

$$3n^\varepsilon + r < N \leq 3(n + 1)^\varepsilon + r,$$

where $N \equiv r \pmod{3}$ and $0 < r < 3$. If $(f_{ij})_{i \in [m+1], j \in [m]}$ is as claimed for $3(n + 1)^\varepsilon + r$, then applying a partial restriction given by a partial 3-partition leaving elements in $[N]$ in the universe $[3(n + 1)^\varepsilon + r]$, we get $(f_{ij})_{i \in [m+1], j \in [m]}$ for $N$. Since

$$m = (3(n + 1)^\varepsilon + r)^{O(1)} = (3n^\varepsilon + r)^{O(1)} = N^{O(1)},$$

the claim for general $N$ follows.

Now, we focus on constructing $(f_{ij})$ in the claim for sufficiently large $3n^\varepsilon + r$.

We renew the expression $3n^\varepsilon + r$ and write it as (new) $n$ from now on for readability, refreshing our mind.

Recall that the evaluation $T$ is sound for Frege rules in $\pi_n$, and it satisfies $T \not\models \text{Count}_{n}^3$ at the same time. It follows that some instance

$$I := \text{oddtown}_n[\sigma_{ij} / s_{ij}, \tau_{ij} / q_{ij}, \varphi_{ie} / p_{ie}, \psi_{iv_e} / r_{iv_e}]$$

in $\pi_n$ satisfies $T \not\models I$. Restricting $O(1)$-elements more if necessary, we may assume that actually $br_0(T_I) = br(T_I)$ holds.

Clearly, $m = n^{O(1)}$. For $i \in [m+1]$ and $j \in [m],

$$f_{ij} := \sum_{b \in br_1(T_{\pi_{ij}})} \prod_{e \in b} x_e.$$

We prove that these polynomials satisfy the required properties.
First, fix $i < i' < [m + 1]$. We construct a $NS$-proof of $\sum_{j=1}^{m} f_{ij} f_{i'j} = 0$ over $\mathbb{F}_2$ from the system $\neg Count^3_n$ For each $j \in [m]$, construct $U^1_j (j \in [m])$ as follows:

$$U^1_j := T_{\sigma_{ij}} \ast \sum_{b \in br_1(T_{\sigma_{ij}})} (T_{\sigma_{i'j}} \ast \sum_{b' \in br_1(T_{\sigma_{i'j}})} (T_{i,i'j})^{b'})^b,$$

where

$$T_{i,i'j} := T_{\neg \sigma_{ij} \lor \neg \sigma_{i'j} \lor \vee_{e,j \in [m]^{(2)}} T_{\psi_{i,e'}}.$$

Now, define $U_j (j \in [m])$ as follows:

- Consider each branch $r \in br(U^1_j)$ of the form $r = b(b')^d e'$, where
  
  $b \in br_1(T_{\sigma_{ij}}), b' \in br_1(T_{\sigma_{i'j}}), d \in br(T_{i,i'j}).$

Let $S^1_j$ be the set of all branches of $U^1_j$ of the above form. Since $d||bb'$ and

$$T \models \neg \sigma_{ij} \lor \neg \sigma_{i'j} \lor \vee_{e,j \in [m]^{(2)}} \psi_{i,e'},$$

$$T \models \neg \psi_{i,e'} \lor \neg \psi_{i',e'} (\forall e' \downarrow e).$$

There is a unique $e_r \in [m]^{(2)}$ such that

- $j \in e_r$, and
- $d$ is an extension of some $d' \in br_1(T_{\psi_{i,e_r}})$.

- Let $j'_{r,j}$ be the element of $e_r$ other than $j$ (that is, $e_r = \{j, j'_{r,j}\}$).

- We define $U^2_j := U^1_j \ast \sum_{r \in S^1_j} (T_{\sigma_{ij}} \lor \neg \psi_{i,e_r} \lor T_{\sigma_{i'j}} \lor \neg \psi_{i',e_r})^r$.

- Let $S^2_j \subseteq br(U^2_j)$ be the set of all branches extending some element of $S^1_j$.

- For each
  
  $u = rs^r \in S^2_j (r \in S^1_j, s \in br(T_{\sigma_{i'j}} \lor \neg \psi_{i',e_r} \lor T_{\sigma_{i'j}} \lor \neg \psi_{i',e_r})),$

Let $J'_{u,j} := j'_{r,j}$.

- We set $U_j := U^2_j \ast \sum_{u \in S^2_j} (U^2_{J'_{u,j}})^u$.

For each $j \in [m]$, let $B_j \subseteq br(U_j)$ be the set of branches extending some element of $S^2_j$. Under $\neg Count^3_n$, we see the equation

$$\sum_{\alpha \in B_j} x_\alpha = f_{ij} f_{i'j}$$
has a NS-proof over $\mathbb{F}_2$ with degree $O(1)$. Therefore, we obtain a NS-proof of

$$\sum_{j \in [m]} \sum_{\alpha \in B_j} x_\alpha = \sum_{j \in [m]} f_{ij} f'_{ij}$$

over $\mathbb{F}_2$ with degree $O(1)$. The LHS is 0 based on the following reasoning: Let $b = uv^u \in B_j$, where $u \in S^2_j$ and $v \in \text{br}(U^2_{j,u})$. Let $l := J'_{u,j}$. It is easy to see that $v \in S^2_l$, and $b \in B_l$. Decomposing $b = cd^c$, where $c \in S^2_l$ and $d \in S^2_{J'_{c,l}}$, we obtain $J'_{c,l} = j$. This argument gives a natural 2-partition of the disjoint union $\bigcup_{j \in [m]} B_j$, pairing branches giving the same partial injections.

Lastly, we prove that $\sum_{j=1}^m f_{ij} = 1$ ($i \in [m+1]$) has a NS-proof from $\neg \text{Count}_3^n$ with degree $O(1)$. For $j \in [m]$, let

$$V_j := T_{\sigma_{ij}} \ast \sum_{b \in \text{br}_1(T_{\sigma_{ij}})} (R_b)^b.$$

where $T_{i,j} := T_{\neg \sigma_{ij} \lor \tau_{ij} \lor \lor_{e \in [n](2)} \varphi_{ie}}$. Let $B_j$ be the set of branches $b \in \text{br}(V_j)$ extending some $b' \in \text{br}_1(T_{\sigma_{ij}})$. Since

$$T \models \neg \tau_{ij} \lor \lor_{e \in [n](2)} \varphi_{ie} \quad (j \in e \in [n](2)) \quad \text{and} \quad T \models \lor_{e' \perp e} \neg \varphi_{ie} \lor \lor_{e' \perp e} \varphi_{ie} \quad (e \perp e'),$$

each $b \in B_j$ satisfies exactly one of the following:

1. $b$ is an extension of some $b' \in \text{br}_1(T_{\tau_{ij}})$.

2. There exists a unique $e \in [m](2)$ ($j \in e$) such that $b$ is an extension of some $b' \in \text{br}_1(T_{\varphi_{ie}})$.

Define $R_b$ as follows:

1. If the condition [1] is satisfied,

   $$R_b := T_i \ast T_{\sigma_{ij} \lor \neg \tau_{ij}},$$

   where $T_i := T_{V_j \tau_{ij}}$.

2. If the condition [2] is satisfied, and $\{j, j'\} := e$, then

   $$R_b := T_{\sigma_{ij} \lor \lor_{\varphi_{ie}} \lor V_{j'} \lor T_{\sigma_{ij} \lor \lor_{\varphi_{ie}}}}.$$

Consider

$$W_j := V_j \ast \sum_{b \in B_j} (R_b)^b.$$

Let $C_j$ be the set of all branches $r \in \text{br}(W_j)$ of the form $r = bd^b$, where $b \in B_j$. The equation

$$\sum_{r \in C_j} x_r = f_{ij}$$

33
has a \( NS \)-proof over \( \mathbb{F}_2 \) from \( \neg \text{Count}_n^3 \) with degree \( O(1) \).

Now, we define \( Q_i \) as follows: since

\[
T \models \bigvee_j \tau_{ij} \quad \text{and} \quad T \models \neg \tau_{ij} \lor \neg \tau_{ij'},
\]

we see each branch \( b \in \text{br}(T_i) \) has the unique \( j_b \) such that \( b \) is an extension of \( b' \in \text{br}_1(T_{\tau_{ij_b}}) \). We set

\[
Q_i := T_i \ast \sum_{b \in \text{br}(T_i)} (T_{\sigma_{ij_b} \lor \neg \tau_{ij_b}} \ast (T_{\sigma_{ij_b} \lor T_{1,j_b}}))^b.
\]

We already know that there exists a \( NS \)-proof of \( \sum_{\beta \in \text{br}(Q_i)} x_{\beta} = 1 \) from \( \neg \text{Count}_n^3 \) with degree \( O(1) \). Observing

\[
\sum_j \sum_{r \in C_j} x_r + \sum_{\beta \in \text{br}(Q_i)} x_{\beta} = 0,
\]

we obtain a \( NS \)-proof of \( \sum_{j=1}^m f_{ij} = 1 \) from \( \neg \text{Count}_n^3 \) with degree \( O(1) \).

The observation follows from a 2-partition of \( (\bigsqcup_j C_j) \sqcup \text{br}(Q_i) \) similar to the one appearing in the proof of item 3. To be concrete, consider the following labeling of \( r = bd^i \in C_j \) (where \( b \in B_j \)):

- If \( b \) satisfies the condition 1 in the definition of \( W_j \), label it by \( \{j\} \).
- If \( b \) satisfies the condition 2 in the definition of \( W_j \), and \( \{j, j'\} := e \), label \( b \) by \( e \).

To make \( W_j \) fully labeled, we label each \( b \in \text{br}(W_j) \setminus C_j \) by a symbol \( \perp \). Then we obtain:

- For each \( j \neq j', \text{br}_{\{j,j'\}}(W_j) = \text{br}_{\{j,j'\}}(W_{j'}). \)
- \( \bigsqcup_{j \in [m]} \text{br}_{\{j\}}(W_j) = \text{br}(Q_i) \).

These give the equation \( \Box \).

5 On the strength of Fisher’s inequality

When we discuss whether the condition given in Theorem 67 actually holds or not, it is natural also to consider the \( K \)-analogue of the condition, where \( K \) is an arbitrary field other than \( \mathbb{F}_2 \). The following combinatorial principle (see Remark 73 for the informal meaning) relates to a condition similar to the analog.
Definition 72. We define the $\Sigma_0^B \mathcal{L}_A^2$ formula $FIE(n, S, R)$ as follows:

$$FIE(n, S, R) :=$$

$$\neg \left( \forall i \in [n + 1] \exists j \in [n] S(i, j) \right)$$

$$\land \forall i_1 < i_2 \in [n + 1] \exists j \in [n] ((S(i_1, j) \land \neg S(i_2, j)) \lor (\neg S(i_1, j) \land S(i_2, j)))$$

$$\land \forall i_1 < i_2 \in [n + 1] \forall i_1' < i_2' \in [n + 1] \forall j \in [n]$$

$$\left( (\neg S(i_1, j) \lor \neg S(i_2, j) \lor \exists j' \in [n] R(i_1, i_2, i_1', i_2', j, j')) \land \forall i_1 < i_2 \in [n + 1] \forall i_1' < i_2' \in [n + 1] \forall j' \in [n]$$

$$\left( (\neg S(i_1', j) \lor \neg S(i_2', j) \lor \exists j' \in [n] R(i_1, i_2, i_1', i_2', j, j')) \right)$$

$$\land \forall i_1 < i_2 \in [n + 1] \forall i_1' < i_2' \in [n + 1] \forall j \in [n]$$

$$\left( \forall j' \in [n] (\neg R(i_1, i_2, i_1', i_2', j, j')) \right)$$

$$\land \forall i_1 < i_2 \in [n + 1] \forall i_1' < i_2' \in [n + 1] \forall j \in [n]$$

$$\left( \forall j' \in [n] (\neg R(i_1, i_2, i_1', i_2', j, j')) \right)$$

$$\left( \forall j \in [n] (\neg R(i_1, i_2, i_1', i_2', j, j')) \right)$$
Furthermore, we define the propositional formula $FIE_n$ as follows:

$$FIE_n := \neg \left( \bigwedge_{i \in [n+1]} \bigvee_{j \in [n]} s_{ij} \right)$$

$$\wedge \bigwedge_{i < j \in [n+1]} \bigvee_{j' \in [n]} \left( \left( s_{ij} \wedge \neg s_{ij'} \right) \lor \left( \neg s_{ij} \wedge s_{ij'} \right) \right)$$

$$\wedge \bigwedge_{i < j \in [n+1]} \bigvee_{j' \in [n]} \left( \neg s_{ij} \lor \neg s_{ij'} \lor \bigvee_{j'' < j'} s_{ij''} \right)$$

$\text{Remark 73.}$ 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 $i$, $\emptyset \neq S_i \subseteq [n]$.
- 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 our definition of $FIE(n, S, R)$, $S$ intuitively gives a family $\{S_i\}_{i \in [n+1]}$, and $R$ gives a family of bijections

$$\{R^{i_1, i_2, i_1', i_2'}: S_{i_1} \cap S_{i_2} \rightarrow S_{i_1'} \cap S_{i_2'}\}_{i_1 < i_2 \& i_1' < i_2'}$$

$\text{Remark 74.}$ In [9], Fisher gave a special case of the statement, and later, it was generalized to the above form by [15] and others. See introductions of [15] and [21] for historical remarks. Note that there are several versions of the statement of Fisher’s inequality. Primarily, it is often presented in a dual form, switching the roles of sets and elements. The form we adopted is following the
presentation of [6]. To verify the above version, see the proof of Theorem 4 in [6].

Although Fisher’s inequality was proposed as a candidate for potentially hard tautology for the Frege system, it is provable in $\text{VTC}^0$. I was unaware of this fact when this paper was submitted, and I would like to thank the anonymous referee for sharing the work of [21]. Around the very time [6] was published, Woodall gave an elementary proof of Fisher’s inequality in [21], which was already sufficient to construct short Frege proofs of Fisher’s inequality. The proof can be interpreted as a proof in $\text{VTC}^0$ augmented with iterated multiplication of integers (or, equivalently, rationals). Recently, Jeřábek showed that $\text{VTC}^0$ can formalize iterated multiplication of integers and prove its basic properties ([11]). Since we have nothing to add to their results, we just present the claim for reference:

Theorem 75 (Essentially by [21] and [11]).

$$\text{VTC}^0 \vdash \text{FIE}(n,S,R).$$

Note that [21] takes the dual approach mentioned in Remark 74 and also we do not need the “nontriviality”-condition assumed in the article.

Now, we focus on the lower bounds of the strength of $\text{FIE}_n$. It is easy to see that $\text{FIE}_n$ is a generalization of the pigeonhole principle.

Proposition 76. $\text{V}^0 + \text{FIE}_k \vdash \text{injPHP}^{n+1}_{n+1}$. Hence, for each $p \geq 2$,

$$\text{V}^0 + \text{Count}^p_n \not\vdash \text{FIE}_n.$$  

Proof. Argue in $\text{V}^0$. Suppose $f$ is an injection from $[n+1]$ to $[n]$. We set $S_i := \{f(i)\}$ ($i \in [n+1]$). Then, the $S_i$’s are distinct and $S_i \cap S_j = \emptyset$ for every $i < j$. Hence, $\text{FIE}_n$ is violated.

The latter part follows immediately from Theorem 8. ■

It is natural to ask the following:

Question 4. Which $p$ satisfies $\text{V}^0 + \text{FIE}_k \vdash \text{Count}^p_n$?

We conjecture that there is no such $p$. The following theorem gives a criterion for proving this conjecture.

Theorem 77. Let $\mathbb{K}$ be a field. Suppose $F_d + \text{FIE}_k \vdash_{\text{poly}(n)} \text{Count}^p_n$. Then, for large enough $n \not\equiv 0 \pmod{p}$, there exist $m = n^{O(1)}$ and families $(f_{ij})_{i \in [m+1], j \in [m]}$, $(a_{ij})_{i \in [m+1], j \in [m]}$ and $(b_{ij})_{i < j \in [m+1], j \in [m]}$ of polynomials over $\mathbb{K}$ such that the following equalities have NS-proofs over $\mathbb{K}$ from $\neg\text{Count}^p_n$ with degree $O(1)$:
\[
\sum_{j=1}^{m} f_{i_1 j} f_{i_2 j} = \sum_{j=1}^{m} f_{i_1' j} f_{i_2' j} \quad (i_1 < i_2 \in [m+1] & i_1' < i_2' \in [m+1]),
\]

\[
a_{ij} (1 - f_{ij}) = 0 \quad (i \in [m+1]),
\]

\[
\sum_{j=1}^{m} a_{ij} = 1 \quad (i \in [m+1]),
\]

\[
b_{ii' j} (1 - f_{ij}) (1 - f_{i' j}) = 0 \quad (i < i' \in [m+1], & j \in [m]).
\]

\[
\sum_{j=1}^{m} b_{ii' j} = 1 \quad (i < i' \in [m+1]).
\]

**Proof.** For readability, we assume \( p = 3 \). Assume proofs \((\pi_n)_{n \in \mathbb{N}}\) witness

\[
F_d + FIE_k \vdash \text{poly}(n) \text{ Count}_n^3.
\]

We focus on \( n \not\equiv 0 \pmod{3} \). Let \( \Gamma_n \) be the set of subformulæ of \( \pi_n \). As the proof of Theorem 67 using the switching lemma for 3-tree and a padding argument, we may assume that there exists an \( O(1) \)-evaluation \( T_n \) of \( \Gamma_n \), and it suffices to construct \((f_{ij}), (a_{ij})\) and \((b_{ii' j})\) for \( n \). We fix a large enough \( n \not\equiv 0 \pmod{3} \), and suppress scripts \( n \) of \( T_n \), \( \rho_n \), etc.

Since \( T \not\models \text{ Count}_n^3 \), soundness gives that some instance

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

in \( \pi_n \) 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 \( T_i := TV_{j \in [m]} \sigma_{ij} \). Since

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

each \( b \in br(T_i) \) has at least one \( j_b \in [m] \) and \( b' \in br_1(T_{\sigma_{ij}}) \) such that \( b' \subseteq b \). We relabel each branch \( b \in br(T_i) \) with \( \langle j_b \rangle \) and obtain a labeled \( injPHP \)-tree \( T_i \).

2. Let \( T_{i_1,i_2} := TV_{j \in [m]} ((\sigma_{i_1 j} \wedge \neg \sigma_{i_2 j}) \vee (\neg \sigma_{i_1 j} \wedge \sigma_{i_2 j})) \). 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 $b' \in \text{br}_0(T_{\sigma_1 \cap b}) \cup \text{br}_1(T_{\sigma_2 \cap b})$, $b \perp b'$
(b) For all $b' \in \text{br}_1(T_{\sigma_1 \cap b}) \cup \text{br}_0(T_{\sigma_2 \cap b})$, $b \perp b'$
We relabel each branch $b \in \text{br}(T_{i_1},i_2)$ with $\langle j b \rangle$ and obtain a labeled $injPHP$-tree $T_{i_1},i_2$.

3. Let $T_{i_1,i_2} := T_{\sigma_1 \cap \neg \sigma_2 \cap \bigvee_{j \in [m]} \forall j,i,j'}$. Each $b \in \text{br}(T_{i_1,i_2})$ is an extension of some element of $\text{br}_0(T_{\sigma_1 \cap \neg \sigma_2 \cap \bigvee_{j \in [m]} \forall j,i,j'})$. If $b$ is an extension of an element of $\text{br}_1(T_{i_1,i_2})$, $b \perp b'$ is unique.

4. Let $T_{i_1,i_2} := T_{\sigma_1 \cap \neg \sigma_2 \cap \bigvee_{j \in [m]} \forall j,i,j'}$. Each $b \in \text{br}(T_{i_1,i_2})$ is an extension of an element of $\text{br}_0(T_{\sigma_1 \cap \neg \sigma_2 \cap \bigvee_{j \in [m]} \forall j,i,j'})$. If $b$ is an extension of an element of $\text{br}_1(T_{i_1,i_2})$, $b \perp b'$ is unique.

Now, we set

$$f_{ij} := \sum_{\alpha \in \text{br}_i(T_{\sigma_j})} x_\alpha,$$

$$a_{ij} := \sum_{\alpha \in \text{br}_j(T_i)} x_\alpha$$

$$b_{i_1,i_2} := \sum_{\alpha \in \text{br}_j(T_{i_1,i_2})} x_\alpha.$$

$(i \in [m+1], j \in [m])$

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

We show that each of the following has a $NS$-proof from $\neg\text{Count}_n^3$ over $\mathbb{K}$ with $O(1)$-degree

$$\sum_{j=1}^{m} a_{ij} = 1,$$  \hspace{1cm} (7)

$$\sum_{j=1}^{m} b_{i_1,i_2,j} = 1,$$  \hspace{1cm} (8)

$$\sum_{j=1}^{m} f_{ij} f_{i_2,j} = \sum_{j=1}^{m} f_{i_1,i_2,j} f_{i_2,j'},$$  \hspace{1cm} (9)

$$a_{ij}(1 - f_{ij}) = 0,$$  \hspace{1cm} (10)

$$b_{i_1,i_2,j} f_{ij} f_{i_2,j} = 0,$$  \hspace{1cm} (11)

$$b_{i_1,i_2,j}(1 - f_{ij})(1 - f_{i_2,j}) = 0.$$  \hspace{1cm} (12)

$(i,i_1,i_2,i_1',i_2' \in [m+1] \& i_1 < i_2 \& i_1' < i_2' \& j \in [m])$
We first define $A_{i_1,i_2,j} := T_{\sigma_1} * T_{\sigma_2}$, $(i_1, i_2 \in [m+1], j \in [m], i_1 < i_2)$. Let $B_{i_1,i_2,j}$ be the set of all branches $b \in A_{i_1,i_2,j}$ having the form

$$b = cd^e \quad (c \in br_1(T_{\sigma_1}), d \in br_1(T_{\sigma_2})).$$

It is easy to construct a $NS$-proof of

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

from $\neg Count^2_k$ over $\mathbb{K}$ with degree $O(1)$. 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

$$R_j := A_{i_1,i_2,j} * \sum_{b \in B_{i_1,i_2,j}} (T_{i_1,i_2,i'_1,i'_2}^b) T_1^{i_1,i_2,i'_1,i'_2}$$

$$R'_j := A_{i'_1,i'_2,j} * \sum_{b \in B_{i'_1,i'_2,j}} (T_{i'_1,i'_2,i_1,i_2}^b) T_2^{i'_1,i'_2,i_1,i_2}.$$

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

Now, we define

$$T_{j,j'} := ((T_{r,j,j',i'_1,i'_2} * T_{r,j,j',i'_1,i'_2} * T_{r,j,j',i'_1,i'_2} * T_{r,j,j',i'_1,i'_2}) * T_{r,j,j',i'_1,i'_2} * T_{r,j,j',i'_1,i'_2} * T_{r,j,j',i'_1,i'_2}).$$

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

$$S_j := R_j * \sum_{r \in B_j} (T_{j,j'} * \sum_{t \in br(T_{j,j'})} (R_t^{j'})^r),$$

$$S'_j := R'_j * \sum_{r' \in B'_j} (T_{j,j'} * \sum_{t \in br(T_{j,j'})} (R_t^{j'})^r).$$

Label each branch $b \in br(S_j)$ as follows:
• If $b$ extends some $r \in B_j$, then label $b$ with $\langle j, j' \rangle$.
• Otherwise, label $b$ with the symbol $\bot$.

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

• If $b$ extends some $r' \in B'_{j'}$, then label $b$ with $\langle \hat{j}, j' \rangle$.
• Otherwise, label $b$ with the symbol $\bot$.

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 $\neg Count^3_n$ over $K$ with $O(1)$-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 (13), they give a NS-proof of $\sum_j f_{i_1,j} f_{i_2,j} = \sum_{j'} f'_{i_1',j'} f'_{i_2',j'}$ satisfying the required conditions.

(10): It follows similarly as (12) below.

(11): $b_{i_1,i_2} f_{i_1,j} f_{i_2,j} = 0$ follows easily from $\neg Count^3_n$ since each $\alpha \in br_{\langle j \rangle}(\tilde{T}_{i_1, i_2})$ satisfies $\alpha \perp b$ for all $b \in B_{i_1, i_2, j}$.

(12): Note that we have NS-proofs of the following:
\[ f_{i_1,j} + \sum_{\beta \in br_0(T_{x_{i_1,j}})} x_\beta = 1, \]
\[ f_{i_2,j} + \sum_{\beta \in br_0(T_{x_{i_2,j}})} x_\beta = 1. \]

$(j \in [m])$

Hence, $b_{i_1,i_2}(1 - f_{i_1,j})(1 - f_{i_2,j}) = 0$ follows easily from $\neg Count^3_n$ by a similar reason as the previous item.

\[ \blacksquare \]
Acknowledgements

The author deeply appreciates the anonymous referee’s pointing out several mistakes in the initial version of this paper, numerous constructive comments and suggestions, and drawing my attention to [21]. The author is also grateful to Toshiyasu Arai for the helpful discussions and his patient support and to Satoru Kuroda for guiding me through the series of work on proof complexity of linear algebra. In addition, the author thanks to Jan Krajíček, Mykyta Narusevych, Ondřej Ježil, Emil Jeřábek, Pavel Pudlák, Erfan Khaniki, and Moritz Müller for their valuable comments on the technical barrier of resolving ontoPHP v.s. injPHP over V0, which are closely related to Remark 68 and pointing out several typos in the initial version of this paper. This research was done during 2020-2022 and supported by:

- FoPM, WINGS Program, the University of Tokyo, and
- the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

The author got the above feedback in 2023.

References

[1] Atserias, A., & Müller, M. (2015). Partially definable forcing and bounded arithmetic. Arch. Math. Logic, 54, no. 1-2, 1-33. https://doi.org/10.1007/s00153-014-0398-3

[2] Ajtai, M. The complexity of the Pigeonhole Principle. Combinatorica, vol. 14 (1994), 417-433. https://doi.org/10.1007/BF01302964

[3] 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. https://doi.org/10.1109/SFCS.1994.365714

[4] 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. https://doi.org/10.1090/dimacs/039/02

[5] Berkowitz, S. J. (1984). On computing the determinant in small parallel time using a small number of processors, Information Processing Letters, 18(3), 147-150. https://doi.org/10.1016/0020-0190(84)90018-8

[6] 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. https://doi.org/10.1007/978-1-4612-2566-9_3
[7] Buss, S. (1998). Lower bounds on Nullstellensatz proofs via designs, 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, 59-71. https://doi.org/10.1090/dimacs/039/04

[8] Cook, S., & Nguyen, P. *Logical foundations of proof complexity*, Perspectives in Logic. Cambridge University Press, New York, NY (2010). https://doi.org/10.1017/CBO9780511676277

[9] Fisher, R. A. (1940). An examination of the different possible solutions of a problem in incomplete blocks. *Ann. Eugenics, 10*, 52-75.

[10] Hrubeš, P. & Tzameret, I. (2015). Short proofs for the determinant identities. *SIAM J. Comput.*, 44(2), 340-383. https://doi.org/10.1137/130917788

[11] Jeřábek, E. (2022). Iterated multiplication in $\text{VTC}^0$. *Arch. Math. Logic*, 61(5-6), 705-767. https://doi.org/10.1007/s00153-021-00810-6

[12] Krajíček, J. *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, 60. Cambridge University Press, Cambridge (1995). https://doi.org/10.1017/CBO9780511529948

[13] Krajíček, J. *Proof complexity*, Encyclopedia of Mathematics and Its Applications, 170. Cambridge University Press, Cambridge (2019). https://doi.org/10.1017/9781108242066

[14] 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. https://doi.org/10.1002/rsa.3240070103

[15] Majumdar, K. N. (1953). On some theorems in combinatorics relating to incomplete block designs. *Ann. Math. Statistics*, 24, 377-389. https://doi.org/10.1214/aoms/1177728978

[16] Pitassi, T., Beame, P., & Impagliazzo, R. Exponential lower bounds for the pigeonhole principle, *Computational Complexity*, vol. 3, no.2 (1993), 97-140. https://doi.org/10.1007/BF01200117

[17] Razborov, A, A. Lower bounds for the polynomial calculus, *Computational Complexity*, vol. 7, no. 4 (1998), 291-324. https://doi.org/10.1007/s000370050013

[18] Soltys, M. (2001). The complexity of derivations of matrix identities, *Thesis (Ph.D.)-University of Toronto (Canada).*

[19] Soltys, M., & Cook, S. (2004). The proof complexity of linear algebra, *Ann. Pure Appl. Logic, 130*(1-3), 277 - 323. https://doi.org/10.1016/j.apal.2003.10.018
[20] Tzameret, I., & Cook, S. (2021). Uniform, integral, and feasible proofs for the determinant identities. *J. ACM*, 68(2), 80. https://doi.org/10.1145/3431922

[21] Woodall, D. R. (1997). A note on Fisher’s inequality. *J. Combin. Theory Ser. A*, 77(1), 171-176. https://doi.org/10.1006/jcta.1996.2729