Cohomological k-consistency

Adam Ó Conghaile

Abstract

k-consistency is a well-known efficient algorithm for CSP, based on propagating compatible local solutions. The limitations of this and the related k-Weisfeiler-Leman algorithm for structure isomorphism are well-known. k-consistency can solve precisely those CSPs of bounded width and k-Weisfeiler-Leman can only distinguish structures which differ in properties definable in C^k. Cohomology formalises obstructions to combining local solutions into global ones. Recent work by Abramsky and others has shown that such obstructions can be used to identify quantum systems which are locally consistent but globally inconsistent. In this paper, we use these insights to expand the k-consistency and k-Weisfeiler-Leman algorithms. We show that the resulting cohomological algorithms are efficient and far more powerful than their classical counterparts. In particular, we show that cohomological k-consistency can solve systems of equations over all finite rings and that cohomological Weisfeiler-Leman can distinguish positive and negative instances of the Cai-Furer-Immerman property over several important classes of structures. This has immediate consequences for descriptive complexity, showing that solvability of linear equations over the integers cannot be expressed in rank logic.

CCS Concepts: • **Theory of computation → Finite Model Theory**.

Keywords: constraint satisfaction problems, finite model theory, descriptive complexity, rank logic, Weisfeiler-Leman algorithm, cohomology

ACM Reference Format:
Adam Ó Conghaile. 2022. Cohomological k-consistency. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Constraint satisfaction problems (CSP) and structure isomorphism (SI) are two of the most well-studied problems in complexity theory. Mathematically speaking, an instance of one of these problems takes a pair of structures (A, B) as input and asks whether there is a homomorphism $A \to B$ for CSP or an isomorphism $A \cong B$ for SI. These problems are not in general thought to be tractable. Indeed the general case of CSP is `NP-Complete` and restricting our structures to graphs the best known algorithm for SI is Babai's quasi-polynomial time algorithm.[6] As a result, it is common in complexity and finite model theory to study approximations of the relations $\to$ and $\cong$.

The k-consistency and k-Weisfeiler-Leman[1] algorithms efficiently determine two such approximations to $\to$ and $\cong$ which we call $\to_k$ and $\equiv_k$. These relations have many characterisations in logic and finite model theory, for example in [13] and [9]. One that is particularly useful is that of the existence of winning strategies for Duplicator in certain Spoiler-Duplicator games with k pebbles[20] [18]. For both of these games Duplicator's winning strategies can be represented as non-empty sets $S \subset \mathbf{Hom}_k(A, B)$ of k-local partial homomorphisms which satisfy some extension properties and connections between these games have been studied before. For example, a joint comonadic semantics is given by the pebbling comonad of Abramsky, Dawar and Wang[3].

The limitations of these approximations are well-known. In particular, it is known that k-consistency only solves CSPs of *bounded width* and k-Weisfeiler-Leman can only distinguish structures which differ on properties expressible in the infinitary counting logic C^k. Feder and Vardi[13] showed that CSP encoding linear equations over the finite fields do not have bounded width, while Cai, Furer, and Immerman[9] demonstrated an efficiently decidable graph property which is not expressible in C^k for any k.

In the present paper, we introduce new efficient extensions to the k-consistency and k-Weisfeiler-Leman algorithms computing relations $\to_k^{\mathbb{Z}}$ and $\equiv_k^{\mathbb{Z}}$ which refine $\to_k$ and $\equiv_k$. These new algorithms exploit the fact that the sets S of k-local partial homomorphisms which witness $\to_k$ and $\equiv_k$ can be seen as presheaves and aspects of the associated sheaf cohomology are both efficiently computable and help us to distinguish sets which cannot be used to construct a witness of $\to$ or $\cong$. For the benefit of the broad computer science audience of this paper, we avoid explicitly defining the sheaves and cohomology involved and instead refer to an analgous application of sheaf theory to quantum contextuality, pioneered by Abramsky and Brandenburger[2] and developed by Abramsky and others for example in [4] and

[1] The algorithm we call "k-Weisfeiler-Leman" is more commonly called "$(k-1)$-Weisfeiler-Leman" in the literature, see for example [9]. We prefer "k-Weisfeiler-Leman" to emphasise its relationship to k-variable logic and sets of k-local isomorphisms.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

Conference'17, July 2017, Washington, DC, USA
© 2022 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

[1]. As a result, our definitions are self-contained and don't require knowledge of algebraic topology.

Using the work of Abramsky et al.[1], we show these new cohomological algorithms are strictly stronger than k-consistency and k-Weisfeiler-Leman. In particular, we show that cohomological k-consistency decides solvability of linear equations with k variables per equation over all finite rings and that there is a fixed k such that $\equiv_k^{\mathbb{Z}}$ distinguishes structures which differ on Cai, Furer and Immerman's property.

It is also interesting to compare $\to_k^{\mathbb{Z}}$ and $\equiv_k^{\mathbb{Z}}$ with other well-studied refinements of $\to_k$ and $\equiv_k$ such as the algorithms of Bulatov[8] and Zhuk[23] which decide all tractable CSPs and the invertible-map equivalence of Dawar and Holm[12] which bounds the expressive power of rank logic. The latter was recently used by Lichter[21] to demonstrate a property which is decidable in PTIME but not expressible in rank logic. In our paper, we show that $\equiv_k^{\mathbb{Z}}$, for some fixed k , can distinguish structures which differ on this property. Comparing $\to_k^{\mathbb{Z}}$ to the Bulatov-Zhuk algorithm remains a direction for future work.

The rest of the paper proceeds as follows. Section 2 establishes some background and notation. Section 3 defines the cohomological k-consistency algorithm and shows that $\to_k^{\mathbb{Z}}$ is transitive. Section 4 proves that $\to_k^{\mathbb{Z}}$ can solve systems of linear equations over any field by connecting the algorithm of the previous section to a theorem of Abramsky, Barbosa, Kishida, Lal and Mansfield[1]. Section 5 defines the cohomological Weisfeiler-Leman algorithm and shows that $\equiv_k^{\mathbb{Z}}$ distinguishes structures which differ on the CFI property. Section 6 concludes with some open questions and directions for future work.

2 Background and definitions

In this section, we record some definitions and background which are necessary for our work.

2.1 Relational structures & finite model theory

Throughout this paper we use the word *structure* to mean a relational structure over some finite relational signature σ. A stucture A consists of an underlying set (which will also call A) and for each relational symbol R of arity r in σ a subset $R^A \subset A^r$ or tuples related by R. A *homomorphism* of structures A, B over a common signature is a function between the underlying sets $f : A \to B$ which preserves related tuples. An *isomorphism* of structures is a bijection between the underlying sets which both preserves and reflects related tuples.

In the paper, we make reference to several important logics from finite model theory and descriptive complexity theory. As the syntax of these logics is not important to our work we simply treat a *logic* L as a collection of formulas $\phi(\mathbf{x}) \in L[\sigma]$ for each finite relational signature σ with some semantics $\models$ defined on structures with signature σ. We write $A, \mathbf{a} \models \phi(\mathbf{x})$ when $\phi(\mathbf{a})$ is true in A. We say that L defines a class of σ-structures C if there is a $\phi_C \in L[\sigma]$ such that

$$A \in C \iff A \models \phi_C$$

The logics we make reference to in this paper are as follows.

- Fixed-point logic with counting (written FPC) is first-order logic extended with operators for inflationary fixed-points and and counting, for example see [14].
- For any natural number k, C^k is infinitary first-order logic extended with counting quantifiers with at most k variables. This logic bounds the expressive power of FPC in the sense that, for each k' there exists k such that any FPC formula in k' variables is equivalent to one in C^k. We write C^ω for the union of these logics.
- Rank logic is first-order logic extended with operators for inflationary fixed-points and computing ranks of matrices over finite fields, see [22].
- Linear algebraic logic is first-order infinitary logic extended with quantifiers for computing *all* linear algebraic functions over finite fields, see [10]. This logic bounds rank logic in the sense described above.

At different points in the history of descriptive complexity theory, both FPC and rank logic were considered as candidates for "capturing PTIME" and thus refuting a well-known conjecture of Gurevich[16]. Each has since been proven not to capture PTIME, for FPC see Cai, Furer and Immerman[9], for rank logic see Lichter[21]. Infinitary logics such as C^ω and linear algebraic logic are capable of expressing properties which are not decidable in PTIME but have been shown not to contain any logic which does not capture PTIME. For C^ω, see Cai, Furer and Immerman [9] and for linear algebraic logic, see Dawar, Grädel, and Lichter[11].

2.2 Constraint satisfaction problems

Throughout we will consider the problem $\mathbf{CSP}(A, B)$ for A and B structures over some fixed finite signature σ, as the problem of deciding whether or not there is a homomorphism $f : A \to B$. We use $\mathbf{CSP}(B)$ to denote the problem of deciding $\mathbf{CSP}(A, B)$, given an instance A. For general B, this problem is well-known to be NP-complete. However for certain structures B the problem is in PTIME. Indeed, the Bulatov-Zhuk Dichotomy Theorem (formerly the Feder-Vardi Dichotomy Conjecture) states that for any B $\mathbf{CSP}(B)$ is either NP-complete or it is PTIME. Working out efficient algorithms which decide $\mathbf{CSP}(B)$ for larger and larger classes of B was an active area of research which culminated in Bulatov and Zhuk's exhaustive classes of algorithms [8], [23].

3 Defining the algorithm

In this section, we define the cohomological k-consistency algorithm and the relation $\to_k^{\mathbb{Z}}$ that it computes between structures. We also show that the algorithm runs in polynomial time in the product of the sizes of the input structures and that the relation is compositional.

3.1 Classical k-consistency algorithm

We start by recalling some definitions related to the classical k-consistency algorithm on which our algorithm will build.

For A and B finite structures over a common (finite) signature, let $\mathbf{Hom}_k(A, B)$ denote the set of partial homomorphisms from A to B with domain of size less than or equal to k. There is a natural partial order $<$ on this set, defined as follows. For any partial homomorphisms $f, g \in \mathbf{Hom}_k(A, B)$ we say that $f < g$ if $\mathbf{dom}(f) \subset \mathbf{dom}(g)$ and $g_{|_{\mathbf{dom}(f)}} = f$.

We say that any $S \subset \mathbf{Hom}_k(A, B)$ has the *forth* property if for every $f \in S$ with $|\mathbf{dom}(f)| < k$ we have the property $\mathbf{Forth}(S, f)$ which is defined as follows:

$$\forall a \in A,\ \exists b \in B \text{ s.t. } f \cup \{(a, b)\} \in S.$$

Given $S \subset \mathbf{Hom}_k(A, B)$ we define $\overline{S}$ to be the largest subset of S which is downwards-closed and has the forth property. Note that $\emptyset$ satisfies these conditions, so such a set always exists. For a fixed k there is a simple algorithm for computing $\overline{S}$ from S.

This is done by starting with $S_0 = S$ and then entering the following loop with $i = 0$

1. Initialise S_{i+1} as being equal to S_i.
2. For each $s \in S_i$, check if $\mathbf{Forth}(S_i, s)$ holds and if not remove it from S_{i+1} along with all $s' > s$.
3. If none fail this test, halt and output S_i.
4. Otherwise, increment i by one and repeat.

It is easily seen that this runs in polynomial time in $|A||B|$.

Now for a pair of structures A, B we say that the pair (A, B) is k consistent if $\overline{\mathbf{Hom}_k(A, B)} \neq \emptyset$. We denote this by writing $A \to_k B$ and the algorithm above shows how to decide this relation in polynomial time for fixed k. This relation has many equivalent logical and algorithmic definitions as seen in [13], and [7].

3.2 Local, global & $\mathbb{Z}$-linear sections

Let S be some set $\emptyset \neq S \subset \mathbf{Hom}_k(A, B)$. Let $A^{\leq k}$ be the set of all subsets of A with at most k elements and for each $\mathbf{a} \in A^{\leq k}$ we consider the *set of local sections of S at* $\mathbf{a}$

$$S_{\mathbf{a}} = \{f \in S \mid \mathbf{dom}(f) = \mathbf{a}\}$$

Given such a section $s \in S_{\mathbf{a}}$, it is natural to ask whether it can be extended to a homomorphism $f : A \to B$ such that $f_{|_{\mathbf{a}}} = s$. If we ask that f should locally look like a section of S at every $\mathbf{a}' \in A^{\leq k}$ then the existence of such an f is equivalent to the existence of a set $\{s_{\mathbf{a}'} \in S_{\mathbf{a}'}\}_{\mathbf{a}' \in A^{\leq k}}$ such that $s_{\mathbf{a}} = s$ and for all $\mathbf{a}_1, \mathbf{a}_2 \in A^{\leq k}$ the corresponding local sections agree on the intersection $\mathbf{a}_1 \cap \mathbf{a}_2$, i.e.

$$s_{\mathbf{a}_1}|_{\mathbf{a}_1 \cap \mathbf{a}_2} = s_{\mathbf{a}_2}|_{\mathbf{a}_1 \cap \mathbf{a}_2}.$$

We call such a set a *global section of S extending s* and if one exists we say that s is *extendable in S*. Deciding whether there is such a global section for general S is equivalent to deciding **CSP** and is, thus, `NP-Complete`. In our algorithm we will ask for the following weaker but efficiently computable relaxation of this condition.

Let $\mathbb{Z}S_{\mathbf{a}}$ be the formal $\mathbb{Z}$-linear combinations of elements of $S_{\mathbf{a}}$. We call these *local $\mathbb{Z}$-linear sections at* $\mathbf{a}$. For any $\mathbf{a}' \subset \mathbf{a}$ and any local $\mathbb{Z}$-linear section $r = \sum_{s \in S_{\mathbf{a}}} z_s s \in \mathbb{Z}S_{\mathbf{a}}$, we write $r_{|_{\mathbf{a}'}}$ for the restriction of this section to $\mathbf{a}'$ given by $\sum_{s \in S_{\mathbf{a}}} z_s s_{|_{\mathbf{a}'}} \in \mathbb{Z}S_{\mathbf{a}'}$. We say that $s \in S_{\mathbf{a}}$ is *$\mathbb{Z}$-extendable in S* if there is a global $\mathbb{Z}$-linear section $\{r_{\mathbf{a}'} \in \mathbb{Z}S_{\mathbf{a}'}\}_{\mathbf{a}' \in A^{\leq k}}$ extending s. By analogy to the case in the previous paragraph we require that $r_{\mathbf{a}} = s$ and for all $\mathbf{a}_1, \mathbf{a}_2 \in A^{\leq k}$ we have

$$r_{\mathbf{a}_1}|_{\mathbf{a}_1 \cap \mathbf{a}_2} = r_{\mathbf{a}_2}|_{\mathbf{a}_1 \cap \mathbf{a}_2}.$$

We note that a local section s being $\mathbb{Z}$-extendable in a set S implies that s has the forth property and that all $s' < s$ are contained in S

Lemma 1. *For any structures A, B, positive integer k, set $S \subset \mathbf{Hom}_k(A, B)$, and local section $s \in S$, if s is $\mathbb{Z}$-extendable in S then for all local sections $s' < s$ $s' \in S$ and, if $|\mathbf{dom}(s)| < k$ then $\mathbf{Forth}(S, s)$ holds.*

Proof. Let $\{r_{\mathbf{a}} = \sum \alpha_f f\}$ be the global $\mathbb{Z}$-linear section extending s. Now suppose that $s' < s$, i.e. that there is a $\mathbf{b} \subset \mathbf{dom(s)}$ such that $s' = s_{|_{\mathbf{b}}}$. However we know that $r_{\mathbf{b}} = (r_{\mathbf{dom}(s)})_{|_{\mathbf{b}}}$ and as r extends s we have that $r_{\mathbf{dom}(s)} = s$ and so $r_{\mathbf{b}} = s_{|_{\mathbf{b}}} = s'$. So s' must appear in r and thus appears in S.
To show that $\mathbf{Forth}(S, s)$ holds, we consider any $a \in A$ and we look for a $b \in B$ such that $s \cup \{(a, b)\} \in S$. For any such a, as r is a global $\mathbb{Z}$-linear section, we have that

$$(r_{\mathbf{dom}(s) \cup \{a\}})_{|_{\mathbf{dom}(s)}} = r_{\mathbf{dom}(s)} = s$$

However, the coefficients of s in the left hand side, is simply the sum of the coefficients of those $s' \in S$ with domain $\mathbf{dom}(s) \cup \{a\}$ such that $s'_{|_{\mathbf{dom}(s)}} = s$. $\mathbf{Forth}(S, s)$ holds precisely when such an s' exists for each $a \in A$. As the coefficient of s on the right hand side of the equation above is always non-zero there must be at least one such s' for each a. □

Finally, the conditions defining the $\mathbb{Z}$-extendability of s in some S are simply systems of $\mathbb{Z}$-linear equations in the variables z_s. Indeed each equality over $\mathbb{Z}S_{\mathbf{a}'}$ in the definition of $\mathbb{Z}$-extendability yields at most $|B|^k$ $\mathbb{Z}$-linear equations, one for the coefficient of each element $s' \in S_{\mathbf{a}'}$. This means that for any $s \in S$, deciding whether s is $\mathbb{Z}$-extendable in S is equivalent to deciding if a system of at most $|A|^{2k} \cdot |B|^k$ $\mathbb{Z}$-linear equations, one equation in $\mathbb{Z}S_{\mathbf{a} \cap \mathbf{a}'}$ for each pair $\mathbf{a}, \mathbf{a}' \in A^{\leq k}$, in at most $|A|^k \cdot |B|^k$ variablesis solvable over $\mathbb{Z}$. As such systems of linear equations over $\mathbb{Z}$ can be sovled in polynomial time in the number of equations and variables via computing Smith Normal Forms of integer matrices as done by Kannan and Bachem [19]), we can, for fixed k, decide whether s is $\mathbb{Z}$-extendable in $S \subset \mathbf{Hom}_k(A,B)$ in polynomial time in $|A|\cdot|B|$. Furthermore, we know that if s is extendable then trivially it is $\mathbb{Z}$-extendable. So removing local sections which fail to be $\mathbb{Z}$-extendable will not remove any genuine global sections in S. This inspires the following algorithm.

3.3 The cohomological k-consistency algorithm

Here, we describe an extension to the k-consistency algorithm which utilises the notion of $\mathbb{Z}$-extendability.

Take as input a pair of σ-structures (A,B). Begin by setting $S_0 = \overline{\mathbf{Hom}_k(A,B)}$ as in the k-consistency algorithm then enter the following loop with $i = 0$:

1. Compute $S_{i+1} = \{s \in S_i \mid s \text{ is } \mathbb{Z}\text{-extendable in } S_i\}$
2. If $S_{i+1} = \emptyset$, then reject (A,B) and halt
3. If $S_{i+1} = S_i$ then accept (A,B) and halt.
4. Otherwise, return to Step 1 with $i = i+1$.

If this algorithm accepts a pair (A,B) we say that $\mathbf{CSP}(A,B)$ is cohomologically k-consistent and we write $A \to_k^{\mathbb{Z}} B$. It is clear that every element of the set S remaining when this algorithm terminates is $\mathbb{Z}$-extendable in S. By Lemma 1, S is also downward-closed and has the forth property. Furthermore, as $\mathbb{Z}$-extendability in any subset of S implies $\mathbb{Z}$-extendability in S (simply by setting any extra coefficients to 0), we have the following observation

Observation 2. *For any structures A and B $A \to_k^{\mathbb{Z}} B$ if and only if there exists a set $\emptyset \neq S \subset \mathbf{Hom}_k(A,B)$ in which each element $s \in S$ is $\mathbb{Z}$-extendable in S.*

We now demonstrate some basic facts about this relation and the given algorithm. Firstly, we show that the algorithm given above is efficient.

Proposition 3. *For fixed k and fixed finite signature σ, the relation $A \to_k^{\mathbb{Z}} B$ is decidable in polynomial time in the product of the sizes of A and B.*

Proof. We begin by noting that the main loop of the $\to_k^{\mathbb{Z}}$ algorithm either results in some S_{i+1} which is strictly smaller than S_i or it halts. This means that the number of iterations is bounded above by $|S_0|$ which is at most $|A|^k \cdot |B|^k$, i.e. polynomial in the product of the sizes of A and B.

Next we show that each iteration of the loop only takes polynomial time in $|A|\cdot|B|$. The body of each loop involves deciding, for each $s \in S_i$, whether or not s is $\mathbb{Z}$-extendable in S_i. For each s, this means checking the solvability of a system of at most $|A|^{2k}\cdot|B|^k$ $\mathbb{Z}$-linear equations in at most $|A|^k\cdot|B|^k$ variables, as noted above. This can be done in polynomial time for each s by the algorithm of Kannan and Bachem [19] and as $|S_i|$ is bounded by $|A|^k \cdot |B|^k$ this whole step takes only polynomial time in $|A|\cdot|B|$.

As the algorithm terminates if either the loop ends with $S_{i+1} = \emptyset$ or $S_{i+1} = S_i$ we know that it terminates and combining the arguments of the previous two paragraphs we know that it does so in polynomial time in $|A|\cdot|B|$. □

We conclude this section by showing that the relation $\to_k^{\mathbb{Z}}$ is transitive. In particular, we prove the following theorem.

Proposition 4. *For all k, given A, B and C structures over a common finite signature*

$$A \to_k^{\mathbb{Z}} B \to_k^{\mathbb{Z}} C \implies A \to_k^{\mathbb{Z}} C.$$

Proof. Success of the $\to_k^{\mathbb{Z}}$ algorithm for the pairs (A,B) and (B,C) results in two non-empty sets $S^{AB} \subset \mathbf{Hom}_k(A,B)$ and $S^{BC} \subset \mathbf{Hom}_k(B,C)$ in both of which each local section is $\mathbb{Z}$-extendable. By Observation 2, to show that $A \to_k^{\mathbb{Z}} C$, it suffices to show that the set $S^{AC} = \{s \circ t \mid s \in S^{BC}, t \in S^{AB}\}$ has the same property.

To show that every $p_0 = s_0 \circ t_0 \in S^{AC}_{\mathbf{a}_0}$ is $\mathbb{Z}$-extendable in S^{AC} we construct a global $\mathbb{Z}$-linear section extending p_0 from the $\mathbb{Z}$-linear sections $\{r^{t_0}_{\mathbf{a}} := \sum_t z_t t\}_{\mathbf{a} \in A^{\leq k}}$ and $\{r^{s_0}_{\mathbf{b}} := \sum_s w_s s\}_{\mathbf{b} \in B^{\leq k}}$ extending t_0 and s_0 respectively. Define $\{r^{p_0}_{\mathbf{a}}\}_{\mathbf{a}\in A^{\leq k}}$ as

$$r^{p_0}_{\mathbf{a}} = \sum_{t \in S^{AB}_{\mathbf{a}}} \sum_{s \in S^{BC}_{t(\mathbf{a})}} z_t w_s (s \circ t)$$

To show that this is a global $\mathbb{Z}$-linear section extending p_0 we need to show firstly that $r^{p_0}_{\mathbf{a}_0} = p_0$ and secondly that the local sections of r^{p_0} agree on the pairwise intersections of their domains.

To show that $r^{p_0}_{\mathbf{a}_0} = p_0$ we observe that, as r^{t_0} $\mathbb{Z}$-linearly extends t_0, for all $t \in S^{AB}_{\mathbf{a}_0}$ we have

$$z_t = \begin{cases} 1, & \text{for } t = t_0 \\ 0, & \text{otherwise,} \end{cases}$$

and similarly, for all $s \in S^{BC}_{t_0(\mathbf{a}_0)}$

$$w_s = \begin{cases} 1, & \text{for } w = w_0 \\ 0, & \text{otherwise.} \end{cases}$$

From this we have that

$$r^{p_0}_{\mathbf{a}_0} = z_{t_0} w_{s_0} (s_0 \circ t_0) = p_0$$

as required.

Finally, we need to show for any $\mathbf{a}, \mathbf{a}'$ in $A^{\leq k}$ with intersection $\mathbf{a}''$ that

$$r^{p_0}_{\mathbf{a}|_{\mathbf{a}''}} = r^{p_0}_{\mathbf{a}'|_{\mathbf{a}''}}.$$

To do this we show that the left hand side depends only on $\mathbf{a}''$ and not on $\mathbf{a}$. As this argument applies equally to the right hand side, the result follows.

To begin with the left hand side is a dependent sum which loops over $t \in S^{AB}_{\mathbf{a}}$ and $s \in S^{BC}_{t(\mathbf{a})}$ as follows:

$$r^{p_0}_{\mathbf{a}|_{\mathbf{a}''}} = \sum_{t,s} w_s z_t (s \circ t)_{|_{\mathbf{a}''}}$$

To emphasise the dependence on $\mathbf{a}''$ we can group this sum together by pairs t'', s'' with $t'' \in S^{AB}_{\mathbf{a}''}$ and $s'' \in S^{BC}_{t''(\mathbf{a}'')}$.

Within each group the the sum loops over $t \in S^{AB}_{\mathbf{a}}$ such that $t_{|_{\mathbf{a}''}} = t''$ and $s \in S^{AB}_{t(\mathbf{a})}$ such that $s_{|_{\mathbf{a}''}} = s''$. We write this as

$$\sum_{t'',s''} \sum_{t_{|_{\mathbf{a}''}}=t''} z_t \sum_{s_{|_{t''(\mathbf{a}'')}}=s''} w_s (s \circ t)_{|_{\mathbf{a}''}}$$

We now show that for each t'', s'' the corresponding part of the sum depends only on t'' and s''. This follows from three oberservations.

The first observation is that in the sum

$$\sum_{t_{|_{\mathbf{a}''}}=t''} z_t \sum_{s_{|_{t''(\mathbf{a}'')}}=s''} w_s (s \circ t)_{|_{\mathbf{a}''}}$$

the formal variables $(s \circ t)_{|_{\mathbf{a}''}}$ are, by definition, all equal to the variable $(s'' \circ t'')$. Thus we need only consider the coefficients, given by the sum

$$\sum_{t_{|_{\mathbf{a}''}}=t''} z_t \sum_{s_{|_{t''(\mathbf{a}'')}}=s''} w_s$$

The second observation is that for each t such that $t_{|_{\mathbf{a}''}} = t''$ the sum

$$\sum_{s_{|_{t''(\mathbf{a}'')}}=s''} w_s$$

is simply the s'' component of $(r^{s_0}_{t(\mathbf{a})})_{|_{t''(\mathbf{a}'')}}$. As r^{s_0} is a global $\mathbb{Z}$-linear section this is equal to the fixed parameter $w_{s''}$. So the sum in question reduces to

$$w_{s''} \cdot \left(\sum_{t_{|_{\mathbf{a}''}}=t''} z_t \right)$$

The final observation, is that the remaining sum is the t'' component of $(r^{t_0}_{\mathbf{a}})_{|_{\mathbf{a}''}}$ which, as r^{t_0} is a global $\mathbb{Z}$-linear section, is equal to $r^{t_0}_{t''}$. This gives the final form of the expression for $(r^{p_0}_{\mathbf{a}})_{|_{\mathbf{a}''}}$ as

$$\sum_{t'',s''} z_{t''} w_{s''} (t'' \circ s'')$$

It is easy to see that the same arguments apply to $r^{p_0}_{\mathbf{a}'}$ and so

$$(r^{p_0}_{\mathbf{a}})_{|_{\mathbf{a}''}} = (r^{p_0}_{\mathbf{a}'})_{|_{\mathbf{a}''}}$$

as required. □

In the next section, we demonstrate the power of this algorithm, using results from Abramsky, Barbosa, Kishida, Lal and Mansfield's paper *Contextuality, cohomology & paradox*[1].

4 Establishing the power of $\to^{\mathbb{Z}}_k$

In this section, we demonstrate the power of the cohomological k-consistency algorithm by proving that it can decide the solvability of systems of equations over finite fields.

To express the main theorem of this section in terms of the finite relational structures on which our algorithm is defined, we first need to fix a notion of a finite ring represented as a relational structure. Let R be a finite ring. Define σ_R as the (countable) set of relational symbols $\{E^m_{\mathbf{a},b} \mid m \in \mathbb{N}, \mathbf{a} \in R^m, b \in R\}$ where the arity for each $E^m_{\mathbf{a},b}$ is m. For any finite $\sigma \subset \sigma_R$ the *representation of R as a relational structure over σ* is the structure with universe the elements of R and for each symbol $E^m_{\mathbf{a},b} \in \sigma$ the related tuples are those $(r_1, \dots, r_m) \in R^m$ such that

$$a_1 \cdot r_1 + \dots a_m \cdot r_m = b$$

When R is represented in this way as a relational structure over σ, then any instance of the constraint satisfaction problem $\mathbf{CSP}(R)$ specifies a system of R-linear equations where each of the equations takes is of the form

$$a_1 \cdot x_1 + \dots a_m \cdot x_m = b$$

for some $E^m_{\mathbf{a},b} \in \sigma$.

With this notation established we can state the theorem we prove in this section.

Theorem 5. *For any finite ring R represented as a relational structure over a finite signature $\sigma \subset \sigma_R$, there is a k such that the cohomological k-consistency algorithm decides* $\mathbf{CSP}(B)$*. Alternatively stated, there exists a k such that for all σ-stuctures A*

$$A \to^{\mathbb{Z}}_k R \iff A \to R$$

This theorem is notable because for such rings R there are families of structures A_k such that $A_k \to_k R$ but $A_k \nrightarrow R$, see [13]. Furthemore there exist pairs (A_k, B_k) where $A_k \equiv_k B_k$, $B_k \to R$ and $A_k \to_k R$ but $A_k \nrightarrow R$, see [5]. As the sequence of relations $\equiv_k$ bounds the expressive power of FPC, this effectively proves the solvability of systems of linear equations over $\mathbb{Z}$ is not expressible in FPC, a result which was until now unknown to the author.

To prove this theorem we invoke a result from [1] which considers a similar set-up to that seen in the previous sections and proves a result relating the non-existence of solutions to a system of linear equations over a ring R to the non-triviality of a family of cohomological "obstructions". We will recall their set-up, the relevant result and a characterisation of these cohomological "obstructions" in terms of global $\mathbb{Z}$-linear sections before proving Theorem 5.

4.1 Result from *Contextuality, cohomology & paradox*

In order to state the relevant theorem, we start with some preliminary definitions. Let a *ring-valued measurement scenario* be a triple $\langle X, \mathcal{M}, R \rangle$ where X is a finite set, $\mathcal{M}$ is a downward closed cover of X and R is a ring. An *R-linear equation* on $\langle X, \mathcal{M}, R \rangle$ is a triple $\phi = (V_\phi, a, b)$ where $V_\phi \in \mathcal{M}$, $a : V_\phi \to R$ and $b \in R$. Then for any $s \in R^{V_\phi}$ we say that $s \models \phi$ if

$$\sum_{m \in V_\phi} a(m)s(m) = b$$

in the ring R.

An *empirical model* S on $\langle X, \mathcal{M}, R\rangle$ is a collection of sets $\{S_C\}_{C\in\mathcal{M}}$ where for each $C, S_C \subset R^C$ satisfying the following compatibility condition for all $C, C' \in \mathcal{M}$

$$\{s_{|C\cap C'} \mid s \in S_C\} = \{s'_{|C\cap C'} \mid s' \in S_{C'}\}$$

We make the following observation linking relational structures over signatures $\sigma \subset \sigma_R$ and empirical models which will be useful later.

Observation 6. *For any* $\mathbf{CSP}(A, R)$ *and* $S \subset \mathbf{Hom}_k(A, R)$ *which is non-empty, and downward-closed and satisfies the forth property then the local sections of* S *form an empirical model for the measurement scenario* $\langle A, A^{\leq k}, R\rangle$.

For an empirical model S on an R-valued measurement scenario, the *R-linear theory* of S is the set of R-linear equations

$$\mathbb{T}_R(S) = \{\phi \mid \forall s \in S_{V_\phi},\ s \models \phi\}$$

If $\mathbb{T}_R(S)$ is inconsistent (i.e. there is no R-assignment to all the variables in X simultaneously satisfying each of the R-linear equations in the theory), then the empirical model S is said to be "all-vs-nothing for R", written $\mathbf{AvN}_R(S)$.

We can now state the following results that we need for Theorem 5. The first result shows an important implication about the cohomological obstructions in an empirical model which has an inconsistent R-linear theory.

Theorem 7 (Abramsky, Barbosa, Kishida, Lal, Mansfield [1])**.** *For any ring* R *and any* R*-valued measurement scenario* $\langle X, \mathcal{M}, R\rangle$ *and any empirical model* S *we have that*

$$\mathbf{AvN}_R(S) \implies \mathbf{CSC}_{\mathbb{Z}}(S)$$

where $\mathbf{CSC}_{\mathbb{Z}}(S)$ *means that for every local section* s *in* S *the "cohomological obstruction" of Abramsky, Barbosa and Mansfield* $\gamma(s)$ *is non-zero.*

Next we have a result due to Abramsky, Barbosa and Mansfield which establishes this useful equivalent condition for $\mathbf{CSC}_{\mathbb{Z}}(S)$

Theorem 8 (Abramsky, Barbosa, Mansfield [4])**.** *For any empirical model* S*,* $\mathbf{CSC}_{\mathbb{Z}}(S)$ *if and only if for every* $s \in S_C$ *there is no collection* $\{r_{C'} \in \mathbb{Z}S_{C'}\}_{C'\in\mathcal{M}}$ *such that* $r_C = s$ *and for all* $C_1, C_2 \in \mathcal{M}$

$$r_{C_1|_{C_1\cap C_2}} = r_{C_2|_{C_1\cap C_2}}$$

This condition is precisely what inspired the cohomological k-consistency algorithm and in the next section we show how these two results imply Theorem 5.

4.2 Proof of Theorem 5

We now prove the main theorem of this section.

Theorem 5. *For any finite ring* R *represented as a relational structure over a finite signature* σ*, there is a* k *such that the cohomological* k*-consistency algorithm decides* $\mathbf{CSP}(B)$*. Alternatively, there exists a* k *such that for all* σ*-stuctures* A

$$A \to_k^{\mathbb{Z}} R \iff A \to R$$

Proof. The direction $A \to R \implies A \to_k^{\mathbb{Z}} R$ is easy and is true for all signatures σ and all $k \leq |A|$. Indeed note that to any homomorphism $f : A \to R$ we can associate the set $S_f = \{f_{|\mathbf{a}}\}_{\mathbf{a}\in A^{\leq k}} \subset \mathbf{Hom}_k(A, B)$. It is not hard to see that S_f is downward closed, has the forth property and that S_f is itself a global section witnessing the $\mathbb{Z}$-extendability of each $f_{|\mathbf{a}} \in S_f$. By Observation 2, this implies that $A \to_k^{\mathbb{Z}} R$.

This leaves the more challenging direction, that there exists a k such that $A \nrightarrow R \implies A \nrightarrow_k^{\mathbb{Z}} R$ for all A. Suppose that the maximum arity of a relation in σ is n. Then as R is a relational model of a finite ring we know that each relation on R is of the form $E^m_{\mathbf{a},b} = \{(r_1, \dots, r_m) \mid \sum_i a_i \cdot r_i = b\}$ where $\mathbf{a}$ is an m-tuple of elements of the ring R and b is an element of R. We show that $k = n$ will suffice to identify all unsatisfiable instances A.

For R and σ as above any instance $\mathbf{CSP}(A, R)$ is specified by a set A of variables where each related tuple $(x_1, \dots, x_m) \in (E^m_{\mathbf{a},b})^A$ specifies an R-linear equation $\sum_i a_i \cdot x_i = b$. Call the collection of such equations $\mathbb{T}^A$. The fact that there is no homomorphism $A \to R$ is exactly the statement that $\mathbb{T}^A$ is unsatisfiable. Taking $k = n$, we have that the R-linear theory $\mathbb{T}_R(\mathbf{Hom}_k(A, R))$ (as defined in the previous section) contains $\mathbb{T}^A$ and so is unsatisfiable. We now show how this is sufficient to prove the theorem.

Consider running the cohomological k-consistency algorithm on the pair (A, R) we get $S_0 = \overline{\mathbf{Hom}_k(A, R)}$. If $S_0 = \emptyset$ we are done. Otherwise, by Observation 6, S_0 can be considered as an empirical model on the measurement scenario $\langle A, A^{\leq k}, R\rangle$. Furthemore, as $S_0 \subset \mathbf{Hom}_k(A, R)$, we have that $\mathbb{T}_R(S_0) \supset \mathbb{T}_R(\mathbf{Hom}_k(A, R))$. This means in particular that $\mathbb{T}_R(S_0)$ is unsatisfiable by the assumption that $A \nrightarrow R$. By Theorems 7 and 8, this means that no local section s of S_0 is $\mathbb{Z}$-extendable in S_0, so $S_1 = \emptyset$. So the cohomological k-consistency algorithm rejects (A, R) and $A \nrightarrow_k^{\mathbb{Z}} R$, as required.

□

It is notable that in the proof of this theorem, we see that the cohomological k-consistency algorithm decides unsatisfiability of these systems of equations after just one iteration of its loop. A future version of this work will investigate whether multiple iterations are required in over different CSP domains. For now, we retain the iterative nature of the algorithm to guarantee the conclusion in Observation 2.

It is known, from a result of Atserias, Bulatov and Dawar[5], that the solvability of systems of linear equations over finite rings (even in a fixed number of variables per equation) is not definable in FPC . As the cohomological k-consistency consistency algorithm can decide the solvability of these systems of equations by Theorem 5 by repeatedly checking solvability of systems of linear equations over $\mathbb{Z}$, we have the following important corollary of Theorem 5.

Corollary 9. *The solvability of systems of linear equations over $\mathbb{Z}$ is not expressible in FPC.*

In the next section, we introduce an efficient algorithm approximating structure isomorphism which, similar to the cohomological k-consistency algorithm, is based on checking solvability systems of linear equations over $\mathbb{Z}$. We will show that this algorithm can distinguish structures which differ on other properties which are known to be inexpressible in FPC.

5 Cohomological k-Weisfeiler-Leman

In this section we define an efficient algorithm for distinguishing non-isomorphic structures inspired by the cohomological approach above. The equivalence, $\equiv_k^{\mathbb{Z}}$ computed refines that computed by the k-Weisfeiler-Leman algorithm on structures. The main result in this section shows that this refinement is strict and, in fact, that there is a fixed k such that $\equiv_k^{\mathbb{Z}}$ cam distinguish structures which disagree on a property which is inexpressible in FPC, rank logic and linear algebraic logic.

5.1 Cohomological k-Weisfeiler-Leman Equivalence

The study of efficient combinatorial algorithms for distinguishing non-isomorphic relational structures has a rich history in finite model theory, a great recent account of which is given, in the case of graphs, by Grohe and Schweitzer[15]. We introduce a novel algorithm of this form which builds on the important k-Weisfeiler-Leman algorithm. For all k, this algorithm computes a colouring of $(k-1)$-tuples of an input structure in polynomial time in its size. This in turn gives an efficiently computable equivalence relation $\equiv_{k-WL}$ on structures where $A \equiv_{k-WL} B$ if the k-Weisfeiler-Leman algorithm assigns the same colouring to the $(k-1)$-tuples of A and B.

Immerman and Lander[18] first established that two structures are $\equiv_{k-WL}$-equivalent if and only if they satisfy the same formulas of infinitary k-variable logic with counting quantifiers (written $A \equiv_k B$). Hella[17] showed that this is true if and only if the set of k-local partial isomorphisms $\mathbf{Isom}_k(A, B)$ contains a non-empty subset S which is downward-closed and has the following *bijective forth property* for all $f \in S$ with $|\mathbf{dom}(f)| < k$:

$$\exists b_f : A \to B \text{ a bijection s.t. } \forall a \in A \; f \cup \{(a, b_f(a))\} \in S$$

Whether such a bijection exists can be determined efficiently given A, B, S and f by determining if the bipartite graph with vertices $A \sqcup B$ and edges $\{(a,b) \mid f \cup \{(a,b)\} \in S\}$ has a perfect matching. For $S \subset \mathbf{Isom}_k(A, B)$, let $\overline{\overline{S}}$ be the largest subset of S which is downward-closed and satisfies the bijective forth property. For fixed k this can be computed in polynomial time in the sizes of A and B and so an alternative polynomial time algorithm for determining $\equiv_{k-WL}$ is computing $\overline{\overline{\mathbf{Isom}_k(A, B)}}$ and checking if it is non-empty.

We now define cohomological k-equivalence to generalise k-WL-equivalence in the same way as we did for cohomological k-consistency, by removing local sections which are not $\mathbb{Z}$-extendable. As $\mathbb{Z}$-extendability in $S \subset \mathbf{Isom}_k(A, B)$ is not *a priori* symmetric in A and B we need to check that both s is $\mathbb{Z}$-extendable in S and s^{-1} is $\mathbb{Z}$-extendable in $S^{-1} = \{t^{-1} \mid t \in S\}$. We call this s being *$\mathbb{Z}$-bi-extendable* in S and we incorporate this in the algorithm as follows. Take as input a pair of σ-structures (A, B). Begin by computing $S_0 = \overline{\overline{\mathbf{Isom}_k(A, B)}}$ as in the k-WL equivalence algorithm. If $S_0 = \emptyset$, then reject the pair (A, B) and halt. Otherwise we enter the following loop with $i = 0$:

1. Compute $S_i^{\mathbb{Z}} = \{s \in S_i \mid s \text{ is } \mathbb{Z}\text{-bi-extendable in } S_i\}$
2. Compute $S_{i+1} = \overline{\overline{S_i^{\mathbb{Z}}}}$
3. If $S_{i+1} = \emptyset$, then reject (A, B) and halt
4. If $S_{i+1} = S_i$ then accept (A, B) and halt.
5. Return to Step 1 with $i = i + 1$.

If this algorithm accepts a pair (A, B) we say that A and B are cohomologically k-equivalent and we write $A \equiv_k^{\mathbb{Z}} B$.

We now record some simple facts about this equivalence. Firstly, by definition, this generalises k-equivalence and so (k)-WL equivalence, i.e.

$$A \equiv_k^{\mathbb{Z}} B \implies A \equiv_k B \iff A \equiv_{(k-1)-WL} B$$

Secondly, this algorithm determines a maximal set $S \subset \mathbf{Isom}_k(A, B)$ which is downward-closed, has the bijective forth property and for which each $f \in S$ is $\mathbb{Z}$-extendable in S and f^{-1} is $\mathbb{Z}$-extendable in S^{-1}. However, analogously to Observation 2, we note that the existence of any non-empty S satisfying these properties is a witness of $\equiv_k^{\mathbb{Z}}$.

Observation 10. *For any two structures A and B, $A \equiv_k^{\mathbb{Z}} B$ if and only if there exists a subset $S \subset \mathbf{Isom}_k(A, B)$ such that both S and S^{-1} are downward-closed, has the bijective forth property and have $\mathbb{Z}$-extendability for each of their elements.*

Finally, we observe that such a set also satisfies the conditions for witnessing cohomological k-consistency of $\mathbf{CSP}(A, B)$ and $\mathbf{CSP}(B, A)$. Formally we have

Observation 11. *For any two structures A and B, $A \equiv_k^{\mathbb{Z}} B$ implies that $A \to_k^{\mathbb{Z}} B$ and $B \to_k^{\mathbb{Z}} A$.*

In the next section we establish how this equivalence relation behaves with respect to logical interpretations.

5.2 $\equiv_k^{\mathbb{Z}}$ and interpretations

There are many different notions of logical interpretation in finite model theory. The one we consider is defined as follows. A C^l-*interpretation* Φ (of order n) of signature τ in signature σ is a tuple of $C^l[\sigma]$ formulas $\langle \phi_R \rangle_{R\in\tau}$. For each relation symbol $R \in \tau$ of arity r, the formula ϕ_R has nr free variables and is written as $\phi_R(\mathbf{x}_1, \dots, \mathbf{x}_r)$, where the $\mathbf{x}_i$ are n-tuples of variables. Such an interpretation defines a map from σ-structures to τ-structures as follows. For any A, $\Phi(A)$ has universe A^n and for each relational symbol $R \in \tau$, the set of related tuples is given by

$$R^{\Phi(A)} := \{(\mathbf{a}_1, \dots, \mathbf{a}_r) \in (A^n)^r \mid A, \mathbf{a}_1, \dots, \mathbf{a}_r \models \phi_R\}$$

In the next result, we show that the equivalence $\equiv_k^{\mathbb{Z}}$ is preserved by C^l-interpretations in the following way.

Proposition 12. *For any (finite, relational) signatures σ and τ, σ-structures A and B, natural numbers n and k, and any order n C^{nk}-interpretation Φ of τ in σ we have that*

$$A \equiv_{nk}^{\mathbb{Z}} B \implies \Phi(A) \equiv_k^{\mathbb{Z}} \Phi(B)$$

Proof. By Observation 10, it suffices to show that there is a set $S' \subset \mathbf{Isom}_k(\Phi(A), \Phi(B))$ which is downward-closed, satisfies the bijective forth property and in which every map is $\mathbb{Z}$-extendable. As $A \equiv_{nk}^{\mathbb{Z}} B$, there is already a set $S \subset \mathbf{Isom}_{nk}(A, B)$ satisfying these properties. For any $Q \subset A$ we use S_Q to mean the elements of S with domain Q. We now show how to construct a suitable S' from S.

For any $C \subset \Phi(A)$, let $\pi(C)$ be the set of element in A which appear in some tuple of C. As elements of $\Phi(A)$ are n-tuples over A, it is clear that $|\pi(C)| \leq n|C|$. We can now define S'_C as the set of partial isomorphisms in $S_{\pi(C)}$ applied coordinatewise to C, namely,

$$\{(f, \dots, f)_{|C} \mid f \in S_{\pi(C)}\}$$

This is well defined for all $C \in (\Phi(A))^{\leq k}$ as $|\pi(C)| \leq nk$. That these maps define partial isomorphisms between $\Phi(A)$ and $\Phi(B)$ follows from Hella's Lemma 5.1 in [17] which states that the elements of $\overline{\overline{\mathbf{Isom}_{nk}(A, B)}}$ are exactly those which preserve and reflect C^{nk} formulas. As the relations on $\Phi(A)$ and $\Phi(B)$ are defined by C^{nk} formulas they are preserved and reflected by the members of S. We now show that $S' = \bigcup_{C\in\Phi(A)^{\leq k}} S'_C$ satisfies the required properties.

Downward-closure. This follows easily from downward-closure of S. Suppose $\mathbf{f} = (f, \dots, f)_{|C} \in S'$ and $\mathbf{g} \leq \mathbf{f}$. Then there is some $C' \subset C$ such that $\mathbf{g} = \mathbf{f}_{|C'}$ and $\mathbf{g} = (f_{|\pi(C')}, \dots, f_{|\pi(C')})_{|C'}$. but $f_{|\pi(C')} \leq f$ and so is an element of S.

Bijective forth property. Let $\mathbf{f} \in S'_C$ with $|C| < k$, with $\mathbf{f}$ given as the coordinatewise application of some $f \in S_{\pi(C)}$. To show that S' has the bijective forth property we must show that there is a bijection $b : \Phi(A) \to \Phi(B)$ such that for any $\mathbf{a} \in \Phi(A)$ the function $\mathbf{f} \cup \{(\mathbf{a}, b(\mathbf{a}))\}$ is in $S'_{C\cup\{\mathbf{a}\}}$. For any such $\mathbf{f}$, we can construct a bijection b whose image on any $\mathbf{a} \in \Phi(A)$ is given as

$$b(\mathbf{a}) = (b^{\epsilon}(a_1), b^{\mathbf{a}_1}(a_2), \dots, b^{(\mathbf{a}_{n-1})}(a_n))$$

where $\mathbf{a}_i$ is the i-tuple of the first i elements in $\mathbf{a}$ and each $b^{\mathbf{a}_i}$ is a bijection $A \to B$. For any $\mathbf{a} \in \Phi(A)$ we choose the bijections $b^{\mathbf{a}_i}$ using the bijective forth property on S. As $\mathbf{f}$ is a coordinatewise application of some $f \in S_{\pi(C)}$ and as $|C| < k$ implies $|\pi(C)| \leq nk - n < nk$, the bijective forth property for S implies the existence of a b_1 such that $f_1 = f \cup \{a_1, b_1(a_1)\} \in S_{\pi(C)\cup\{a_1\}}$. Let $b^{\epsilon} := b_1$. Now suppose for any $i < n$ we have defined the bijections $b^{\epsilon}, b^{\mathbf{a}_1}, \dots, b^{\mathbf{a}_i}$ and $f_i = f \cup \{(a_j, b^{\mathbf{a}_{j-1}}(a_j))\}_{1\leq j\leq i} \in S_{\pi(C)\cup\{a_1,\dots,a_i\}}$. We still have $|\pi(C) \cup \{a_1, \dots, a_i\}| < nk$ so can use the bijective forth property on S again to find a bijection $b^{\mathbf{a}_i}$ such that $f_{i+1} = f_i \cup \{(a_i, b_{\mathbf{a}_i}(a_i))\} \in S_{\pi(C)\cup\{a_1,\dots,a_{i+1}\}}$. This inductive procedure defines all the required bijections and furthermore shows that $\mathbf{f} \cup \{(\mathbf{a}, b(\mathbf{a})\}$ is the coordinatewise application of some $f_n \in S_{\pi(C\cup\{\mathbf{a}\})}$. This means in particular that $\mathbf{f} \cup \{(\mathbf{a}, b(\mathbf{a})\}$ is in $S'_{C\cup\{\mathbf{a}\}}$, as required.

$\mathbb{Z}$-extendability. Our choice of S' makes $\mathbb{Z}$-entendability rather easy. Indeed, we see that any $\mathbf{f} = (f, \dots, f) \in S'_C$ is $\mathbb{Z}$-extendable because the $\mathbb{Z}$-linear global section extending $f \in S_{\pi(C)}$ given as $s_C = \sum_{g\in S_C} \alpha_g g$ can be lifted to a $\mathbb{Z}$-linear extension of $\mathbf{f}$ by defining $s'_C = \sum_{g\in S_{\pi(C)}} \alpha_g(g, \dots, g)$. The properties of being a $\mathbb{Z}$-linear extension follow from those properties on S.

□

5.3 Deciding the CFI property

Cai, Furer and Immerman[9] showed that there is a property of relational structures which can be decided in polynomial time but which cannot be expressed in infinitary first-order logic with counting quantifiers for any number of variables. This construction essentially encodes certain systems of linear equations (over $\mathbb{Z}_2$) on top of graphs in such a way that isomorphism of the constructed structures is determined by checking solvability of the systems of equations. In their seminal paper[9], Cai, Furer and Immerman show that the solvable and unsovable versions of their construction cannot be disguished in fixed point logic with counting. Adaptations of this construction, encoding equations over different finite fields were used by Dawar, Grädel and Pakusa to show that adding rank quantifiers over each finite field added distinct expressive power to FPC and a version using equations over the rings $\mathbb{Z}_{2^q}$ was used by Lichter[21] to separate rank logic from `PTIME`.

As cohomological k-consistency was shown in the previous section to simultaneously decide solvability over any finite ring, it is natural to ask whether the related equivalence $\equiv_k^{\mathbb{Z}}$ can decide these CFI properties which are not definable in FPC, rank logic or linear algebraic logic. We show in this section that it can.

Following Lichter[21], we define the general CFI construction $\mathbf{CFI}_q(G, g)$ for q a prime power, $G = (G, <)$ an ordered undirected graph and g a function from the edge set of G to $\mathbb{Z}_q$. The idea is that the construction encodes a system of linear equations over $\mathbb{Z}_q$ into G while the function g "twists" these equations in a certain way. For CFI structures, $\mathbf{CFI}_q(G, g)$ the property $\sum g = 0$ is sometimes called the *CFI property*. The following well-known fact (see [22], for example) shows that this property is closed under isomorphisms and is useful in our later arguments.

Fact 13. *For any prime power, q, ordered graph G, and functions g, h from the edges of G to $\mathbb{Z}_q$,*

$$\mathbf{CFI}_q(G, g) \cong \mathbf{CFI}_q(G, h) \iff \sum g = \sum h$$

$\mathbf{CFI}_q(G, g)$ is built in three steps. First, we define a gadget which will replaces each vertex of x with elements that form a ring. Secondly, we define relations between gadgets which impose consistency equations between gadgets. Finally, the function g is used to insert the important twists into the consistency equations. We now describe this in detail below, following a presentation by Lichter[21].

Vertex gadgets. For any vertex $x \in G$, let $N(x)$ be the neighbourhood of x in G (i.e. those vertices which share edges with x) and let $\mathbb{Z}_q^{N(x)}$ denote the ring of functions from $N(x)$ to the ring $\mathbb{Z}_q$. We will replace each vertex x of the base graph with a gadget whose vertices are the following subset of $\mathbb{Z}_q^{N(x)}$,

$$A_x = \{\mathbf{a} \in \mathbb{Z}_q^{N(x)} \mid \sum_{y \in N(x)} \mathbf{a}(y) = 0\}$$

The relations on the gadget are for each y in $N(x)$ a symmetric relation

$$I_{x,y} = \{(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}(y) = \mathbf{b}(y)\}$$

and a directed cycle encoded by the relation

$$C_{x,y} = \{(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}(y) = \mathbf{b}(y) + 1\}$$

Together these impose the ring structure of $\mathbb{Z}_q^{N(x)}$ onto the vertices of the gadget.

Edge equations. Next define a relation between gadgets for each edge $\{x, y\}$ in G and each constant $c \in \mathbb{Z}_q$ of the form

$$E_{\{x,y\},c} = \{(\mathbf{a}, \mathbf{b}) \mid \mathbf{a} \in A_x,\ \mathbf{b} \in A_y,\ \mathbf{a}(y) + \mathbf{b}(x) = c\}$$

Putting it together with a twist. We finally define the structure $\mathbf{CFI}_q(G, g)$ as $\langle A, \prec, R_I, R_C, R_{E,0}, R_{E,1}, \ldots, R_{E,q-1} \rangle$ where the universe is $A = \cup_x A_x$ where $\prec$ is the linear pre-order

$$\prec = \bigcup_{x<y} A_x \times A_y$$

and the edge equations $R_{E,c}$ are interpreted according to the twists in g as

$$R_{E,c} = \bigcup_{e \in E} E_{e,c+g(e)}$$

where the sum in the subscript is over $\mathbb{Z}_q$ For the relations R_I and R_C we deviate slightly from Lichter's construction and interpret these as ternary relations of the following form

$$R_I = \bigcup_{\{x,y\} \in E} I_{x,y} \times A_y$$

$$R_C = \bigcup_{\{x,y\} \in E} C_{x,y} \times A_y$$

We now use recall the two major separation results based on this construction. The first is a landmark result of descriptive complexity from the early 1990's.

Theorem 14 (Cai, Furer, Immerman[9])**.** *There is a class of ordered (3-regular) graphs $\mathcal{G} = \{G_n\}_{n \in \mathbb{N}}$ such that in the respective class of CFI structures*

$$\mathcal{K} = \{\mathbf{CFI}_2(G, g) \mid G \in \mathcal{G}\}$$

the CFI property is decidable in polynomial-time but cannot be expressed in FPC.

The second is a recent breakthrough due to Moritz Lichter.

Theorem 15 (Lichter[21])**.** *There is a class of ordered graphs $\mathcal{G} = \{G_n\}_{n \in \mathbb{N}}$ such that in the respective class of CFI structures*

$$\mathcal{K} = \{\mathbf{CFI}_{2^k}(G, g) \mid G \in \mathcal{G}\}$$

the CFI property is decideable in polynomial-time (indeed, expressible in choiceless polynomial time) but cannot be expressed in rank logic.

We now show that in both of these classes there exists a fixed k such that $\equiv_k^{\mathbb{Z}}$ distinguishes structures which differ on the CFI property. This relies on two lemmas. The first shows that this property is equivalent to the solvability of a certain system of equations over $\mathbb{Z}_q$, while the second shows that this system of equations can be interpreted in on the classes above with a uniform bound on the number of variables per equation.

The first lemma is an adaptation of Lemma 4.36 from Wied Pakusa's PhD thesis[22]. We begin by defining for any $\mathbf{CFI}q(G, g)$ a system of linear equations over $\mathbb{Z}_q$. This system, $\mathbf{Eq}_q(G, g)$, is the following collection of equations:

- $X_{\mathbf{a},u}$ for all $u \in G$ and all $\mathbf{a} \in A_u \subset \mathbf{CFI}_q(G, g)$,
- $I_{\mathbf{a},\mathbf{b},v}$ for all $u \in G$ and $\mathbf{a}, \mathbf{b} \in A_u$ such that there exists $v \in N(u)$ and $\mathbf{c} \in A_v$ such that $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in R_I$,

- $C_{\mathbf{a},\mathbf{b},v}$ for all $u \in G$ and $\mathbf{a}, \mathbf{b} \in A_u$ such that there exists $v \in N(u)$ and $\mathbf{c} \in A_v$ $(\mathbf{a}, \mathbf{b}, \mathbf{c}) \in R_C$, and
- $E_{\mathbf{a},\mathbf{b},c}$ for all $\mathbf{a} \in A_u, \mathbf{b} \in A_v$ and $(\mathbf{a}, \mathbf{b}) \in R_{E,c}$

where the variables are $w_{\mathbf{a},v}$ for every $u \in G$, $\mathbf{a} \in A_u$ and $v \in N(u)$ and the equations are given as:

$$\begin{aligned} X_{\mathbf{a},u} : &\quad \sum_{v \in N(u)} w_{\mathbf{a},v} = 0 \\ I_{\mathbf{a},\mathbf{b},v} : &\quad w_{\mathbf{a},v} - w_{\mathbf{b},v} = 0 \\ C_{\mathbf{a},\mathbf{b},v} : &\quad w_{\mathbf{a},v} - w_{\mathbf{b},v} = 1 \\ E_{\mathbf{a},\mathbf{b},c} : &\quad w_{\mathbf{a},v} + w_{\mathbf{b},u} = c \end{aligned}$$

Then we have the following lemma.

Lemma 16. $\mathbf{CFI}_q(G, g)$ *a CFI structure, has* $\sum g = 0$ *if and only if* $\mathbf{Eq}_q(G, g)$ *is solvable in* $\mathbb{Z}_q$

Proof. Fristly we recall Fact 13 that $\sum g = 0$ if and only if there is an isomorphism $f : \mathbf{CFI}_q(G, g) \to \mathbf{CFI}_q(G, \mathbf{0})$, where $\mathbf{0}$ is the constant 0 function. We now show that there is such an isomorphism if and only if there is a solution to $\mathbf{Eq}_q(G, g)$.

For the forward direction, suppose that we have an isomorphism $f : \mathbf{CFI}_q(G, g) \to \mathbf{CFI}_q(G, \mathbf{0})$. Now as f is a bijection and preserves the pre-order $\prec$, we have that for any $u \in G$, f maps A_u to A_u. This means that for any $\mathbf{a} \in A_u$ $f(\mathbf{a})$ is a function in $\mathbb{Z}_q^{N(u)}$. This means that the assignment $w_{\mathbf{a},v} \mapsto f(\mathbf{a})(v)$ is well-defined for all the variables in $\mathbf{Eq}_q(G, g)$. We now show that this assigment satisfies the system of equations. The X equations in $\mathbf{Eq}_q(G, g)$ become the statement that for all $u \in G$ and $\mathbf{a} \in A_u$

$$\sum_{v \in N(u)} f(\mathbf{a})(v) = 0$$

which follows directly from the fact that $f(\mathbf{a}) \in A_u$. For the I and C equations, we note that as f preserves all relations from $\mathbf{CFI}_q(G, g)$. So for any $\mathbf{a}, \mathbf{b} \in A_u$ and $\mathbf{c} \in A_v$ such that $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ is related by R_I or R_C in $\mathbf{CFI}_q(G, g)$ then $(f(\mathbf{a}), f(\mathbf{b}), f(\mathbf{c}))$ is similarly related in $\mathbf{CFI}_q(G, \mathbf{0})$. The definitions of these relations imply that $f(\mathbf{a})(v) - f(\mathbf{b})(v)$ is 0 or 1 respectively, which implies that our assignment to the variables $w_{\mathbf{a},v}$ and $w_{\mathbf{b},v}$ satisfies the relevant I or C equation. A similar argument applies to the E equations except that the conclusion from $(f(\mathbf{a}), f(\mathbf{b})) \in R_{E,c}$ in $\mathbf{CFI}_q(G, \mathbf{0})$ that the relevant E equation is satisfied follows from the fact that there is no twisting of the $R_{E,c}$ relation in $\mathbf{CFI}_q(G, \mathbf{0})$.

The reverse direction is the observation that any satisfying assignment to the variables $w_{\mathbf{a},v}$ in $\mathbf{Eq}_q(G, g)$ defines an isomorphism from $\mathbf{CFI}_q(G, g)$ to $\mathbf{CFI}_q(G, \mathbf{0})$ where $f(\mathbf{a})(v) = w_{\mathbf{a},v}$. Satisfying the X equation guarantees that for $\mathbf{a} \in A_u$ its image $f(\mathbf{a})$ is also in A_u. Satisfying the I and C equations ensures that the R_I and R_C relations are preserved. So, the additive structure of $\mathbb{Z}_q^{N(u)}$ is preserved in A_u and thus f is bijective. Finally the E equations define the $R_{E,c}$ relation in $\mathbf{CFI}_q(G, \mathbf{0})$ and so satisfying these ensures that f preserves the $R_{E,c}$ relation. □

It is not hard to see that the system $\mathbf{Eq}_q(G, g)$ is first order interpretable in $\mathbf{CFI}_q(G, g)$. However, Theorem 5 shows that cohomological k-consistency decides satisfiability of systems of equations over any ring in with up to k variables per equation. Thus to show that cohomological k-equivalence distinguishes positive and negative instances of the CFI property for some fixed k we need to show that an equivalent system of equations can be interpreted which fixes the number of variables per equation. This is the content of the following lemma.

Lemma 17. *For any prime power q, there is an interpretation* Φ_q *from the signature of the CFI structures* $\mathbf{CFI}_q(G, g)$ *to the signature of the ring* $\mathbb{Z}_q$ *with relations of arity at most* 3 *such that*

$$\Phi_q(\mathbf{CFI}_q(G, g)) \to \mathbb{Z}_q \iff \sum g = 0$$

Proof. From Lemma 16, we know that interpreting the system of equations $\mathbf{Eq}_q(G, g)$ would suffice for this purpose. However, the X equations in $\mathbf{Eq}_q(G, g)$ contain a number of variables which grows with the size of the maximum degree of a vertex in G. As this is, in general, unbounded - and in particular is unbounded in Lichter's class - we need to introduce some equivalent equations in a bounded number of variables. To do this we will introduce some slack vairables and utilise the ordering on G to turn any such equation in n variables into a series of equations in 3 variables. We now describe the interpretation Φ_q as follows.
Let 3-$\mathbb{Z}_q$ denote the relational structure which contains a relation $T_{\alpha,\beta}$ for each α a tuple of elements of $\mathbb{Z}_q$ size up to 3 and $\beta \in \mathbb{Z}_q$. Each related tuple $(x, y, z) \in T_{\alpha,\beta}$ in a 3-$\mathbb{Z}_q$ structure is an equation

$$\alpha_1 x + \alpha_2 y + \alpha_3 z = \beta$$

To help define the interpretation we introduce some shorthand for some easily interpretable relations on CFI structures A. For $\mathbf{a}, \mathbf{b} \in A$ write $\mathbf{a} \sim \mathbf{b}$ if the two elements belong to the same gadget in A and $\mathbf{a} \frown \mathbf{b}$ if they belong to adjacent gadgets. Both of these relations are easily first-order definable as $\mathbf{a} \sim \mathbf{b}$ if and only if they are incomparable in the $\prec$ relation and $\mathbf{a} \frown \mathbf{b}$ if and only if $(\mathbf{a}, \mathbf{b}) \in R_{E,c}$ for some c. For $\mathbf{a} \frown \mathbf{b}$ in A we will refer to the elements $(\mathbf{a}, \mathbf{a}, \mathbf{b})$ and $(\mathbf{a}, \mathbf{b}, \mathbf{b})$ as $w_{\mathbf{a},\mathbf{b}}$ and $z_{\mathbf{a},\mathbf{b}}$. These will be the variables in the interpreted system of equations. As A comes with a linear pre-order $\prec$ inherited from the order on G, we can also define a local predecessor relation in the neighbourhood of any $\mathbf{a} \in A$. We say that $\mathbf{b}$ is a local predecessor of $\mathbf{b}'$ at $\mathbf{a}$ and write $\mathbf{b} \vdash_{\mathbf{a}} \mathbf{b}'$ if $\mathbf{a} \frown \mathbf{b}$ and $\mathbf{a} \frown \mathbf{b}'$ and there is no $\mathbf{b}''$ with $\mathbf{a} \frown \mathbf{b}''$ such that $\mathbf{b} \prec \mathbf{b}'' \prec \mathbf{b}'$.

Now we define the interpretation on A^3 in three steps, resulting in a system of equations which is solvable if and only if $\mathbf{Eq}_q(G, g)$ is solvable.

Step 1: Reducing variables. We note that in $\mathbf{Eq}_q(G, g)$ there are only variables $w_{\mathbf{a},y}$ for $\mathbf{a} \in A_x$ and $y \in N(x)$, whereas the shorthand above describes variables $w_{\mathbf{a},\mathbf{b}}$ and $z_{\mathbf{a},\mathbf{b}}$ for all $\mathbf{a} \in A_x$ and $\mathbf{b} \in A_y$. To reduce the number of variables we want to interpret, for all $\mathbf{a} \frown \mathbf{b}$ and $\mathbf{b} \sim \mathbf{b}'$, the equations $w_{\mathbf{a},\mathbf{b}} = w_{\mathbf{a},\mathbf{b}'}$ and $z_{\mathbf{a},\mathbf{b}} = z_{\mathbf{a},\mathbf{b}'}$. This is done by add the pairs $(w_{\mathbf{a},\mathbf{b}}, w_{\mathbf{a},\mathbf{b}'})$ and $(z_{\mathbf{a},\mathbf{b}}, z_{\mathbf{a},\mathbf{b}'})$ to the relation $T_{(1,-1),0}$ which can be done as $\frown$ and $\sim$ are definable.

Step 2: Interpreting I, C and E equations. Defining these equations in $\Phi(A)$ is straightforward as they all have fewer than 3 variables. In particular we want to add equations

$$w_{\mathbf{a},\mathbf{b}} - w_{\mathbf{a}',\mathbf{b}} = 0$$

for any $(\mathbf{a}, \mathbf{a}', \mathbf{b}) \in R_I$,

$$w_{\mathbf{a},\mathbf{b}} - w_{\mathbf{a}',\mathbf{b}} = 1$$

for any $(\mathbf{a}, \mathbf{a}', \mathbf{b}) \in R_C$, and

$$w_{\mathbf{a},\mathbf{b}} + w_{\mathbf{b},\mathbf{a}} = c$$

for any $(\mathbf{a}, \mathbf{b}) \in R_{E,c}$. These are all easily first-order definable in the $\mathbf{CFI}_q$ signature.

Step 3: Interpreting X equations. To interpret the equations for each $u \in G$ and $\mathbf{a} \in A_u$

$$\sum_{v \in N(u)} w_{\mathbf{a},v} = 0$$

in $\Phi(A)$, we first note that the linear order on G restricts to a linear order on $N(u)$ which we can write as $\{v_1, \ldots, v_n\}$ where $i < j$ if and only if $v_i < v_j$. To do this it suffices to impose the equations

$$w_{\mathbf{a},\mathbf{b}_1} + \cdots + w_{\mathbf{a},\mathbf{b}_n} = 0$$

for each sequence of elements $\mathbf{b}_1 \vdash_\mathbf{a} \ldots \vdash_\mathbf{a} \mathbf{b}_n$ with $\mathbf{b}_i \in A_{v_i}$. To do this in equations with at most three variables we employ the auxilliary z variables in the following way. For any $\mathbf{ab} \in A$ such that $\mathbf{a} \frown \mathbf{b}$, if there is no $\mathbf{b}'$ such that $\mathbf{b}' \vdash_\mathbf{a} \mathbf{b}$, then we interpret the equation

$$w_{\mathbf{a},\mathbf{b}} - z_{\mathbf{a},\mathbf{b}} = 0$$

if there is $\mathbf{b}'$ such that $\mathbf{b}' \vdash_\mathbf{a} \mathbf{b}$ then interpret for all such $\mathbf{b}'$ the equation

$$z_{\mathbf{a},\mathbf{b}'} + w_{\mathbf{a},\mathbf{b}} - z_{\mathbf{a},\mathbf{b}} = 0$$

and if there is no $\mathbf{b}'$ such that $\mathbf{b} \vdash_\mathbf{a} \mathbf{b}'$ then interpret the equation

$$z_{\mathbf{a},\mathbf{b}} = 0$$

In this system of equations the $z_{\mathbf{a},\mathbf{b}}$ variables act as running totals for the sum $\sum w_{\mathbf{a},\mathbf{b}_i}$ and so it is not hard to see that solutions to these equations are precisely solutions to the equations $\sum w_{\mathbf{a},\mathbf{b}_i} = 0$. Furthermore, as the relation $\vdash_\mathbf{a}$ is definable in the signature of the $\mathbf{CFI}_q$ structures so too are these equations.

To conclude, we have interpreted in $\Phi(\mathbf{CFI}_q(G, g))$ a system of linear equations with three variables per equation which is solvable over $\mathbb{Z}_q$ if and only if $\mathbf{Eq}_q(G, g)$ is solvable. Thus there is a homomorphism $\Phi(\mathbf{CFI}_q(G, g)) \to \mathbb{Z}_q$ (as 3-$\mathbb{Z}_q$ structures) if and only if $\sum g = 0$. □

We can now conclude that the CFI property is preserved by $\equiv_k^\mathbb{Z}$ for some fixed k.

Theorem 18. *There is a fixed k such that for any q given $\mathbf{CFI}_q(G, g)$ and $\mathbf{CFI}_q(G, h)$ with $\sum g = 0$ we have*

$$\mathbf{CFI}_q(G, g) \equiv_k^\mathbb{Z} \mathbf{CFI}_q(G, h) \iff \sum h = 0$$

Proof. By Fact 13, the reverse implication is easy as $\sum h = 0$ implies that $\mathbf{CFI}_q(G, g) \cong \mathbf{CFI}_q(G, h)$ and so the structures are cohomologically k-equivalent for any k.
The converse follows from the series of lemmas we have just presented. If $\sum h \neq 0$ then by Lemma 17 there is an interpretation Φ_q of order 3 such that $\Phi_q(\mathbf{CFI}_q(G, g)) \to \mathbb{Z}_q$ but $\Phi_q(\mathbf{CFI}_q(G, h)) \nrightarrow \mathbb{Z}_q$. By Theorem 5, This is means that $\Phi_q(\mathbf{CFI}_q(G, g)) \to_3^\mathbb{Z} \mathbb{Z}_q$ but $\Phi_q(\mathbf{CFI}_q(G, h)) \nrightarrow_3^\mathbb{Z} \mathbb{Z}_q$. So by Observation 11, we must have that $\Phi_q(\mathbf{CFI}_q(G, g)) \not\equiv_3^\mathbb{Z} \Phi_q(\mathbf{CFI}_q(G, h))$. Then noting that the number of variables used in the interpretation Φ_q is some constant c not depending on q and assuming without loss of generality that k is greater than $3c$ then Proposition 12 implies that $\mathbf{CFI}_q(G, g) \not\equiv_k^\mathbb{Z} \mathbf{CFI}_q(G, h)$, as required. □

As a direct consequence of this result, there is some k such that the set of structures with the CFI property in Lichter's class $\mathcal{K}$ from Theorem 15 is closed under $\equiv_k^\mathbb{Z}$. This means that, by the conclusion of Theorem 15, the equivalence relation $\equiv_k^\mathbb{Z}$ can distinguish structures which disagree on a property that is not expressible in rank logic. Indeed, as Dawar, Grädel and Lichter[11] show that this property is also inexpressible in linear algebraic logic, the following strengthening of Corollary 9 follows from Theorem 18 and our definition of the cohomological k-Weisfeiler-Leman algorithm.

Corollary 19. *The solvability of $\mathbb{Z}$-linear equations is not expressible in linear algebraic logic.*

6 Conclusions & future work

In this paper, we have presented novel efficient generalisations of the k-consistency and k-Weisfeiler-Leman algorithms, based on solving systems of equations over $\mathbb{Z}$ and inspired by recent cohomological approaches in quantum contextuality[4]. We have shown that the relations, $\to_k^\mathbb{Z}$ and $\equiv_k^\mathbb{Z}$, computed by these new algorithms are strict refinements of their well-studied classical counterparts $\to_k$ and $\equiv_k$. In particular, we have shown in Theorem 5 that cohomological k-consistency suffices to solve linear equations over all finite rings and in Theorem 18 that cohomological k-Weisfeiler-Leman distinguishes positive and negative instances of the CFI property on the classes of structures studied by Cai, Furer and Immerman [9] and more recently by Lichter[21]. These results have important consequences for descriptive complexity theory showing, in particular, that the solvability of systems of linear equations over $\mathbb{Z}$ is not expressible in FPC, rank logic or linear algebraic logic. Furthermore, the results of this paper demonstrate the unexpected effectiveness of a cohomological approach to constraint satisfaction and structure isomorphism, analogous to that pioneered by Abramsky and others for the study of quantum contextuality.

The results of this paper suggest several directions for future work to establish the extent and limits of this cohomological approach. We ask the following questions which connect it to important themes in algorithms, logic and finite model theory.

Cohomology and constraint satisfaction. Firstly, Bulatov and Zhuk's recent independent resolutions of the Feder-Vardi conjecture[8][23], show that for all domains B either $\mathbf{CSP}(B)$ is `NP-Complete` or B admits a weak near-unanimity polymorphism and $\mathbf{CSP}(B)$ is tractable. As the cohomological k-consistency algorithm expands the power of the k-consistency algorithm which features as one case of Bulatov and Zhuk's general efficient algorithms, we ask if it is sufficient to decide all tractable **CSP**s.

Question 20. *For all domains B which admit a weak near-unanimity polymorphism, does there exists a k such that for all A*

$$A \to B \iff A \to_k^{\mathbb{Z}} B?$$

Cohomology and structure isomorphism. Secondly, as cohomological k-Weisfeiler-Leman is an efficient algorithm for distinguishing some non-isomorphic relational structures we ask if it distinguishes all non-isomorphic structures. As the best known structure isomorphism algorithm is quasi-polynomial[6], we do not expect a positive answer to this question but expect that negative answers would aid our understanding of the hard cases of structure isomorphism in general.

Question 21. *For every signature σ does there exists a k such that for all σ-structures A, B*

$$A \cong B \iff A \equiv_k^{\mathbb{Z}} B?$$

Cohomology and game comonads. Thirdly, as $\to_k$ and $\equiv_k$ have been shown by Abramsky, Dawar, and Wang[3] to be correspond to the coKleisli morphisms and isomorphisms of a comonad $\mathbb{P}_k$, we ask whether a similar account can be given to $\to_k^{\mathbb{Z}}$ and $\equiv_k^{\mathbb{Z}}$. As the coalgebras of the $\mathbb{P}_k$ comonad relate to the combinatorial notion of treewidth, an answer to this question could provide a new notion of "cohomological" treewidth.

Question 22. *Does there exist a comonad $\mathbb{C}_k$ for which the notion of morphism and isomorphism in the coKleisli category are $\to_k^{\mathbb{Z}}$ and $\equiv_k^{\mathbb{Z}}$?*

The search for a logic for **`PTIME`.** Finally, as the algorithms for $\to_k^{\mathbb{Z}}$ and $\equiv_k^{\mathbb{Z}}$ are likely expressible in rank logic extended with a quantifier for solving systems of linear equations over $\mathbb{Z}$ and as $\equiv_k^{\mathbb{Z}}$ distinguishes all the best known family separating rank logic from `PTIME`, we ask if solving systems of equations over $\mathbb{Z}$ is enough to capture all `PTIME` queries.

Question 23. *Is there a logic FPC+rk+$\mathbb{Z}$ incorporating solvability of $\mathbb{Z}$-linear equations into rank logic which captures* `PTIME`*?*

References

[1] Samson Abramsky, Rui Soares Barbosa, Kohei Kishida, Raymond Lal, and Shane Mansfield. 2015. Contextuality, Cohomology and Paradox. In *24th EACSL Annual Conference on Computer Science Logic (CSL 2015) (Leibniz International Proceedings in Informatics (LIPIcs))*, Stephan Kreutzer (Ed.), Vol. 41. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 211–228. https://doi.org/10.4230/LIPIcs.CSL.2015.211

[2] Samson Abramsky and Adam Brandenburger. 2011. The sheaf-theoretic structure of non-locality and contextuality. *New Journal of Physics* 13, 11 (Nov 2011), 113036. https://doi.org/10.1088/1367-2630/13/11/113036

[3] Samson Abramsky, Anuj Dawar, and Pengming Wang. 2017. The Pebbling Comonad in Finite Model Theory. In *Proceedings of the 32nd Annual ACM/IEEE Symposium on Logic in Computer Science* (Reykjavík, Iceland) *(LICS '17)*. IEEE Press, Article 69, 12 pages.

[4] Samson Abramsky, Shane Mansfield, and Rui Soares Barbosa. 2011. The Cohomology of Non-Locality and Contextuality. In *Proceedings of 8th International Workshop on Quantum Physics and Logic (QPL 2011)*, B. Jacobs, P. Selinger, and B. Spitters (Eds.), Vol. 95. 1–14. https://doi.org/10.4204/EPTCS.95.1

[5] Albert Atserias, Andrei Bulatov, and Anuj Dawar. 2007. Affine systems of equations and counting infinitary logic. In *In ICALP'07, volume 4596 of LNCS*. 558–570.

[6] László Babai. 2016. Graph Isomorphism in Quasipolynomial Time [Extended Abstract]. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing* (Cambridge, MA, USA) *(STOC '16)*. Association for Computing Machinery, New York, NY, USA, 684–697. https://doi.org/10.1145/2897518.2897542

[7] L. Barto and M. Kozik. 2009. Constraint satisfaction problems of bounded width. *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS* (2009), 595–603. https://doi.org/10.1109/FOCS.2009.32 cited By 99.

[8] Andrei A. Bulatov. 2017. A Dichotomy Theorem for Nonuniform CSPs. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*. 319–330. https://doi.org/10.1109/FOCS.2017.37

[9] Jin-Yi Cai, Martin Fürer, and Neil Immerman. 1992. An optimal lower bound on the number of variables for graph identification. *Combinatorica* 12, 4 (Dec. 1992), 389–410. https://doi.org/10.1007/BF01305232

[10] Anuj Dawar, Erich Grädel, and Wied Pakusa. 2019. Approximations of Isomorphism and Logics with Linear-Algebraic Operators. In *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019) (Leibniz International Proceedings in Informatics (LIPIcs))*, Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi (Eds.), Vol. 132. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 112:1–112:14. https://doi.org/10.4230/LIPIcs.ICALP.2019.112

[11] Anuj Dawar, Erich Grädel, and Moritz Lichter. 2021. Limitations of the Invertible-Map Equivalences. arXiv:2109.07218 [cs.LO]

[12] Anuj Dawar and Bjarki Holm. 2012. Pebble Games with Algebraic Rules. In *Automata, Languages, and Programming*, Artur Czumaj, Kurt Mehlhorn, Andrew Pitts, and Roger Wattenhofer (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 251–262.

[13] Tomás Feder and Moshe Y. Vardi. 1998. The Computational Structure of Monotone Monadic SNP and Constraint Satisfaction: A Study through Datalog and Group Theory. *SIAM J. Comput.* 28, 1 (1998), 57–104. https://doi.org/10.1137/S0097539794266766 arXiv:https://doi.org/10.1137/S0097539794266766

[14] Jörg Flum and Martin Grohe. 2000. On Fixed-Point Logic with Counting. *The Journal of Symbolic Logic* 65, 2 (2000), 777–787. http://www.jstor.org/stable/2586569

[15] Martin Grohe and Pascal Schweitzer. 2020. The Graph Isomorphism Problem. *Commun. ACM* 63, 11 (oct 2020), 128–134. https://doi.org/10.1145/3372123

[16] Yuri Gurevich. 1988. Logic and the Challenge of Computer Science.

[17] Lauri Hella. 1996. Logical Hierarchies in PTIME. *Information and Computation* 129, 1 (1996), 1–19. https://doi.org/10.1006/inco.1996.0070

[18] Neil Immerman and Eric S. Lander. 1990. Describing Graphs: A First-Order Approach to Graph Canonization.

[19] Ravindran Kannan and Achim Bachem. 1979. Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix. *SIAM J. Comput.* 8, 4 (11 1979), 499–9. https://ezp.lib.cam.ac.uk/login?url=https://www.proquest.com/scholarly-journals/polynomial-algorithms-computing-smith-hermite/docview/918468506/se-2?accountid=9851 Copyright - Copyright] © 1979 © Society for Industrial and Applied Mathematics; Last updated - 2021-09-11.

[20] P.G. Kolaitis and M.Y. Vardi. 1995. On the Expressive Power of Datalog: Tools and a Case Study. *J. Comput. System Sci.* 51, 1 (1995), 110–134. https://doi.org/10.1006/jcss.1995.1055

[21] Moritz Lichter. 2021. Separating Rank Logic from Polynomial Time. In *36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021, Rome, Italy, June 29 - July 2, 2021*. IEEE, 1–13. https://doi.org/10.1109/LICS52264.2021.9470598

[22] Wied Pakusa. 2016. *Linear Equation Systems and the Search for a Logical Characterisation of Polynomial Time*. Ph.D. Dissertation. RWTH Aachen University. https://logic.rwth-aachen.de/~pakusa/diss.pdf

[23] Dmitriy Zhuk. 2020. A Proof of the CSP Dichotomy Conjecture. *J. ACM* 67, 5, Article 30 (aug 2020), 78 pages. https://doi.org/10.1145/3402029