Choiceless Polynomial Time on structures with small Abelian colour classes

F. Abu Zaid, E. Grädel, M. Grohe, and W. Pakusa

RWTH Aachen University, Germany
{abuzaid,graedel,pakusa}@logic.rwth-aachen.de,
grohe@informatik.rwth-aachen.de

Abstract. Choiceless Polynomial Time (CPT) is one of the candidates in the quest for a logic for polynomial time. It is a strict extension of fixed-point logic with counting (FPC) but to date it is unknown whether it expresses all polynomial-time properties of finite structures. We study the CPT-definability of the isomorphism problem for relational structures of bounded colour class size q (for short, *q-bounded structures*). Our main result gives a positive answer, and even CPT-definable canonisation procedures, for classes of q-bounded structures with small Abelian groups on the colour classes. Such classes of q-bounded structures with *Abelian colours* naturally arise in many contexts. For instance, 2-bounded structures have Abelian colours which shows that CPT captures PTIME on 2-bounded structures. In particular, this shows that the isomorphism problem of multipedes is definable in CPT, an open question posed by Blass, Gurevich, and Shelah.

1 Introduction

The quest for a logical characterisation of PTIME remains an important challenge in the field of finite model theory [10, 12]. A natural logic of reference is fixed-point logic with counting (FPC) which comes rather close to capturing PTIME. It can express many fundamental graph properties and algorithmic techniques including for instance by a recent result of Anderson, Dawar and Holm, the ellipsoid method for linear programs [1]. Moreover, FPC captures PTIME on many important classes of graphs such as planar graphs and graphs of bounded tree-width, and more generally, on *every* class of graphs which excludes a fixed graph as a minor [13]. More specifically, the aforementioned classes even admit FPC-*definable canonisation* which means that FPC can define, given an input graph, an isomorphic copy of that graph over a linearly ordered universe. Clearly, if a class of structures admits FPC-definable canonisations, then FPC captures PTIME on this class, since by the Immerman-Vardi Theorem (see e.g. [10]) fixed-point logic can define every polynomial-time query on ordered structures. The technique of *definable canonisation* will also play a crucial role in this paper.

On the other hand, FPC fails to capture PTIME in general, which was shown by the CFI-construction of Cai, Fürer and Immerman [6]. Given our current knowledge, the two main sources of "hard" problems for FPC are tractable

cases of the graph isomorphism problem and queries from the field of linear algebra. First of all, the CFI-construction shows that FPC cannot define the graph isomorphism problem on graphs with bounded degree and with bounded colour class size. Recall that a graph of *colour class size* q is a graph coloured by an ordered set, say natural numbers, where at most q vertices get the same colour. On the other hand, the graph isomorphism problem is tractable on graphs with bounded degree or bounded colour class size [3, 11, 16]. Secondly, Atserias, Bulatov and Dawar [2] proved that FPC cannot express the solvability of linear equation systems over finite Abelian groups. Interestingly, also the CFI-query can be formulated using a linear equation system over $\mathbb{Z}_2$ [7].

This observation motivated Dawar, Holm, Grohe and Laubner [7] to introduce an extension of FPC by operators which compute the rank of definable matrices. The resulting logic, denoted as *rank logic* (FPR), is a strict extension of FPC and capable of defining the solvability of linear equation systems over finite fields and the CFI-query. Similar extensions of FPC by operators which solve linear equation systems over finite rings (and not only over finite fields) have been studied in [8]. It remains open whether one of these extensions suffices to capture PTIME and specifically, whether it can define the graph isomorphism problem on graphs of bounded degree and bounded colour class size.

In this paper we focus on *Choiceless Polynomial Time* (CPT), an extension of FPC which has been proposed by Blass, Gurevich and Shelah in [4]. Instead of extending the expressive power of FPC by operators for certain undefinable queries (such as the rank of a matrix), the basic idea of CPT is to combine the manipulation of higher order objects (hereditarily finite sets over the input structure) with a bounded amount of parallel computations. Technically, Choiceless Polynomial Time is based on BGS-machines (for Blass, Gurevich and Shelah), a computation model which directly works on relational input structures (and not on string encodings of those like Turing machines do). As a matter of fact, computations of BGS-machines have to respect symmetries of the input structure. Specifically, the set of states in a run of a BGS-program is closed under automorphisms of the input structure. More informally this means that BGS-computations are *choiceless*: it is impossible to implement statements like "pick an arbitrary element x and continue" which occur in many high-level descriptions of polynomial-time algorithms (e.g. Gaussian elimination, the Blossom algorithm for maximum matchings, and so on). On the other hand, BGS-machines are also very powerful which is due to their ability to construct and manipulate hereditarily finite sets built over the atoms of the input structure. If one imposes no further restriction on BGS-logic then *every* decidable class of structures can be defined in BGS-logic. Thus, to define CPT, the *polynomial-time* fragment of BGS-logic, one clearly has to restrict the amount of access a BGS-program has to the class of hereditarily finite sets.

Choiceless Polynomial Time is a strict extension of FPC [5]. More strikingly, Dawar, Richerby and Rossman [9] were able to show that CPT can define the CFI-query. Their very clever construction uses the power of CPT to avoid arbitrary choices by finding succinct (polynomial-time representable) encodings of

exponential-sized sets of symmetric objects. However, to date, it is not known whether CPT suffices to capture PTIME, whether it can express the graph isomorphism problem for graphs of bounded colour class size or bounded degree, and similarly, it is open whether CPT can define the solvability of linear equation systems over finite fields. As a consequence, the relation between rank logic FPR and Choiceless Polynomial Time CPT remains unclear.

This paper is motivated by the question whether for every fixed q the isomorphism problem for relational structures of colour class size q (for short, *q-bounded structures*) can be defined in CPT. Our main result gives a positive answer for classes of q-bounded structures with *Abelian colours*, i.e. q-bounded structures where all colour classes induce substructures with Abelian automorphism groups (we give the formal definition in Section 4). More generally we establish for every class of q-bounded structures with Abelian colours a CPT-definable canonisation procedure which shows that CPT captures PTIME on such classes.

Classes of q-bounded structures with Abelian colours naturally arise in many contexts. First of all, every class of 2-bounded structures has Abelian colours which in turn shows that CPT captures PTIME on 2-bounded structures. On the other hand, FPC fails to capture PTIME on this class, since the CFI-query can easily be formulated using 2-bounded structures. Moreover, this solves an open question from [5] where the authors ask whether the isomorphism problem of *multipedes* is CPT-definable (cf. *Question 24* in [5]). Since multipedes are 2-bounded structures our result shows that the isomorphism problem for multipedes is CPT-definable.

Another important example arises from generalising the CFI-query for other Abelian groups than $\mathbb{Z}_2$. In particular, in [15] Holm uses such generalisations (called *$\mathcal{C}$-structures*) to define a query which separates certain fragments of rank logics from each other. Interestingly, $\mathcal{C}$-structures are q-bounded structures with Abelian colours which means that CPT can define the queries used by Holm which separates CPT from the fragments of FPR considered in [15].

Choiceless Polynomial Time In this paper, we consider *finite* structures $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, \dots, R_k^{\mathfrak{A}})$ over *relational* signatures $\tau = \{R_1, \dots, R_k\}$. To define CPT compactly, we follow Rossman [17]. For a vocabulary τ we define $\tau^{\mathsf{HF}} = \tau \uplus \{\emptyset, \mathsf{Atoms}, \mathsf{Pair}, \mathsf{Union}, \mathsf{Unique}, \mathsf{Card}\}$ as the extension of τ by the set-theoretic function symbols $\emptyset, \mathsf{Atoms}$ (constant symbols), $\mathsf{Union}, \mathsf{Unique}, \mathsf{Card}$ (unary function symbols) and Pair (binary function symbol). For a set A we denote by $\mathsf{HF}(A)$ the class of *hereditarily finite sets* over the *atoms* A, i.e. $\mathsf{HF}(A)$ is the least set with $A \subseteq \mathsf{HF}(A)$ and $x \in \mathsf{HF}(A)$ for every $x \subseteq \mathsf{HF}(A)$. A set $x \in \mathsf{HF}(A)$ is *transitive* if for all $z \in y \in x$ we have $z \in x$. The *transitive closure* of $x \in \mathsf{HF}(A)$ is the least transitive set $\mathrm{TC}(x)$ with $x \subseteq \mathrm{TC}(x)$.

For a τ-structure $\mathfrak{A}$, its *hereditarily finite expansion* $\mathsf{HF}(\mathfrak{A})$ is the following τ^{HF}-structure over the universe $\mathsf{HF}(A)$ where relations $R \in \tau$ are interpreted as in $\mathfrak{A}$ and the set theoretic functions in $\tau^{\mathsf{HF}} \setminus \tau$ are interpreted as follows:

- $\emptyset^{\mathsf{HF}(\mathfrak{A})} = \emptyset$, $\mathsf{Atoms}^{\mathsf{HF}(\mathfrak{A})} = A$, and
- $\mathsf{Pair}^{\mathsf{HF}(\mathfrak{A})}(x, y) = \{x, y\}$, $\mathsf{Union}^{\mathsf{HF}(\mathfrak{A})}(x) = \{y \in z : z \in x\}$, and

– $\mathsf{Unique}^{\mathsf{HF}(\mathfrak{A})}(x) = \begin{cases} y, & \text{if } x = \{y\} \\ \emptyset, & \text{else,} \end{cases}$ and $\mathsf{Card}^{\mathsf{HF}(\mathfrak{A})}(x) = \begin{cases} |x|, & x \notin A \\ \emptyset, & \text{else.} \end{cases}$,
where $|x|$ is the cardinality of x encoded as a von Neumann ordinal.

A bijection $\pi : A \to A$ extends to a bijection $\pi' : \mathsf{HF}(A) \to \mathsf{HF}(A)$ in a natural way. If π is an automorphism of $\mathfrak{A}$, then π' is an automorphism of $\mathsf{HF}(\mathfrak{A})$. BGS-*logic* is evaluated over hereditarily finite expansions $\mathsf{HF}(\mathfrak{A})$ and is defined using three syntactic elements: *terms*, *formulas* and *programs*.

– *Terms* are built from *variables* and functions from τ^{HF} using the standard rules. For an input structure $\mathfrak{A}$, terms take values in $\mathsf{HF}(A)$. Additionally we allow *comprehension terms*: if $s(\bar{x}, y)$ and $t(\bar{x})$ are terms, and $\varphi(\bar{x}, y)$ is a formula then $r(\bar{x}) = \{s(\bar{x}, y) : y \in t(\bar{x}) : \varphi(\bar{x}, y)\}$ is a term (in which y is bound). The value $r^{\mathfrak{A}}(\bar{a})$ of the term $r(\bar{x})$ under an assignment $\bar{a} \subseteq \mathsf{HF}(A)$ is the set $r^{\mathfrak{A}}(\bar{a}) = \{s^{\mathfrak{A}}(\bar{a}, b) : b \in t^{\mathfrak{A}}(\bar{a}) : \mathsf{HF}(\mathfrak{A}) \models \varphi(\bar{a}, b)\} \in \mathsf{HF}(A)$.
– *Formulas* can be built from terms $t_1, t_2, \ldots, t_k$ as $t_1 = t_2$ and $R(t_1, \ldots, t_k)$ (for $R \in \tau$), and from other formulas using the Boolean connectives $\wedge, \vee, \neg$.
– *Programs* are triples $\Pi = (\Pi_{\text{step}}, \Pi_{\text{halt}}, \Pi_{\text{out}})$ where $\Pi_{\text{step}}(x)$ is a term, and $\Pi_{\text{halt}}(x)$ and $\Pi_{\text{out}}(x)$ are formulas. On an input structure $\mathfrak{A}$ a program Π induces a *run* which is the sequence $(x_i)_{i \geq 0}$ of *states* $x_i \in \mathsf{HF}(A)$ defined inductively as $x_0 = \emptyset$ and $x_{i+1} = \Pi_{\text{step}}(x_i)$. Let $\rho = \rho(\mathfrak{A}) \in \mathbb{N} \cup \{\infty\}$ be minimal such that $\mathfrak{A} \models \Pi_{\text{halt}}(x_\rho)$. The *output* $\Pi(\mathfrak{A})$ of the run of Π on $\mathfrak{A}$ is *undefined* ($\Pi(\mathfrak{A}) = \bot$) if $\rho = \infty$ and is defined as the truth value of $\mathfrak{A} \models \Pi_{\text{out}}(x_\rho)$ otherwise.

BGS-programs transform states (objects in $\mathsf{HF}(A)$) until a halting condition is reached, and produce their output from the ultimately constructed state. To obtain CPT-programs we put polynomial bounds on both, the complexity of states and the length of a run. To measure the complexity of objects in $\mathsf{HF}(A)$ we use the size of their transitive closure.

Definition 1. *A* CPT-program *is a pair $\mathcal{C} = (\Pi, p(n))$ of a* BGS-*program Π and a polynomial $p(n)$. The output $\mathcal{C}(\mathfrak{A})$ on an input structure $\mathfrak{A}$ is $\mathcal{C}(\mathfrak{A}) = \Pi(\mathfrak{A})$ if the following resource bounds are satisfied (otherwise we set $\mathcal{C}(\mathfrak{A}) = false$):*

– *the length $\rho(\mathfrak{A})$ of the run of Π on $\mathfrak{A}$ is at most $p(|A|)$ and*
– *for each state in the run $(x_i)_{i \leq \rho(\mathfrak{A})}$ of Π on $\mathfrak{A}$ it holds that $|TC(x_i)| \leq p(|A|)$.*

The main difference to fixed-point logics like FPC is that CPT can manipulate *higher-order* objects from $\mathsf{HF}(A)$ which have polynomial size. These objects can be, for example, clever data structures which succinctly encode exponential-sized sets, or just exhaustive search trees on small parts of the input. In contrast, FPC can access only (constant-sized) lists of elements.

Algebra and permutation groups For a set V, we denote by $\mathrm{Sym}(V)$ the *symmetric group* acting on V. As usual we use *cycle notation* $(v_1\, v_2\, \cdots\, v_\ell)$ to specify permutations in $\mathrm{Sym}(V)$. For a *permutation group* $\Gamma \leq \mathrm{Sym}(V)$ and

$v \in V$ we write $\Gamma(v) = \{\gamma(v) : \gamma \in \Gamma\}$ to denote the *orbit* of v under the action of Γ. The set of Γ-orbits $\{\Gamma(v) : v \in V\}$ yields a partition of V. We say that Γ acts *transitively* on V if $\Gamma(v) = V$ for some (equivalently each) $v \in V$. We read group operations from *right to left* and use the notation γ^σ as a shorthand for $\sigma\gamma\sigma^{-1}$ whenever this makes sense (hence $(\gamma^\sigma)^\tau = \gamma^{\tau\sigma}$). Likewise, we let $\sigma\Gamma = \{\sigma\gamma : \gamma \in \Gamma\}$ and $\Gamma^\sigma = \{\gamma^\sigma : \gamma \in \Gamma\}$.

For a τ-structure $\mathfrak{A}$ we let $\mathrm{Aut}(\mathfrak{A}) \leq \mathrm{Sym}(A)$ denote the *automorphism group* of $\mathfrak{A}$. In this paper, $\mathrm{Aut}(\mathfrak{A})$ will often be *Abelian*. Recall that every finite Abelian group is an inner direct sum of cyclic groups of prime power order. For a group Γ and $\gamma \in \Gamma$ we denote by $\langle\gamma\rangle$ the *cyclic* subgroup of Γ generated by γ.

We define *linear equation systems* over finite rings $\mathbb{Z}_d$ where $d = p^k$ is a prime-power. Let V be a set of variables over $\mathbb{Z}_d$. By $\mathbb{Z}_d^V$ we denote the set of (unordered) $\mathbb{Z}_d$-vectors $x : V \mapsto \mathbb{Z}_d$ with indices in V. An *atomic linear term* is of the form $z \cdot v$ for $z \in \mathbb{Z}_d, v \in V$. A *linear term* is a set of atomic linear terms. An *assignment* is a map $\alpha : V \to \mathbb{Z}_d$. The *value* $t[\alpha] \in \mathbb{Z}_d$ of an atomic linear term $t = z \cdot v$ under α is $t[\alpha] = z \cdot \alpha(v)$. The value $t[\alpha] \in \mathbb{Z}_d$ of a term t under α is $t[\alpha] = \sum_{s \in t} s[\alpha]$. A *linear equation* is a pair (t, z) where t is a linear term and $z \in \mathbb{Z}_d$. An assignment $\alpha : V \to \mathbb{Z}_d$ *satisfies* $e = (t, z)$ if $t[\alpha] = z$. A *linear equation system* is a set S of linear equations. A linear equation system S is *solvable* (or *consistent*) if an assignment $\alpha : V \to \mathbb{Z}_d$ satisfies all equations in S. For more background on (linear) algebra and permutation groups see [14].

2 Relational structures of bounded colour class size

We describe a procedure to define, given an input structure of bounded colour class size, an isomorphic copy over an ordered universe (a *canonical copy* or *canonisation*). The idea is to split the input structure into an ordered sequence of small substructures which can be canonised easily. We then combine these small canonised parts to obtain a canonisation of the full structure. To guarantee consistency, we maintain a set of isomorphisms between (the canonised part of) the input structure and its (partial) canonisation.

A *(linear) preorder* $\preceq$ of *width* $q \geq 1$ is a reflexive, transitive and total binary relation where the induced equivalence $x \sim y := (x \preceq y \text{ and } y \preceq x)$ only contains classes of size $\leq q$. A preorder $\preceq$ on A induces a linear order on the equivalence classes $A/_\sim$ and we write $A = A_1 \preceq \cdots \preceq A_n$ if A_i is the i-th equivalence class with respect to this linear order. A preorder $\preceq'$ *refines* $\preceq$ if $x \preceq' y$ implies $x \preceq y$.

Definition 2. *Let $\tau = \{R_1, \ldots, R_k\}$. A q-*bounded *τ-structure $\mathcal{H}$ is a $\tau \uplus \{\preceq\}$-structure $\mathcal{H} = (H, R_1^{\mathcal{H}}, \ldots, R_k^{\mathcal{H}}, \preceq)$ where $\preceq$ is a preorder on H of width $\leq q$. We write $H = H_1 \preceq \cdots \preceq H_n$ and denote by $q_i := |H_i| \leq q$ the size of the i-th* colour class *H_i. We set $H_i^< = \{(i, 0), \ldots, (i, q_i - 1)\}$ and write $\mathcal{O}(H_i)$ to denote the set of bijections between H_i and $H_i^<$, that is $\mathcal{O}(H_i) = \{\pi : H_i \to H_i^< , \pi \text{ is a bijection}\}$.*

For a class of q-bounded structures we always assume a *fixed* vocabulary τ. Thus the arity of all relations is bounded by a constant, say by r. Let $\mathcal{P} = \mathcal{P}(n, r)$ denote the set of non-empty subsets $I \subseteq \{1, \ldots, n\}$ of size $\leq r$. We can

define $\mathcal{P}$ together with a linear order in CPT (as r is fixed). For $I \in \mathcal{P}$ we set $H_I = \biguplus_{i\in I} H_i$ and denote by $\mathcal{H}_I \subseteq \mathcal{H}$ the substructure of $\mathcal{H}$ *induced* on H_I. Since r bounds the arity of relations in τ we have $\mathcal{H} = \bigcup_{I\in\mathcal{P}} \mathcal{H}_I$.

We set $\mathcal{O}(H) = \mathcal{O}(H_1) \times \cdots \times \mathcal{O}(H_n)$ and $\mathcal{O}(H_I) = \mathcal{O}(H_{i_1}) \times \cdots \times \mathcal{O}(H_{i_\ell})$ for $I = \{i_1, \ldots, i_\ell\} \in \mathcal{P}$. Given $C \subseteq \mathcal{O}(H_I)$ the *extension* of C to $\mathcal{O}(H)$ is the set $\mathrm{ext}(C) = \{(\sigma_1, \ldots, \sigma_n) \in \mathcal{O}(H) : (\sigma_{i_1}, \ldots, \sigma_{i_\ell}) \in C\}$.

Every $\sigma \in \mathcal{O}(H)$ defines a bijection between H and the *ordered* set $H^< = \{(i, j) : 1 \le i \le n, 0 \le j < q_i\}$. The preorder $\preceq$ on H translates to the preorder $\sigma(\preceq)$ on $H^<$ which is defined as $(i, j)\sigma(\preceq)(i', j')$ if, and only if, $i \le i'$. Specifically, $\sigma \in \mathcal{O}(H)$ defines an isomorphism between the input structure $\mathcal{H}$ and the structure $\sigma(\mathcal{H}) = (H^<, \sigma(R_1^{\mathcal{H}}), \ldots, \sigma(R_k^{\mathcal{H}}), \sigma(\preceq))$. Of course we can apply $\sigma \in \mathcal{O}(H)$ also to substructures of $\mathcal{H}$. In particular for $I \in \mathcal{P}$, every $\sigma \in \mathcal{O}(H_I)$ defines an isomorphism between $\mathcal{H}_I$ and $\sigma(\mathcal{H}_I) = (H_I^<, \sigma(R_1^{\mathcal{H}_I}), \ldots, \sigma(R_k^{\mathcal{H}_I}), \sigma(\preceq^{\mathcal{H}_I}))$ where $H_I^< = \{(i, j) \in H^< : i \in I\}$. We want to construct, given $\mathcal{H}$, an isomorphic copy $\sigma(\mathcal{H})$ which we call the *canonisation* or the *canonical copy* of $\mathcal{H}$.

In general, for different $\sigma, \tau \in \mathcal{O}(H)$ we have $\sigma(\mathcal{H}) \neq \tau(\mathcal{H})$. Since the structures $\sigma(\mathcal{H})$ and $\tau(\mathcal{H})$ are defined over an ordered universe we can distinguish them in CPT. Moreover, $\sigma(\mathcal{H}) = \tau(\mathcal{H})$ holds if, and only if, $\tau^{-1}\sigma \in \mathrm{Aut}(\mathcal{H})$.

Lemma 3. $\{\tau : \tau(\mathcal{H}) = \sigma(\mathcal{H})\} = \sigma Aut(\mathcal{H}) = Aut(\sigma(\mathcal{H}))\sigma$ *for* $\sigma \in \mathcal{O}(H)$.

Let $I_1 < I_2 < \cdots < I_m$ be the enumeration of $\mathcal{P}$ according to the definable order. We denote by $\mathcal{H}[1 \cdots s] \subseteq \mathcal{H}$ the (not necessarily induced) substructure of $\mathcal{H}$ that consists of the first s components, i.e. $\mathcal{H}[1 \cdots s] = \mathcal{H}_{I_1} \cup \cdots \cup \mathcal{H}_{I_s}$.

Definition 4. *An* s-canonisation *is a canonisation of* $\mathcal{H}[1 \cdots s]$*, i.e. a structure* $\sigma(\mathcal{H}[1 \cdots s]) = \sigma(\mathcal{H}_{I_1}) \cup \cdots \cup \sigma(\mathcal{H}_{I_s})$ *for* $\sigma \in \mathcal{O}(H)$*. A non-empty set* $C \subseteq \mathcal{O}(H)$ witnesses *an* s*-canonisation if* $\tau(\mathcal{H}_{I_j}) = \sigma(\mathcal{H}_{I_j})$ *for all* $\sigma, \tau \in C$ *and* $j = 1, \ldots, s$.

Since $\mathcal{H} = \bigcup_{I\in\mathcal{P}} \mathcal{H}_I$, an m-canonisation of $\mathcal{H}$ also is a canonisation of $\mathcal{H}$. To describe our generic CPT-canonisation procedure for q-bounded structures, we assume that we have already preselected for each colour class H_i a set of linear orderings $\sigma_i\Gamma_i \subseteq \mathcal{O}(H_i)$ where $\Gamma_i \le \mathrm{Sym}(H_i)$ and $\sigma_i \in \mathcal{O}(H_i)$. The group $\Gamma = \Gamma_1 \times \cdots \times \Gamma_n$ acts on $\mathcal{O}(H)$ in the obvious way and for $\sigma = (\sigma_1, \ldots, \sigma_n) \in \mathcal{O}(H)$ we have $\sigma\Gamma = \tau\Gamma$ for every $\tau \in \sigma\Gamma$. For an index set $I = \{i_1, \ldots, i_\ell\} \in \mathcal{P}$ we write Γ_I to denote the group $\Gamma_I = \Gamma_{i_1} \times \cdots \times \Gamma_{i_\ell}$ and $(\sigma\Gamma)_I$ to denote the set $(\sigma\Gamma)_I = \sigma_{i_1}\Gamma_{i_1} \times \cdots \times \sigma_{i_\ell}\Gamma_{i_\ell} \subseteq \mathcal{O}(H_I)$. The *extension* of a set of partial orderings $C \subseteq (\sigma\Gamma)_I$ to $\sigma\Gamma$ is the set $\mathrm{ext}(C) = \{(\tau_1, \ldots, \tau_n) \in \sigma\Gamma : (\tau_{i_1}, \ldots, \tau_{i_\ell}) \in C\} \subseteq \sigma\Gamma$. The canonisation procedure for q-bounded structures is given below.

Given: q-bounded structure $\mathcal{H}$ and sets $\sigma_i\Gamma_i \subseteq \mathcal{O}(H_i)$ for $\Gamma_i \le \mathrm{Sym}(H_i)$, $\sigma_i \in \mathcal{O}(H_i)$
  $C_0 := \sigma\Gamma$ and $\mathcal{H}_0^< := \emptyset$
  for $s = 1$ **to** m **do**
    Set $I := I_s$ and define $\Delta := \mathrm{Aut}(\mathcal{H}_I) \cap \Gamma_I$ and $D := \{\tau\Delta : \tau \in (\sigma\Gamma)_I\}$
    Fix $\tau\Delta \in D$ such that $C_{s-1} \cap \mathrm{ext}(\tau\Delta) \neq \emptyset$ (possible by Lemma 3)
    Set $C_s := C_{s-1} \cap \mathrm{ext}(\tau\Delta)$ and $\mathcal{H}_s^< := \mathcal{H}_{s-1}^< \cup \tau'(\mathcal{H}_I)$ for some (all) $\tau' \in \tau\Delta$
  end for
Return: The canonisation $\mathcal{H}^< := \mathcal{H}_m^<$ of $\mathcal{H}$

To express this procedure in CPT, the difficulty is to find suitable representations for the sets C_s. Clearly, storing them explicitly is impossible as their size is exponential in the size of the input structure. In the following sections we establish suitable representations based on linear algebra. We summarise the requirements for such representations in the following definition.

Definition 5. *For explicitly given sets $\sigma_i\Gamma_i \subseteq \mathcal{O}(H_i)$, a* CPT*-definable representation of sets $\tau\Delta$ with $\Delta \leq \Gamma$ and $\tau \in \sigma\Gamma$ is* suitable *if the following operations are* CPT*-definable.*

(i) Consistency. *Given a representation of $\tau\Delta$, it is* CPT*-definable whether $\tau\Delta \neq \emptyset$.*

(ii) Intersection. *Given two representations of sets $\tau_1\Delta_1$ and $\tau_2\Delta_2$, a representation of the set $\tau_1\Delta_1 \cap \tau_2\Delta_2$ is* CPT*-definable.*

(iii) Representation of basic sets. *Given $\tau\Delta$ with $\tau \in (\sigma\Gamma)_I$ and $\Delta \leq \Gamma_I$ for $I \in \mathcal{P}$, a representation of ext$(\tau\Delta) \subseteq \sigma\Gamma$ can be defined in* CPT*.*

3 Cyclic linear equation systems over finite rings

We proceed to show that the solvability of *cyclic linear equation systems* (CESs) over finite rings $\mathbb{Z}_d$, where $d = p^k$ is a prime power, can be defined in CPT. In Section 4, we will see that solution spaces of CESs can be used to represent sets of witnessing isomorphisms as required in Definition 5. Having this connection a *consistency check* corresponds to deciding the solvability of a linear equation system, the *intersection operation* corresponds to combining the equations of two linear systems, and the *representation of basic sets* corresponds to constructing a linear equation systems over a small set of variables.

Definition 6. *Let V be a set of variables over $\mathbb{Z}_d$ where d is a prime power.*

(a) A cyclic constraint *on $W \subseteq V$ is a consistent set C of linear equations with variables in W which contains for every pair $v, w \in W$ an equation of the form $v - w = z$ for $z \in \mathbb{Z}_d$.*

(b) A cyclic linear equation systems (CES) *over $\mathbb{Z}_d$ is a triple $(V, S, \preceq)$ where $\preceq$ is a preorder on $V = V_1 \preceq \cdots \preceq V_n$ and S is a linear equation system which contains for every block V_i a cyclic constraint C_i.*

In the definition we do not require that $\preceq$ is of bounded width. However, given the cyclic constraints $C_i \subseteq S$ we can assume that $|V_i| = d$ for all $1 \leq i \leq n$.

Lemma 7. *Given a CES $(V, S, \preceq)$ over $\mathbb{Z}_d$, we can define in* CPT *a CES $(V', S', \preceq')$ over $\mathbb{Z}_d$ such that $V' = V'_1 \preceq' \cdots \preceq' V'_n$ and $|V'_i| = d$ for all i, together with a bijection between the set of assignments that satisfy the two CESs.*

For $z \in \mathbb{Z}_d$ and $v \in V_i$ we denote by $v^{+z} \in V_i$ the (unique) variable such that C_i contains the constraint $v^{+z} - v = z$. There are precisely d different assignments $\alpha : V_i \to \mathbb{Z}_d$ with $\alpha \models C_i$ and each one is determined by fixing the value of a single variable $v \in V_i$. The crucial ingredient of our CPT-procedure for solving CESs over $\mathbb{Z}_d$ is the notion of a *hyperterm* which is based on the CPT-procedure of Dawar, Richerby and Rossman for expressing the CFI-query [9].

Definition 8. *Let A be the set of assignments that satisfy all cyclic constraints C_i, i.e. $A := \{\alpha : V \to \mathbb{Z}_d : \alpha \models C_i \text{ for } i = 1, \dots, n\}$. We inductively define*

(i) hyperterms T *and associated* shifted hyperterms T^{+z} *for $z \in \mathbb{Z}_d$ such that $T^{+(z_1+z_2)} = (T^{+z_1})^{+z_2}$ for $z_1, z_2 \in \mathbb{Z}_d$, and $T^{+d} = T$,*
(ii) for assignments $\alpha \in A$ the value $T[\alpha] \in \mathbb{Z}_d$ *such that $T^{+z}[\alpha] - T[\alpha] = z$,*
(iii) and the coefficient $c(V_i, T) = c(V_i, T^{+z}) \in \mathbb{Z}_d$ *of variable block V_i in the hyperterms $T, T^{+1}, \dots, T^{+(d-1)}$.*

- *For $z \in \mathbb{Z}_d$ we define the hyperterm $T = z$ and set $T^{+y} = z + y$ for $y \in \mathbb{Z}_d$. We let $c(V_i, T) = c(V_i, T^{+y}) = 0$ for each variable block V_i and all $y \in \mathbb{Z}_d$ and let $T[\alpha] = z$ and $T^{+y}[\alpha] = z + y$ for all assignments $\alpha \in A$ and $y \in \mathbb{Z}_d$. Moreover, for $v \in V_i$, $T = v$ is a hyperterm where $T^{+y} = v^{+y}$ for $y \in \mathbb{Z}_d$. We set $c(V_j, T) = c(V_j, T^{+y}) = 1$ for $y \in \mathbb{Z}_d$ if $j = i$ and $c(V_j, T) = c(V_j, T^{+y}) = 0$ otherwise. Finally, we let $T[\alpha] = \alpha(v)$. Then $T^{+y}[\alpha] = \alpha(v^{+y}) = \alpha(v) + y$.*
- *Let Q, R be hyperterms. Then $T = Q \oplus R := \{\langle Q^{+z_1}, R^{+z_2}\rangle : z_1 + z_2 = 0\}$ is a hyperterm with shifted hyperterm $T^{+y} = \{\langle Q^{+z_1}, R^{+z_2}\rangle : z_1 + z_2 = y\}$ for $y \in \mathbb{Z}_d$. We set $c(V_i, T) = c(V_i, T^{+y}) = c(V_i, Q) + c(V_i, R)$, $T[\alpha] := Q[\alpha] + R[\alpha]$ and we have $T^{+y}[\alpha] = Q[\alpha] + R[\alpha] + y$ for $\alpha \in A$.*
- *Let Q be a hyperterm, $z \in \mathbb{Z}_d$. Then a new hyperterm $T = z \odot Q := Q \oplus \cdots \oplus Q$ results by applying the $\oplus$-operation z-times to Q (where we implicitly agree on an application from left to right). The definitions of $T^{+y}, c(V_i, T)$ and $T[\alpha]$ follow from the definition of $\oplus$.*

Definition 9. *For $\alpha \in A$, $1 \le i \le n$ and $z \in \mathbb{Z}_d$ we define the assignment $\alpha^{i:+z} \in A$ which results from a* semantical z-shift *of variable block V_i which means that $\alpha^{i:+z}(v) = \alpha(v) + z$ for $v \in V_i$ and $\alpha^{i:+z}(v) = \alpha(v)$ for $v \notin V_i$. Moreover we let $\pi^{i:+z} : V_i \to V_i$ be the* syntactic z-shift *on the set V_i which is defined as $\pi^{i:+z}(v) := v^{+z}$ for $v \in V_i$ lifted to a permutation acting on $\mathsf{HF}(V)$.*

There is a tight correspondence between the syntactic structure and the intended semantics for hyperterms as expressed in the following lemma.

Lemma 10. *Let $1 \le i \le n, z \in \mathbb{Z}_d$, let T be a hyperterm and let $c = c(V_i, T) \in \mathbb{Z}_d$ be the coefficient of variable block V_i in T.*

(a) Then $\pi^{i:+z}(T) = T^{+c \cdot z}$. In particular if $c = 0$ then $\pi^{i:+z}(T) = T$.
(b) For any assignment $\alpha \in A$ we have $T[\alpha^{i:+z}] = \pi^{i:+z}(T)[\alpha]$.

Intuitively, a hyperterm is a succinct encoding of a class of linear terms that are (given the cyclic constraints) equivalent. Using the preorder $\preceq$ it is possible to define in CPT a linearly ordered partition $S = \biguplus_{i=1}^{m} S_i$ of S, corresponding hyperterms $T_1, \dots, T_m$ and constants $z_1, \dots, z_m \in \mathbb{Z}_d$ such that for every equation $(t, z) \in S_i$ and $\alpha \in A$ we have $t[\alpha] = T_i[\alpha]$ and $z = z_i$ (or the CES is inconsistent). This means that the system S^* consisting of the *ordered* set of *hyperequations* (T_i, z_i) is equivalent to the given CES. Given the linear order on S^*, we want to use Gaussian elimination in order to determine the solvability of S^*. As a simple preparation we observe that elementary transformations can be applied to systems of hyperequations.

Lemma 11. *Let S^* be a system of hyperequations, and let $(T, z), (T', z') \in S^*$. Then S^* and $(S^* \setminus \{(T, z)\}) \cup \{(T \oplus T', z + z')\}$ have the same solutions (in A).*

We assign the $m \times n$-matrix $M[S^*] : \{1, \ldots, m\} \times \{1, \ldots, n\} \to \mathbb{Z}_d$ to the system S^* of hyperequations defined as $M[S^*](i, j) := c(V_j, T_i)$. Applying elementary operations to S^* as in Lemma 11 corresponds to applying elementary row operations to $M[S^*]$. Using a slightly adapted version of Gaussian elimination ($\mathbb{Z}_d$ is a *ring*, not a *field*) it is possible to transform S^* such that $M[S^*]$ is in *Hermite normal form*. This transformation can be expressed in CPT.

We say that a hyperterm T is *atomic* if $c(V_i, T) = 0$ for every variable block V_i. By Lemma 10 this means $T[\alpha] = T[\alpha']$ for all $\alpha, \alpha' \in A$, hence, T has a constant value $c_T = T[\alpha]$ for some (all) $\alpha \in A$. By exploiting the fact that $M[S^*]$ is in Hermite normal form it can be shown that the solvability of S^* can be characterised by determining the consistency of a set of hyperequations (T, z) with *atomic* hyperterms T, which is to check whether $c_T = z$.

It remains to express the consistency of hyperequations (T, z) for atomic hyperterms T in CPT. This is easy if T is built from constants in $\mathbb{Z}_d$.

Lemma 12. *The value of a hyperterm $T' \in \mathsf{HF}(\mathbb{Z}_d)$ can be defined in* CPT.

Given an atomic hyperterm T, it remains to construct in CPT an equivalent hyperterm $T' \in \mathsf{HF}(\mathbb{Z}_d)$. To this end, we crucially make use of the strong connection between syntax and semantics of hyperterms as stated in Lemma 10.

Lemma 13. *Let $T \in \mathsf{HF}(V)$ be an atomic hyperterm. Then we can define in* CPT *an equivalent hyperterm $T' \in \mathsf{HF}(\mathbb{Z}_d)$.*

Theorem 14. *The solvability of CESs over $\mathbb{Z}_d$ can be defined in* CPT.

4 Canonising q-bounded structures with Abelian colours

We apply the CPT-procedure for solving CESs to show that q-bounded structures with *Abelian colours* can be canonised in CPT. Recall that we denote by $\mathcal{H}_i$ the substructure of $\mathcal{H}$ induced on the colour class H_i.

Definition 15. *A class $\mathcal{K}$ of q-bounded τ-structures has* Abelian colours *if $Aut(\mathcal{H}_i) \leq Sym(H_i)$ is Abelian for all $\mathcal{H} \in \mathcal{K}$ and colour classes $H_i \subseteq H$.*

Moreover, we say that $\mathcal{K}$ allows (CPT-)constructible transitive Abelian symmetries *if there are* CPT*-programs which define, given $\mathcal{H} \in \mathcal{K}$, on each colour class $H_i \subseteq H$ a* transitive Abelian *group $\Gamma_i \leq Sym(H_i)$ together with a linear order on $\{\sigma\Gamma_i : \sigma \in \mathcal{O}(H_i)\}$ and a linear order on Γ_i.*

We proceed to show that classes of q-bounded structures with Abelian colours can be reduced to classes with constructible transitive Abelian symmetries.

Theorem 16. *Let $\mathcal{K}$ be a class of q-bounded τ-structures with Abelian colours.*

There is a CPT*-program which defines, given $\mathcal{H} \in \mathcal{K}$, a refinement $\preceq_r^{\mathcal{H}}$ of the preorder $\preceq^{\mathcal{H}}$ on H such that the class $\mathcal{K}'$ of structures $\mathcal{H}' = \mathcal{H}[\preceq^{\mathcal{H}} \setminus \preceq_r^{\mathcal{H}}]$ (which result from substituting $\preceq^{\mathcal{H}}$ by its refinement $\preceq_r^{\mathcal{H}}$) allows constructible transitive Abelian symmetries.*

The translation $\mathcal{H} \in \mathcal{K} \mapsto \mathcal{H}' \in \mathcal{K}'$ only refines the preorder on H, hence a canonisation of $\mathcal{H}'$ yields a canonisation of $\mathcal{H}$. Thus, CPT-definable canonisation procedures on classes of q-bounded structures with constructible transitive Abelian symmetries provide CPT-definable canonisation procedures on classes of q-bounded structures with Abelian colours.

Fix a class $\mathcal{K}$ of q-bounded structures with constructible transitive Abelian symmetries. Let $\mathcal{H} \in \mathcal{K}$ with colour classes $H = H_1 \preceq \cdots \preceq H_n$ and let $\Gamma_i \leq \mathrm{Sym}(H_i)$ denote the associated Abelian transitive groups. To express our generic canonisation procedure from Section 2 in CPT, it suffices to find CPT-definable representations of sets $\tau\Delta$ where $\Delta \leq \Gamma$ and $\tau \in \mathcal{O}(H)$ which satisfy the requirements of Definition 5. Let us first find appropriate representations for the basic sets $\sigma\Delta \subseteq \mathcal{O}(H_i)$ with $\Delta \leq \Gamma_i$ and $\sigma \in \mathcal{O}(H_i)$ for each colour class H_i.

Lemma 17. *Given a set $B \subseteq \mathsf{HF}(H)$ with $|B| \leq q$ and an Abelian transitive group $\Gamma \leq Sym(B)$ which is the direct sum of k cyclic subgroups of prime-power order, i.e. $\Gamma = \langle \delta_1 \rangle \oplus \cdots \oplus \langle \delta_k \rangle$ for $\delta_1, \ldots, \delta_k \in \Gamma$ where $|\delta_i| = d_i$ is a prime-power, and given a set $\sigma\Gamma \subseteq \mathcal{O}(B)$ for $\sigma \in \mathcal{O}(B)$ we can define in* CPT

- *sets $W_1, \ldots, W_k \subseteq \mathsf{HF}(B)$ with $|W_i| = d_i$, an order $W_1 < W_2 < \cdots < W_k$,*
- *and if we set $L_i := \mathbb{Z}_{d_i}^{W_i}$ and let $e_i \in L_i$ denote the L_i-unit vector which is $e_i(w) = 1$ for all $w \in W_i$, then we can define in* CPT *an embedding $\varphi : \sigma\Gamma \to L_1 \times \cdots \times L_k$ which respects the action of Γ on $\sigma\Gamma$ in the following way. For all $\tau \in \sigma\Gamma$ and $\gamma = \ell_1 \cdot \delta_1 \oplus \cdots \oplus \ell_k \cdot \delta_k \in \Gamma$ we have that*

$$\varphi(\tau \circ \gamma) = \varphi(\tau) + (\ell_1 \cdot e_1, \cdots, \ell_k \cdot e_k).$$

Using the linear order on $\{\sigma\Gamma_i : \sigma \in \mathcal{O}(H_i)\}$ we fix for every colour class H_i a set $\sigma_i\Gamma_i \subseteq \mathcal{O}(H_i)$. Let $\sigma\Gamma = \sigma_1\Gamma_1 \times \cdots \times \sigma_n\Gamma_n$. Using Lemma 17 we write $\Gamma_i = \langle \delta_1^i \rangle \oplus \cdots \oplus \langle \delta_{k_i}^i \rangle$ where $|\delta_j^i| = d_j^i$ is a prime-power and define in CPT

- sets $W_1^i < W_2^i < \cdots < W_{k_i}^i$ of size $|W_j^i| = d_j^i$ and for $L_j^i := \mathbb{Z}_{d_j^i}^{W_j^i}$ embeddings

$$\varphi^i : \sigma_i\Gamma_i \to L_1^i \times \cdots \times L_{k_i}^i,$$

- such that for the L_j^i-unit vectors $e_j^i \in L_j^i$, each $\gamma = \ell_1 \cdot \delta_1^i \oplus \cdots \oplus \ell_{k_i} \cdot \delta_{k_i}^i \in \Gamma_i$ and each $\tau \in \sigma_i\Gamma_i$ it holds that $\varphi^i(\tau \circ \gamma) = \varphi^i(\tau) + (\ell_1 \cdot e_1^i, \ldots, \ell_{k_i} \cdot e_{k_i}^i)$.

We let $L = L_1^1 \times \cdots \times L_{k_1}^1 \times \cdots \times L_1^n \times \cdots \times L_{k_n}^n$ and combine the mappings φ^i to get a CPT-definable mapping $\varphi : \sigma\Gamma \to L, (\tau_1, \ldots, \tau_n) \mapsto (\varphi^1(\tau_1), \ldots, \varphi^n(\tau_n))$. Since $\Gamma = \Gamma_1 \times \cdots \times \Gamma_n = \langle \delta_1^1 \rangle \oplus \cdots \oplus \langle \delta_{k_1}^1 \rangle \times \cdots \times \langle \delta_1^n \rangle \oplus \cdots \oplus \langle \delta_{k_n}^n \rangle$ we also obtain a definable group embedding $\psi : \Gamma \to L$ as the homomorphic extension of setting $\psi(\delta_j^i) = e_j^i$. For all $\tau \in \sigma\Gamma$ and $\gamma \in \Gamma$ we have $\varphi(\tau \circ \gamma) = \varphi(\tau) + \psi(\gamma)$.

Next we analyse for $\sigma_i\Gamma_i$ the image under φ restricted to a component L_j^i, i.e. the set $(\varphi(\sigma_i\Gamma_i) \restriction L_j^i) \subseteq L_j^i$. If we denote by $E_j^i := \{\ell \cdot e_j^i : 0 \leq \ell \leq d_j^i - 1\} \subseteq L_j^i$, we get $O_j^i := (\varphi(\sigma_i\Gamma_i) \restriction L_j^i) = (\varphi(\sigma_i) \restriction L_j^i) + E_j^i$. This means that for two vectors $x, y \in O_j^i$ it holds that $x - y \in E_j^i$. This in turn implies that for all

vectors $x, y \in O^i_j$ and indices $w, w' \in W^i_j$ we have $x(w) - x(w') = y(w) - y(w')$. Hence we can define a cyclic constraint C^i_j on the set W^i_j such that O^i_j precisely corresponds to the set of assignments $\alpha : W^i_j \to \{0, \dots, d^i_j - 1\}$ with $\alpha \models C^i_j$.

Let $P := \{p_1, \dots, p_s\}$ be the set of all primes p_i such that Γ contains elements of order p_i. For $p \in P$ let $\Gamma^p_i \leq \Gamma_i$ denote the subgroup of Γ_i which consists of all elements $\gamma \in \Gamma_i$ whose order is a power of p. Then $\Gamma_i = \Gamma_i^{p_1} \oplus \dots \oplus \Gamma_i^{p_s}$. In particular we have $\psi(\Gamma_i) = \psi(\Gamma_i^{p_1}) + \dots + \psi(\Gamma_i^{p_s})$.

Similarly, for any subgroup $\Delta \leq \Gamma$ and prime $p \in P$ we let $\Delta^p \leq \Delta$ denote the subgroup of Δ which consists of elements $\delta \in \Delta$ whose order is a p-power. Then $\Delta = \Delta^{p_1} \oplus \dots \oplus \Delta^{p_s}$ and $\Delta^p \leq \Gamma^p_1 \times \Gamma^p_2 \times \dots \times \Gamma^p_n =: \Gamma^p$.

We also obtain a corresponding decomposition of L. For $p \in P$ we let $L[p] = \{(v^1_1, \dots, v^1_{k_1}, \dots, v^n_1, \dots, v^n_{k_n}) \in L : \text{if } v^i_j \neq 0 \text{ then } d^i_j \text{ is a } p\text{-power}\}$. Then $\psi(\Gamma^p) \leq L[p]$ and $L = L[p_1] \oplus \dots \oplus L[p_s]$.

For $\tau \in \mathcal{O}(H)$ and $\Delta \leq \Gamma$ we let $\varphi(\tau)^{L[p]}$ denote the projection of $\varphi(\tau) \in L$ onto the component $L[p]$. Then we have

$$\varphi(\tau\Delta) = \varphi(\tau)^{L[p_1]} + \psi(\Delta^{p_1}) \oplus \dots \oplus \varphi(\tau)^{L[p_s]} + \psi(\Delta^{p_s}) \subseteq L[p_1] \oplus \dots \oplus L[p_s].$$

To represent $\varphi(\tau\Delta)$ it thus suffices to represent each individual component $\varphi(\tau)^{L[p]} + \psi(\Delta^p) \subseteq L[p]$ as the set of solutions of a CES $\mathcal{S}_p$ over $\mathbb{Z}_d$ where d is a p-power. Using the cyclic constraints C^i_j from above, this is indeed possible. Altogether we represent a set $\tau\Delta$ with $\Delta \leq \Gamma$ and $\tau \in \sigma\Gamma$ as a sequence of CESs $(\mathcal{S}_{p_1}, \dots, \mathcal{S}_{p_s})$ where the solutions of $\mathcal{S}_p$ correspond to $\varphi(\tau)^{L[p]} + \psi(\Delta^p)$. This representation is suitable with respect to Definition 5:

(i) *Consistency.* To express whether $(\mathcal{S}_{p_1}, \dots, \mathcal{S}_{p_s})$ represents a non-empty set we check each $\mathcal{S}_p$ for consistency. This is CPT-definable by Theorem 14.

(ii) *Intersection.* Given two representations of sets $\tau_1\Delta_1$ and $\tau_2\Delta_2$ as sequences of CESs $(\mathcal{S}_{p_1}, \dots, \mathcal{S}_{p_s})$ and $(\mathcal{T}_{p_1}, \dots, \mathcal{T}_{p_s})$, we represent $\tau_1\Delta_1 \cap \tau_2\Delta_2$ by the sequence $(\mathcal{S}_{p_1} \cup \mathcal{T}_{p_1}, \dots, \mathcal{S}_{p_s} \cup \mathcal{T}_{p_s})$ where $\mathcal{S}_p \cup \mathcal{T}_p$ is the CPT-definable CES which results from combining the linear equations of $\mathcal{S}_p$ and $\mathcal{T}_p$.

(iii) *Representation of basic sets.* Given a set $\rho\Delta$ with $\rho \in (\sigma\Gamma)_I$ and $\Delta \leq \Gamma_I$ for $I \in \mathcal{P}$, we get a sequence of CESs $(\mathcal{S}_{p_1}, \dots, \mathcal{S}_{p_s})$ which represents $\mathrm{ext}(\rho\Delta)$ of $\rho\Delta$ simply by trying all possible sequences of CESs (this is definable in CPT since the set of relevant variables is bounded by a constant).

Theorem 18. CPT *captures* PTIME *on classes of q-bounded structures with constructible transitive Abelian symmetries.*

Corollary 19. CPT *captures* PTIME *on classes of q-bounded structures with Abelian colours, and specifically, on 2-bounded structures.*

5 Discussion

We showed that CPT captures PTIME on classes of q-bounded structures with Abelian colours. It remains open whether this holds for every class of q-bounded

structures. A natural way to proceed would be to allow more complex groups acting on the colour classes, for example *solvable* groups. In fact, we can modify our techniques to show that 3-bounded structures can be canonised in CPT.

Another question is whether CPT can define the solvability of linear equation systems over finite rings. A positive answer would render rank logic FPR [7] and solvability logic [8] a fragment of CPT, and otherwise, we would have a candidate for separating CPT from PTIME. It is also interesting to investigate how far our canonisation procedures for CPT can be expressed in such extensions of FPC by operators from linear algebra. For example, it is easy to see that our canonisation procedure for 2-bounded structures can be expressed in FPR.

We also want to study CPT on other classes of graphs with polynomial-time canonisation algorithms on which FPC fails to capture PTIME. Important examples are graphs of bounded degree or graphs of moderately growing treewidth.

References

1. M. Anderson, A. Dawar, and B. Holm. Maximum matching and linear programming in fixed-point logic with counting. In *LICS 2013*, pages 173–182, 2013.
2. A. Atserias, A. Bulatov, and A. Dawar. Affine systems of equations and counting infinitary logic. *Theoretical Computer Science*, 410(18):1666–1683, 2009.
3. L. Babai. Monte-Carlo algorithms in graph isomorphism testing. *Université de Montréal Technical Report, DMS*, pages 79–10, 1979.
4. A. Blass, Y. Gurevich, and S. Shelah. Choiceless polynomial time. *Annals of Pure and Applied Logic*, 100(1):141–187, 1999.
5. A. Blass, Y. Gurevich, and S. Shelah. On polynomial time computation over unordered structures. *Journal of Symbolic Logic*, 67(3):1093–1125, 2002.
6. J. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992.
7. A. Dawar, M. Grohe, B. Holm, and B. Laubner. Logics with rank operators. In *LICS 2009*, pages 113–122, 2009.
8. A. Dawar, E. Grädel, B. Holm, E. Kopczynski, and W. Pakusa. Definability of linear equation systems over groups and rings. *LMCS*, 9(4), 2013.
9. A. Dawar, D. Richerby, and B. Rossman. Choiceless polynomial time, counting and the Cai–Fürer–Immerman graphs. *Annals of Pure and Applied Logic*, 152(1–3):31 – 50, 2008.
10. E. Grädel et. al. *Finite Model Theory and Its Applications*. Springer, 2007.
11. M. Furst, J. E. Hopcroft, and E. Luks. A subexponential algorithm for trivalent graph isomorphism. Technical report, 1980.
12. M. Grohe. The quest for a logic capturing PTIME. In *LICS 2008*, pages 267–271, 2008.
13. M. Grohe. Fixed-point definability and polynomial time on graphs with excluded minors. *Journal of the ACM (JACM)*, 59(5):27, 2012.
14. M. Hall. *The theory of groups*. American Mathematical Soc., 1976.
15. B. Holm. *Descriptive complexity of linear algebra*. PhD thesis, University of Cambridge, 2010.
16. E. M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *Journal of Computer and System Sciences*, 25(1):42–65, 1982.
17. B. Rossman. Choiceless computation and symmetry. In *Fields of logic and computation*, pages 565–580. Springer, 2010.