Definability of linear equation systems over groups and rings*

Anuj Dawar[1], Erich Grädel[2], Bjarki Holm[1], Eryk Kopczynski[3], and Wied Pakusa[2]

1 University of Cambridge Computer Laboratory
{anuj.dawar,bjarki.holm}@cl.cam.ac.uk
2 Mathematical Foundations of Computer Science, RWTH Aachen University
{graedel,pakusa}@logic.rwth-aachen.de
3 Institute of Informatics, University of Warsaw
erykk@mimuw.edu.pl

Abstract

Motivated by the quest for a logic for PTIME and recent insights that the descriptive complexity of problems from linear algebra is a crucial aspect of this problem, we study the solvability of linear equation systems over finite groups and rings from the viewpoint of logical (inter-)definability. All problems that we consider are decidable in polynomial time, but not expressible in fixed-point logic with counting. They also provide natural candidates for a separation of polynomial time from rank logics, which extend fixed-point logics by operators for determining the rank of definable matrices and which are sufficient for solvability problems over fields.

Based on the structure theory of finite rings, we establish logical reductions among various solvability problems. Our results indicate that *all* solvability problems for linear equation systems that separate fixed-point logic with counting from PTIME can be reduced to solvability over commutative rings. Further, we prove closure properties for classes of queries that reduce to solvability over rings. As an application, these closure properties provide normal forms for logics extended with solvability operators.

1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, F.4.1 Math. Logic

Keywords and phrases finite model theory, logics with algebraic operators

Digital Object Identifier 10.4230/LIPIcs.CSL.2012.213

1 Introduction

The quest for a logic for PTIME [10, 13] is one of the central open problems in both finite model theory and database theory. Specifically, it asks whether there is a logic in which a class of finite structures is expressible if, and only if, membership in the class is decidable in deterministic polynomial time.

Much of the research in this area has focused on the logic FPC, the extension of inflationary fixed-point logic by counting terms. In fact, FPC has been shown to capture polynomial time on many natural classes of structures, including planar graphs and structures of bounded tree-width [12, 13, 15]. Most recently, it was shown by Grohe [14] that FPC captures

* The first and third authors were supported by EPSRC grant EP/H026835/1 and the fourth and fifth authors were supported by ESF Research Networking Programme GAMES. The fourth author was also partially supported by the Polish Ministry of Science grant N N206 567840. An extended version of this paper is available at http://arxiv.org/abs/1204.3022.

polynomial time on all classes of graphs with excluded minors, a result that generalises most of the previous partial capturing results. On the other side, already in 1992, Cai, Fürer and Immerman [6] constructed a query on a class of finite graphs that can be decided in polynomial time, but which is not definable by any sentence of FPC. But while this CFI query, as it is now called, is very elegant and has led to new insights in many different areas, it can hardly be called a natural problem in polynomial time. Therefore, it was often remarked that possibly all *natural* polynomial-time properties of finite structures could be expressed in FPC. However, this hope was eventually refuted in a strong sense by Atserias, Bulatov and Dawar [3] who proved that the very important problem of *solvability of linear equation systems* (over any fixed finite Abelian group) is not definable in FPC and that, indeed, the CFI query reduces to this problem. This motivates the systematic study of the relationship between finite model theory and linear algebra, and suggests that operators from linear algebra could be a source of new extensions to fixed-point logic, in an attempt to find a logical characterisation of PTIME. In [8], Dawar et al. pursued this direction of study by adding operators for expressing the rank of definable matrices over finite fields to first-order logic and fixed-point logic. They showed that fixed-point logic with rank operators (FPR) can define not only the solvability of linear equation systems over any finite field, but also the CFI query and essentially all other properties that were known to separate FPC from PTIME. However, although FPR is strictly more expressive than FPC and to date no examples are known to separate PTIME from FPR, it seems rather unlikely that FPR suffices to capture PTIME on the class of all finite structures.

A natural class of problems that might witness such a separation arises from linear equation systems over finite domains other than fields. Indeed, the results of Atserias, Bulatov and Dawar [3] imply that FPC fails to express the solvability of linear equation systems over any finite ring. On the other side, it is known that linear equation systems over finite rings can be solved in polynomial time [1], but it is unclear whether any notion of matrix rank is helpful for this purpose. We remark in this context that there are several non-equivalent notions of matrix rank over rings, but both the computability in polynomial time and the relationship to linear equation systems remains unclear. Thus, rather than matrix rank, the solvability of linear equation systems could be used directly as a source of operators (in the form of generalised quantifiers) for extending fixed-point logics.

Instead of introducing a host of new logics, with operators for various solvability problems, we set out here to investigate whether these problems are inter-definable. In other words, are they reducible to each other within FPC? Clearly, if they are, then any logic that generalises FPC and can define one, can also define the others. We thus study relations between solvability problems over (finite) rings, fields and Abelian groups in the context of logical many-to-one and Turing reductions, i.e., interpretations and generalised quantifiers. In this way, we show that solvability both over Abelian groups and over arbitrary (possibly non-commutative) rings reduces to solvability over commutative rings. We also show that solvability over commutative rings reduces to solvability over local rings, which are the basic building blocks of finite commutative rings. Finally, in the other direction, we show that solvability over rings endowed with a linear order and solvability over k-generated local rings, i.e. local rings for which the maximal ideal is generated by k elements, reduces to solvability over cyclic groups of prime-power order. These results indicate that *all* solvability problems for linear equation systems that separate FPC from PTIME can be reduced to solvability over commutative rings. Further, we prove closure properties for classes of queries that reduce to solvability over rings, and establish normal forms for first-order logic extended with operators for solvability over finite fields.

2 Background on logic and algebra

Throughout this paper, all structures (and in particular, all algebraic structures such as groups, rings and fields) are assumed to be finite. Furthermore, it is assumed that all groups are Abelian, unless otherwise noted.

2.1 Logic and structures

The logics we consider in this paper include *first-order logic* (FO) and *inflationary fixed-point logic* (FP) as well as their extensions by counting terms, which we denote by FOC and FPC, respectively. We also consider the extension of first-order logic with operators for deterministic transitive closure, which we denote by DTC. For details see [9, 10].

A *vocabulary* τ is a finite sequence of relation and constant symbols $(R_1, \dots, R_k, c_1, \dots, c_l)$ in which every R_i has an *arity* $r_i \geq 1$. A *τ-structure* $\mathbf{A} = (D(\mathbf{A}), R_1^{\mathbf{A}}, \dots, R_k^{\mathbf{A}}, c_1^{\mathbf{A}}, \dots, c_l^{\mathbf{A}})$ consists of a non-empty set $D(\mathbf{A})$, called the *domain* of $\mathbf{A}$, together with relations $R_i^{\mathbf{A}} \subseteq D(\mathbf{A})^{r_i}$ and constants $c_j^{\mathbf{A}} \in D(\mathbf{A})$ for each $i \leq k$ and $j \leq l$. Given a logic L and a vocabulary τ, we write $\mathrm{L}[\tau]$ to denote the set of τ-formulas of L. A τ-formula $\phi(\vec{x})$ with $|\,\vec{x}\,| = k$ defines a *k-ary query* that takes any τ-structure $\mathbf{A}$ to the set $\phi(\vec{x})^{\mathbf{A}} := \{\vec{a} \in D(\mathbf{A})^k \mid \mathbf{A} \models \phi[\vec{a}]\}$.

Lindström quantifiers and extensions. Let $\sigma = (R_1, \dots, R_k)$ be a vocabulary and consider a class $\mathcal{K}$ of σ-structures that is closed under isomorphism. With $\mathcal{K}$ we associate a *Lindström quantifier* $Q_{\mathcal{K}}$ whose *type* is the tuple $(r_1, \dots, r_k)$. For a logic L, we define the extension $\mathrm{L}(Q_{\mathcal{K}})$ by adding rules for constructing formulas of the kind $Q_{\mathcal{K}}\vec{x}_1 \dots \vec{x}_k \,.\, (\phi_1, \dots, \phi_k)$, where $\phi_1, \dots, \phi_k$ are formulas and each $\vec{x}_i$ has length r_i. The semantics of the quantifier $Q_{\mathcal{K}}$ is defined such that $\mathbf{A} \models Q_{\mathcal{K}}\vec{x}_1 \dots \vec{x}_k \,.\, (\phi_1, \dots, \phi_k)$ if $(D(\mathbf{A}), \phi_1(\vec{x}_1)^{\mathbf{A}}, \dots, \phi_k(\vec{x}_k)^{\mathbf{A}}) \in \mathcal{K}$ as a σ-structure (see [18, 20]). Similarly we can consider the extension of L by a collection $\mathbf{Q}$ of Lindström quantifiers. The logic $\mathrm{L}(\mathbf{Q})$ is defined by adding a rule for constructing formulas with Q, for each $Q \in \mathbf{Q}$, and the semantics is defined by considering the semantics for each quantifier $Q \in \mathbf{Q}$, as above. For $m \geq 1$, we write $\mathcal{K}_m$ to denote the m-ary vectorisation of $\mathcal{K}$. If Q_m is the Lindström quantifier associated with $\mathcal{K}_m$ then we write $\langle Q_{\mathcal{K}} \rangle := \{Q_m \mid m \in \mathbb{N}\}$ to denote the *vectorised sequence* of Lindström quantifiers associated with $\mathcal{K}$ (see [7]).

Interpretations and logical reductions. Consider signatures σ and τ and a logic L. An *m-ary* L*-interpretation of τ in σ* is a sequence of formulas of L in vocabulary σ consisting of: (i) a formula $\delta(\vec{x})$; (ii) a formula $\varepsilon(\vec{x}, \vec{y})$; (iii) for each relation symbol $R \in \tau$ of arity k, a formula $\phi_R(\vec{x}_1, \dots, \vec{x}_k)$; and (iv) for each constant symbol $c \in \tau$, a formula $\gamma_c(\vec{x})$, where each $\vec{x}$, $\vec{y}$ or $\vec{x}_i$ is an m-tuple of free variables. We call m the *width* of the interpretation. We say that an interpretation $\mathcal{I}$ associates a τ-structure $\mathcal{I}(\mathbf{A}) = \mathbf{B}$ to a σ-structure $\mathbf{A}$ if there is a surjective map h from the m-tuples $\delta(\vec{x}) = \{\vec{a} \in D(\mathbf{A})^m \mid \mathbf{A} \models \delta[\vec{a}]\}$ to $\mathbf{B}$ such that:

- $h(\vec{a}_1) = h(\vec{a}_2)$ if, and only if, $\mathbf{A} \models \varepsilon[\vec{a}_1, \vec{a}_2]$;
- $R^{\mathbf{B}}(h(\vec{a}_1), \dots, h(\vec{a}_k))$ if, and only if, $\mathbf{A} \models \phi_R[\vec{a}_1, \dots, \vec{a}_k]$; and
- $h(\vec{a}) = c^{\mathbf{B}}$ if, and only if, $\mathbf{A} \models \gamma_c[\vec{a}]$.

▶ **Definition 1** (Logical reductions). Let $\mathcal{C}$ be a class of σ-structures and $\mathcal{D}$ a class of τ-structures closed under isomorphism.

- $\mathcal{C}$ is said to be L-*many-to-one reducible* to $\mathcal{D}$ ($\mathcal{C} \leq_{\mathrm{L}} \mathcal{D}$) if there is an L-interpretation $\mathcal{I}$ of τ in σ such that for every σ-structure $\mathbf{A}$ it holds that $\mathbf{A} \in \mathcal{C}$ if, and only if, $\mathcal{I}(\mathbf{A}) \in \mathcal{D}$.
- $\mathcal{C}$ is said to be L-*Turing reducible* to $\mathcal{D}$ ($\mathcal{C} \leq_{\text{L-T}} \mathcal{D}$) if $\mathcal{C}$ is definable in $\mathrm{L}(\langle Q_{\mathcal{D}} \rangle)$. ■

2.2 Rings and systems of linear equations

We recall some definitions from commutative and linear algebra, assuming that the reader has knowledge of basic algebra and group theory (for further details see Atiyah et al. [2]). For $m \geq 2$, we write $\mathbb{Z}_m$ to denote the ring of integers modulo m.

Commutative rings. Let $(R, \cdot, +, 1, 0)$ be a commutative ring. An element $x \in R$ is a *unit* if $xy = yx = 1$ for some $y \in R$ and we denote by $R^\times$ the set of all units. Moreover, we say that y *divides* x (written $y \mid x$) if $x = yz$ for some $z \in R$. An element $x \in R$ is *nilpotent* if $x^n = 0$ for some $n \in \mathbb{N}$, and we call the least such $n \in \mathbb{N}$ the *nilpotency* of x. The element $x \in R$ is *idempotent* if $x^2 = x$. Clearly $0, 1 \in R$ are idempotent elements, and we say that an idempotent x is *non-trivial* if $x \notin \{0, 1\}$. Two elements $x, y \in R$ are *orthogonal* if $xy = 0$.

We say that R is a *principal ideal ring* if every ideal of R is generated by a single element. An ideal $m \subseteq R$ is called *maximal* if $m \neq R$ and there is no ideal $m' \subsetneq R$ with $m \subsetneq m'$. A commutative ring R is *local* if it contains a unique maximal ideal m. We often consider *chain rings* that are both local and principal. For example, all prime rings $\mathbb{Z}_{p^n}$ are chain rings and so too are all finite fields. More generally, a *k-generated local ring* is a local ring for which the maximal ideal is generated by k elements. See McDonald [19] for further background.

▶ Remark. When we speak of a "commutative ring with a linear order", then in general the ordering does not respect the ring operations (cf. the notion of ordered rings from algebra).

Systems of linear equations. We consider systems of linear equations over groups and rings whose equations and variables are indexed by arbitrary sets, not necessarily ordered. In the following, if I, J and X are finite and non-empty sets then an $I \times J$ *matrix* over X is a function $A : I \times J \to X$. An I*-vector* over X is defined similarly as a function $\mathbf{b} : I \to X$.

A system of linear equations over a group G is a pair $(A, \mathbf{b})$ with $A\colon I \times J \to \{0, 1\}$ and $\mathbf{b}\colon I \to G$. By viewing G as a $\mathbb{Z}$-module (i.e. by defining the natural multiplication between integers and group elements respecting $1 \cdot g = g$, $(n+1) \cdot g = n \cdot g + g$, and $(n-1) \cdot g = n \cdot g - g$), we write $(A, \mathbf{b})$ as a matrix equation $A \cdot \mathbf{x} = \mathbf{b}$, where $\mathbf{x}$ is a J-vector of variables that range over G. The system $(A, \mathbf{b})$ is said to be *solvable* if there exists a solution vector $\mathbf{c}\colon J \to G$ such that $A \cdot \mathbf{c} = \mathbf{b}$, where we define multiplication of unordered matrices and vectors in the usual way by $(A \cdot \mathbf{c})(i) = \sum_{j \in J} A(i, j) \cdot \mathbf{c}(j)$ for all $i \in I$. We represent linear equation systems over groups as finite structures over the vocabulary $\tau_{\text{les-g}} := \{G, A, b\} \cup \tau_{\text{group}}$, where $\tau_{\text{group}} := \{+, e\}$ denotes the language of groups, G is a unary relation symbol (identifying the elements of the group) and A, b are two binary relation symbols.

Similarly, a system of linear equations over a commutative ring R is a pair $(A, \mathbf{b})$ where A is an $I \times J$ matrix with entries in R and $\mathbf{b}$ is an I-vector over R. As before, we usually write $(A, \mathbf{b})$ as a matrix equation $A \cdot \mathbf{x} = \mathbf{b}$ and say that $(A, \mathbf{b})$ is solvable if there is a solution vector $\mathbf{c} : J \to R$ such that $A \cdot \mathbf{c} = \mathbf{b}$. In the case that the ring R is not commutative, we represent linear systems in the form $A_l \cdot \mathbf{x} + \mathbf{x} \cdot A_r = \mathbf{b}$.

We consider three different ways to represent linear systems over rings as relational structures. For simplicity, we restrict to commutative rings here. Firstly, we consider the case where the ring is part of the structure. Let $\tau_{\text{les-r}} := \{R, A, b\} \cup \tau_{\text{ring}}$, where $\tau_{\text{ring}} = \{+, \cdot, 1, 0\}$ is the language of rings, R is a unary relation symbol (identifying the ring elements), and A and b are ternary and binary relation symbols, respectively. Then a finite $\tau_{\text{les-r}}$-structure $\mathbf{S}$ describes the linear equation system $(A^{\mathbf{S}}, \mathbf{b}^{\mathbf{S}})$ over the ring $\mathbf{R}^{\mathbf{S}} = (R^{\mathbf{S}}, +^{\mathbf{S}}, \cdot^{\mathbf{S}})$. Secondly, we consider a similar encoding but with the additional assumption that the elements of the ring (and not the equations or variables of the equation systems) are linearly ordered. Such systems can be seen as finite structures over the vocabulary $\tau_{\text{les-r}}^{\leqslant} := \tau_{\text{les-r}} \cup \{\leqslant\}$. Finally, we consider linear equation systems over a fixed ring encoded in the vocabulary: for every ring R, we define the vocabulary $\tau_{\text{les}}(R) := \{A_r, b_r \mid r \in R\}$, where for each $r \in R$ the symbols A_r and b_r are binary and unary, respectively. A finite $\tau_{\text{les}}(R)$-structure $\mathbf{S}$ describes the linear equation system $(A, \mathbf{b})$ over R where $A(i,j) = r$ if, and only if, $(i,j) \in A_r^{\mathbf{S}}$ and similarly for $\mathbf{b}$ (assuming that the $A_r^{\mathbf{S}}$ form a partition of $I \times J$ and that the $b_r^{\mathbf{S}}$ form a partition of I).

Finally, we frequently say that two linear equation systems $\mathbf{S}$ and $\mathbf{S}'$ over a common domain X are *equivalent* if either both systems are solvable over X or neither system is solvable over X.

3 Solvability problems over different algebraic domains

It follows from the work of Atserias, Bulatov and Dawar [3] that FPC cannot express solvability of linear equation systems ('solvability problems') over any class of (finite) groups or rings. In this section we study solvability problems over such different algebraic domains in terms of logical reductions. Our main result here is to show that the solvability problem over groups (SlvAG) DTC-reduces to the corresponding problem over commutative rings (SlvCR) and that solvability over commutative rings equipped with a linear ordering (SlvCR$_{\leqslant}$) FP-reduces to solvability over cyclic groups (SlvCycG). Note that over any non-Abelian group, the solvability problem is NP-complete [11].

Our methods can be further adapted to show that solvability over arbitrary (not necessarily commutative) rings (SlvR) DTC-reduces to SlvCR. We then consider solvability restricted to special classes of commutative rings: local rings (SlvLR) and k-generated local rings (SlvLR$_k$), which generalises solvability over finite fields (SlvF). The reductions that we establish are illustrated in Figure 1.

$$\begin{tikzcd}
\textsc{SlvCycG} \arrow[r, hook] & \textsc{SlvAG} \arrow[d, "\text{DTC}"] & \\
\textsc{SlvCR}_{\leqslant} \arrow[u, "\text{FP}"] \arrow[r, hook] & \textsc{SlvCR} \arrow[dr, "\text{FO-T}"'] & \textsc{SlvR} \arrow[l, "\text{DTC}"'] \\
\textsc{SlvLR}_k \arrow[u, "\text{FP-T}"] & \textsc{SlvF} \arrow[l, hook'] & \textsc{SlvLR} \arrow[ul, hook, bend right]
\end{tikzcd}$$

Figure 1 Logical reductions between solvability problems. Curved arrows ($\hookrightarrow$) denote inclusion of one class in another.

In the remainder of this section we describe three of the outlined reductions: from commutative rings equipped with a linear order to cyclic groups, from groups to commutative rings, and finally from general rings to commutative rings. To give the reductions from commutative rings to local rings and from k-generated local rings to commutative linearly ordered rings we need to delve further into the theory of finite commutative rings, which is the subject of §4.

▶ **Theorem 2.** SlvCR$_{\leqslant}$ $\leq_{\text{FP}}$ SlvCycG.

Proof. Consider a system of linear equations $(A, \mathbf{b})$ over a commutative ring R of characteristic m and let $\leqslant$ be a linear order on R. In the following we describe a mapping that translates the system $(A, \mathbf{b})$ into a system of equations $(A^\star, \mathbf{b}^\star)$ over the cyclic group $\mathbb{Z}_m$ which is solvable if, and only if, $(A, \mathbf{b})$ has a solution over R.

Let $\{g_1, \ldots, g_k\} \subseteq R$ be a (minimal) generating set for the additive group $(R, +)$ and let ℓ_i denote the order of g_i. We consider the group generated by g_i as a subgroup of $\mathbb{Z}_m$, i.e. $\langle g_i \rangle = \mathbb{Z}_{\ell_i} \cong (m/\ell_i)\,\mathbb{Z}_m \leq \mathbb{Z}_m$. Then $(R, +) \cong \bigoplus_i (m/\ell_i)\,\mathbb{Z}_m$ and we obtain a unique representation for each element $r \in R$ as $r = (r_1, \ldots, r_k)$ where $r_i \in (m/\ell_i)\,\mathbb{Z}_m$. Similarly, we identify variables x ranging over R with tuples $x = (x_1, \ldots, x_k)$ where x_i ranges over $(m/\ell_i)\,\mathbb{Z}_m$. Note that, in general, subgroups $(m/\ell)\,\mathbb{Z}_m$ are definable in linear systems over $\mathbb{Z}_m$: the equation $\ell \cdot x = 0$ ensures that the variable x takes values in $(m/\ell)\,\mathbb{Z}_m$.

To translate linear equations over R into equivalent equations over $\mathbb{Z}_m$, we consider the multiplication of a coefficient $r \in R$ with a variable x with respect to the chosen representation, i.e. the formal expression $r \cdot x = (r_1, \ldots, r_k) \cdot (x_1, \ldots, x_k)$. If we write all products $g_i \cdot g_j$ of pairs of generators as elements in $\bigoplus_i (m/\ell_i)\,\mathbb{Z}_m$, then the product $r \cdot x$ is uniquely determined as a k-tuple of the form $(\sum_i b^1_{i,r} \cdot x_i, \ldots, \sum_i b^k_{i,r} \cdot x_i)$, where for every $\ell \leq k$ the coefficients $b^\ell_{1,r}, \ldots, b^\ell_{k,r}$ only depend on $r = (r_1, \ldots, r_k)$ and ℓ, and where x_i ranges over $(m/\ell_i)\,\mathbb{Z}_m$. Furthermore, the decomposition $\bigoplus_i (m/\ell_i)\,\mathbb{Z}_m$ allows us to handle addition component-wise. Hence, altogether we can translate each linear equation of the original system $(A, \mathbf{b})$ into k equations over $\mathbb{Z}_m$ and obtain a system of linear equations $(A^\star, \mathbf{b}^\star)$ over $\mathbb{Z}_m$ which is solvable if, and only if, the original system $(A, \mathbf{b})$ has a solution over R.

We proceed to show that the mapping $(A, \mathbf{b}) \mapsto (A^\star, \mathbf{b}^\star)$ can be expressed in FP. Here, we crucially rely on the given order on R to fix a set of generators. More specifically, as we can compute a set of generators in time polynomial in $|\,R\,|$, it follows from the Immerman-Vardi theorem [17, 22] that there is an FP-formula $\phi(x)$ such that $\phi(x)^R = \{g_1, \ldots, g_k\}$ generates $(R, +)$ and $g_1 \leqslant \cdots \leqslant g_k$. Having fixed a set of generators, it is obvious that the map $\iota : R \to (m/\ell_1)\,\mathbb{Z}_m \times \cdots \times (m/\ell_k)\,\mathbb{Z}_m$ taking $r \mapsto (r_1, \ldots, r_k)$, is FP-definable. Furthermore, the map $(l, i, r) \mapsto b^l_{i,r}$ can easily be formalised in FP, since we have $b^l_{i,r} = \sum_{j=1}^k r_j \cdot c^{ij}_l$ where c^{ij}_l is the coefficient of g_l in the expression $g_i \cdot g_j = \sum_{y=1}^k c^{ij}_y \cdot g_y$. Splitting the original system of equations component-wise into k systems of linear equations and combining them again to a single system over $\mathbb{Z}_m$ is trivial.

Finally, we note that a linear system over the *ring* $\mathbb{Z}_m$ can be reduced to an equivalent system over the *group* $\mathbb{Z}_m$, by rewriting terms ax with $a \in \mathbb{Z}_m$ as $x + x + \cdots + x$ (a-times). ◀

So far, we have shown that solvability problems over linearly ordered commutative rings can be reduced to solvability problems over basic groups. This raises the question whether a translation in the other direction is also possible; that is, whether we can reduce solvability over groups to solvability over commutative rings. Essentially, such a reduction requires an interpretation of a commutative ring in a group, which is what we describe in the proof of the following theorem.

▶ **Theorem 3.** SLVAG $\leq_{\mathrm{DTC}}$ SLVCR.

Proof. Let $(A, \mathbf{b})$ be a system of linear equations over a group $(G, +_G, e)$, where $A \in \{0,1\}^{I \times J}$ and $\mathbf{b} \in G^I$. For the reduction, we first construct a commutative ring $\phi(G)$ from G and then lift $(A, \mathbf{b})$ to a system of equations $(A^\star, \mathbf{b}^\star)$ which is solvable over $\phi(G)$ if, and only if, $(A, \mathbf{b})$ is solvable over G.

We consider G as a $\mathbb{Z}$-module in the usual way and write $\cdot_\mathbb{Z}$ for multiplication of group elements by integers. Let d be the least common multiple of the order of all group elements. Then we have $\mathrm{ord}_G(g) \mid d$ for all $g \in G$, where $\mathrm{ord}_G(g)$ denotes the order of g. This allows us to obtain from $\cdot_\mathbb{Z}$ a well-defined multiplication of G by elements of $\mathbb{Z}_d = \{[0]_d, \ldots, [d-1]_d\}$ which commutes with group addition. We write $+_d$ and $\cdot_d$ for addition and multiplication in $\mathbb{Z}_d$, where $[0]_d$ and $[1]_d$ denote the additive and multiplicative identities, respectively. We now consider the set $G \times \mathbb{Z}_d$ as a group, with component-wise addition defined by $(g_1, m_1) + (g_2, m_2) := (g_1 +_G g_2, m_1 +_d m_2)$, for all $(g_1, m_1), (g_2, m_2) \in G \times \mathbb{Z}_d$, and identity element $0 = (e, [0]_d)$. We endow $G \times \mathbb{Z}_d$ with a multiplication $\bullet$ which is defined as $(g_1, m_1) \bullet (g_2, m_2) := \big((g_1 \cdot_\mathbb{Z} m_2 +_G g_2 \cdot_\mathbb{Z} m_1), (m_1 \cdot_d m_2)\big)$.

It is easily verified that this multiplication is associative, commutative and distributive over $+$. It follows that $\phi(G) := (G \times \mathbb{Z}_d, +, \bullet, 1, 0)$ is a commutative ring, with identity $1 = (e, [1]_d)$. For $g \in G$ and $z \in \mathbb{Z}$ we set $\overline{g} := (g, [0]_d) \in \phi(G)$ and $\overline{z} := (e, [z]_d) \in \phi(G)$. Let

$\iota : \mathbb{Z} \cup G \to \phi(G)$ be the map defined by $x \mapsto \overline{x}$. Extending ι to relations in the obvious way, we write $A^\star := \iota(A) \in \iota(\mathbb{Z}_d)^{I \times J}$ and $\mathbf{b}^\star := \iota(\mathbf{b}) \in \iota(G)^I$.

Claim. The system $(A^\star, \mathbf{b}^\star)$ is solvable over $\phi(G)$ if, and only if, $(A, \mathbf{b})$ is solvable over G.

Proof of claim. In one direction, observe that a solution $\mathbf{s}$ to $(A, \mathbf{b})$ gives the solution $\iota(\mathbf{s})$ to $(A^\star, \mathbf{b}^\star)$. For the other direction, suppose that $\mathbf{s} \in \phi(G)^J$ is a vector such that $A^\star \cdot \mathbf{s} = \mathbf{b}^\star$. Since each element $(g, [m]_d) \in \phi(G)$ can be written uniquely as $(g, [m]_d) = \overline{g} + \overline{m}$, we write $\mathbf{s} = \mathbf{s}_g + \mathbf{s}_n$, where $\mathbf{s}_g \in \iota(G)^J$ and $\mathbf{s}_n \in \iota(\mathbb{Z}_d)^J$. Observe that we have $\overline{g} \bullet \overline{m} \in \iota(G) \subseteq \phi(G)$ and $\overline{n} \bullet \overline{m} \in \iota(\mathbb{Z}_d) \subseteq \phi(G)$ for all $g \in G$ and $n, m \in \mathbb{Z}$. Hence, it follows that $A^\star \cdot \mathbf{s}_n \in \iota(\mathbb{Z}_d)^I$ and $A^\star \cdot \mathbf{s}_g \in \iota(G)^I$. Now, since $\mathbf{b}^\star \in \iota(G)^I$, we have $\mathbf{b}^\star = A^\star \cdot \mathbf{s} = A^\star \cdot \mathbf{s}_g + A^\star \cdot \mathbf{s}_n = A^\star \cdot \mathbf{s}_g$. Hence, $\mathbf{s}_g$ gives a solution to $(A, \mathbf{b})$, as required.

All that remains is to show that our reduction can be formalised as a DTC-interpretation. Essentially, this comes down to showing that the ring $\phi(G)$ can be interpreted in G by formulas of DTC. By elementary group theory, we know that for elements $g \in G$ of maximal order we have $\mathrm{ord}\,(g) = d$. It is not hard to see that the set of group elements of maximal order can be defined in DTC; hence, we can interpret $\mathbb{Z}_d$ in G. Also, it is not hard to show that the the multiplication of $\phi(G)$ is DTC-definable, which completes the proof. ◀

We conclude this section by describing a DTC-reduction from the solvability problem over general rings R to solvability over commutative rings. As a technical preparation, we first give a first-order interpretation that transforms a linear equation systems over R into an equivalent system with the following property: the linear equation system is solvable if, and only if, the solution space contains a *numerical solution*, i.e. a solution over $\mathbb{Z}$.

For convenience, we only consider left-multiplicative linear systems, which are systems of the form $A \cdot \mathbf{x} = \mathbf{b}$; however, the more general case of linear equation systems of the form $A_l \cdot \mathbf{x} + \mathbf{x} \cdot A_r = \mathbf{b}$ can be treated similarly.

▶ **Lemma 4.** *There is an* FO*-interpretation* $\mathcal{I}$ *of* $\tau_{les\text{-}r}$ *in* $\tau_{les\text{-}r}$ *such that for every linear system* $\mathbf{S} : A \cdot \mathbf{x} = \mathbf{b}$ *over* R*,* $\mathcal{I}(\mathbf{S})$ *describes a linear system* $\mathbf{S}^\star : A^\star \cdot_{\mathbb{Z}} \mathbf{x}^\star = \mathbf{b}^\star$ *over the* $\mathbb{Z}$*-module* $(R, +)$ *such that* $\mathbf{S}$ *is solvable over* R *if, and only if,* $\mathbf{S}^\star$ *has a solution over* $\mathbb{Z}$*.*

Proof (sketch). Let $A \in R^{I \times J}$ and $\mathbf{b} \in R^I$. For $\mathbf{S}^\star$, we introduce for each variable x_j $(j \in J)$ and each element $s \in R$ a new variable x_j^s, i.e. the index set for the variables of $\mathbf{S}^\star$ is $J \times R$. Finally, we replace all terms of the form rx_j by $\sum_{s \in R} rsx_j^s$. ◀

By Lemma 4, we can restrict to linear systems $(A, \mathbf{b})$ over the $\mathbb{Z}$-module $(R, +)$ that have numerical solutions. At this point, we reuse our construction from Theorem 3 to obtain a linear system $(A^\star, \mathbf{b}^\star)$ over the commutative ring $R^\star := \phi((R, +))$, where $A^\star := \iota(A)$ and $\mathbf{b}^\star := \iota(\mathbf{b})$. We claim that $(A^\star, \mathbf{b}^\star)$ is solvable over $R^\star$ if, and only if, $(A, \mathbf{b})$ is solvable over R. For the non-trivial direction, suppose $\mathbf{s}$ is a solution to $(A^\star, \mathbf{b}^\star)$ and decompose $\mathbf{s} = \mathbf{s}_g + \mathbf{s}_n$ into group elements and number elements, as explained in the proof of Theorem 3. Recalling that $\overline{r}_1 \bullet \overline{r}_2 = 0$ for all $r_1, r_2 \in R$, it follows that $A^\star \bullet (\mathbf{s}_g + \mathbf{s}_n) = A^\star \bullet \mathbf{s}_n = \mathbf{b}^\star$. Hence, there is a solution $\mathbf{s}_n$ to $(A^\star, \mathbf{b}^\star)$ that consists *only* of number elements, as claimed.

▶ **Theorem 5.** $\textsc{SlvR} \le_{\mathrm{DTC}} \textsc{SlvCR}$.

4 The structure of finite commutative rings

In this section we study structural properties of (finite) commutative rings and present the remaining reductions for solvability outlined in §3: from commutative rings to local rings, and from k-generated local rings to commutative rings with a linear order. Recall that a commutative ring R is local if it contains a unique maximal ideal m. The importance of the notion of local rings comes from the fact that they are the basic building blocks of finite commutative rings. We start by summarising some of their useful properties.

▶ **Proposition 6** (Properties of local rings)**.** *For any finite commutative ring R we have:*
- *If R is local, then the unique maximal ideal is $m = R \setminus R^\times$.*
- *R is local if, and only if, all idempotent elements in R are trivial.*
- *If $x \in R$ is idempotent then $R = x \cdot R \oplus (1-x) \cdot R$ as a direct sum of rings.*
- *If R is local then its cardinality (and hence its characteristic) is a prime power.*

By this proposition we know that finite commutative rings can be decomposed into local summands that are primary ideals generated by pairwise orthogonal idempotent elements. Indeed, this decomposition is unique (for details, see e.g. [5]).

▶ **Proposition 7** (Decomposition into local rings)**.** *Let R be a (finite) commutative ring. Then there is a unique set $\mathcal{B}(R) \subseteq R$ of pairwise orthogonal idempotents elements for which it holds that (i) $e \cdot R$ is local for each $e \in \mathcal{B}(R)$; (ii) $\sum_{e \in \mathcal{B}(R)} e = 1$; and (iii) $R = \bigoplus_{e \in \mathcal{B}(R)} e \cdot R$.*

We next show that the ring decomposition $R = \bigoplus_{e \in \mathcal{B}(R)} e \cdot R$ is FO-definable. As a first step, we note that $\mathcal{B}(R)$ (the *base* of R) is FO-definable over R.

▶ **Lemma 8.** *There is $\phi(x) \in \mathrm{FO}(\tau_{ring})$ such that $\phi(x)^R = \mathcal{B}(R)$ for commutative rings R.*

Proof (sketch). It can be shown that $\mathcal{B}(R)$ consists precisely of those non-trivial idempotent elements of R which cannot be expressed as the sum of two orthogonal non-trivial idempotents, which is a first-order definable property. In particular, if R is local then trivially $\mathcal{B}(R) = \{1\}$. To test for locality, it suffices by Proposition 6 to check whether all idempotent elements in R are trivial and this can be expressed easily in first-order logic. ◀

The next step is to show that the canonical mapping $R \to \bigoplus_{e \in \mathcal{B}(R)} e \cdot R$ can be defined in FO. To this end, recall from Proposition 6 that for every $e \in \mathcal{B}(R)$ (indeed, for any idempotent element $e \in R$), we can decompose the ring R as $R = e \cdot R \oplus (1-e) \cdot R$. This fact allows us to define for all base elements $e \in \mathcal{B}(R)$ the projection of elements $r \in R$ onto the summand $e \cdot R$ in first-order logic, without having to keep track of all local summands simultaneously.

▶ **Lemma 9.** *There is a formula $\psi(x, y, z) \in \mathrm{FO}(\tau_{ring})$ such that for all rings R, $e \in \mathcal{B}(R)$ and $r, s \in R$, it holds that $(R, e, r, s) \models \psi$ if, and only if, s is the projection of r onto $e \cdot R$.*

It follows that any relation over R can be decomposed in first-order logic according to the decomposition of R into local summands. In particular, a linear equation system $(A \mid \mathbf{b})$ over R is solvable if, and only if, each of the projected linear equation systems $(A^e \mid \mathbf{b}^e)$ is solvable over eR. Hence, we obtain:

▶ **Theorem 10.** $\textsc{SlvCR} \leq_{FO\text{-}T} \textsc{SlvLR}$.

In §3 we proved that solvability over rings with a linear ordering can be reduced in fixed-point logic to solvability over cyclic groups. This naturally raises the question: which classes of rings can be linearly ordered in fixed-point logic? By Lemma 9, we know that for this question it suffices to focus on local rings, which have a well-studied structure. The simplest type of local ring are rings of the form $\mathbb{Z}_{p^n}$ and the natural ordering of such rings can be easily defined by a formula of FP. Moreover, the same holds for finite fields as they have a cyclic multiplicative group [16]. In the following lemma, we are able to generalise these insights in a strong sense: for any fixed $k \geq 1$ we can define an ordering on the class of all local rings for which the maximal ideal is generated by at most k elements. We refer to such rings as *k-generated local rings*. Note that for $k = 1$ we obtain the notion of chain rings which include all finite fields and rings of the form $\mathbb{Z}_{p^n}$. For increasing values of k the structure of k-generated local rings becomes more and more sophisticated. For instance, the ring $R_k = \mathbb{Z}_2[X_1, \dots, X_k]/(X_1^2, \dots, X_k^2)$ is a k-generated local ring which is not $(k-1)$-generated.

▶ **Lemma 11** (Ordering k-generated local rings)**.** *There is an* FP*-formula $\phi(x, z_1, \dots, z_k; v, w)$ such that for all k-generated local rings R there are $\alpha, \pi_1, \dots, \pi_k \in R$ such that*

$$\phi^R(\alpha/x, \vec{\pi}/\vec{z}; v, w) = \{(a, b) \in R \times R \mid (R, \alpha, \vec{\pi}; a, b) \models \phi\}, \text{ is a linear order on } R.$$

Proof. Firstly, there are FP-formulas $\phi_u(x), \phi_m(x), \phi_g(x_1, \dots, x_k)$ that define in each k-generated local ring R the set of units, the maximal ideal m (which is the set of non-units) and the property of being a set of size k that generates m, respectively. More specifically, for all $(\pi_1, \dots, \pi_k) \in \phi_g^R$ we have that $\sum_i \pi_i R = \phi_m^R$ is the maximal ideal of R and $R^\times = \phi_u^R = R \setminus m$. In particular there is a first-order interpretation of the field $k := R/m$ in R.

The idea of the proof is to represent the elements of R as polynomial expressions of a certain kind. Let $q := |k|$ and define $\Gamma(R) := \{r \in R : r^q = r\}$. It can be seen that $\Gamma(R) \setminus \{0\}$ forms a multiplicative group which is known as the *Teichmüller coordinate set* [5]. Now, the map $\iota : \Gamma(R) \to k$ defined by $r \mapsto r + m$ is a bijection. Indeed, for two different units $r, s \in \Gamma(R)$ we have $r - s \notin m$. Otherwise, we would have $r - s = x$ for some $x \in m$ and thus $r = (s + x)^q = s + \sum_{k=1}^{q} \binom{q}{k} x^k s^{q-k}$. Since $q \in m$ and $r - s = x$ we obtain that $x = xy$ for some $y \in m$. Hence $x(1 - y) = 0$ and since $(1 - y) \in R^\times$ this means $x = 0$.

As explained above, we can define in FP an order on k by fixing a generator $\alpha \in k^\times$ of the cyclic group $k^\times$. Combining this order with ι^{-1}, we obtain an FP-definable order on $\Gamma(R)$. The importance of $\Gamma(R)$ lies in the fact that every ring element can be expressed as a polynomial expression over a set of k generators of the maximal ideal m with coefficients lying in $\Gamma(R)$. To be precise, let $\pi_1, \dots, \pi_k \in m$ be a set of generators for m, i.e. $m = \pi_1 R + \cdots + \pi_k R$, where each π_i has nilpotency n_i for $1 \leq i \leq k$. We claim that we can express $r \in R$ as

$$r = \sum_{(i_1, \dots, i_k) \leq_{\text{lex}} (n_1, \dots, n_k)} a_{i_1 \cdots i_k} \pi_1^{i_1} \cdots \pi_k^{i_k}, \quad \text{with } a_{i_1 \cdots i_k} \in \Gamma(R). \tag{P}$$

To see this, consider the following recursive algorithm:

- If $r \in R^\times$, then for a unique $a \in \Gamma(R)$ we have that $r \in a + m$, so $r = a + (\pi_1 r_1 + \cdots + \pi_k r_k)$ for some $r_1, \dots, r_k \in R$ and we continue with $r_1, \dots, r_k$.
- Else $r \in m$, and $r = \pi_1 r_1 + \cdots + \pi_k r_k$ for some $r_1, \dots, r_k \in R$; continue with $r_1, \dots, r_k$.

Observe that for all pairs $a, b \in \Gamma(R)$ there exist elements $c \in \Gamma(R), r \in m$ such that $a\pi_1^{i_1} \cdots \pi_k^{i_k} + b\pi_1^{i_1} \cdots \pi_k^{i_k} = c\pi_1^{i_1} \cdots \pi_k^{i_k} + r\pi_1^{i_1} \cdots \pi_k^{i_k}$. Since $\pi_1^{i_1} \cdots \pi_k^{i_k} = 0$ if $i_l \geq n_l$ for some $1 \leq l \leq k$, the process is guaranteed to stop and the claim follows.

Note that this procedure neither yields a polynomial-time algorithm nor do we obtain a *unique* expression, as for instance, the choice of elements $r_1, \dots, r_k \in R$ (in both recursion steps) need not to be unique. However, knowing only the existence of an expression of this kind, we can proceed as follows. For any sequence of exponents $(\ell_1, \dots, \ell_k) \leq_{\text{lex}} (n_1, \dots, n_k)$

define the ideal $R[\ell_1, \dots, \ell_k] \trianglelefteq R$ as the set of all elements having an expression of the form (P) where $a_{i_1 \cdots i_k} = 0$ for all $(i_1, \dots, i_k) \leq_{\mathrm{lex}} (\ell_1, \dots, \ell_k)$.

It is clear that we can define the ideal $R[\ell_1, \dots, \ell_k]$ in FP. Having this, we can use the following recursive procedure to define a unique expression of the form (P) for all $r \in R$:

- Choose the minimal $(i_1, \dots, i_k) \leq_{\mathrm{lex}} (n_1, \dots, n_k)$ such that $r = a\pi_1^{i_1} \cdots \pi_k^{i_k} + s$ for some (minimal) $a \in \Gamma(R)$ and $s \in R[i_1, \dots, i_k]$. Continue the process with s.

Finally, the lexicographical ordering induced by the ordering on $n_1 \times \cdots \times n_k$ and the ordering on $\Gamma(R)$ yields an FP-definable order on R (with parameters for generators of $k^\times$ and m). ◀

▶ **Corollary 12.** $\textsc{SlvLR}_k \leq_{\text{FP-T}} \textsc{SlvCR}_{\leqslant} \leq_{\text{FP}} \textsc{SlvCycG}$.

5 Solvability problems under logical reductions

In the previous two sections we studied reductions between solvability problems over different algebraic domains. Here we change our perspective and investigate classes of *queries* that are reducible to solvability over a fixed commutative ring. Our motivation for this work was to study extensions of first-order logic with generalised quantifiers which express solvability problems over rings. In particular, the aim was to establish various *normal forms* for such logics. However, rather than defining a host of new logics in full detail, we state our results in this section in terms of closure properties of classes of finite structures that are themselves defined by reductions to solvability problems. We explain the connection between the specific closure properties and the corresponding logical normal forms in more detail below.

To state our main results formally, let R be a commutative ring and write $\textsc{Slv}(R)$ to denote the solvability problem over R, as a class of $\tau_{\mathrm{les}}(R)$-structures. Let $\Sigma_{\mathrm{FO}}^{\mathrm{qf}}(R)$ and $\Sigma_{\mathrm{FO}}(R)$ denote the classes of queries that are reducible to $\textsc{Slv}(R)$ under quantifier-free and first-order many-to-one reductions, respectively. Then we show that $\Sigma_{\mathrm{FO}}^{\mathrm{qf}}(R)$ and $\Sigma_{\mathrm{FO}}(R)$ are closed under first-order operations for any commutative ring R, which also shows that $\Sigma_{\mathrm{FO}}^{\mathrm{qf}}(R)$ contains *any* FO-definable query. Furthermore, we prove that if R has prime characteristic, then $\Sigma_{\mathrm{FO}}^{\mathrm{qf}}(R)$ and $\Sigma_{\mathrm{FO}}(R)$ are closed under oracle queries. Thus, if we denote by $\Sigma_{\mathrm{FO}}^{\mathrm{T}}(R)$ the class of queries reducible to $\textsc{Slv}(R)$ by first-order Turing reductions, then for all commutative rings R of prime characteristic the three solvability reduction classes coincide, i.e. we have $\Sigma_{\mathrm{FO}}^{\mathrm{qf}}(R) = \Sigma_{\mathrm{FO}}(R) = \Sigma_{\mathrm{FO}}^{\mathrm{T}}(R)$.

To relate these results to logical normal forms, we let $\mathcal{D} = \textsc{Slv}(R)$ and write $\mathrm{FOS}_{\mathrm{R}} := \mathrm{FO}(\langle Q_{\mathcal{D}} \rangle)$ to denote first-order logic extended by generalised Lindström quantifiers deciding solvability over R. Then the closure of $\Sigma_{\mathrm{FO}}(R)$ under first-order operations amounts to showing that the fragment of $\mathrm{FOS}_{\mathrm{R}}$ which consists of formulas without *nested* solvability quantifiers has a normal form which consists of a single application of a solvability quantifier to a first-order formula. Moreover, for the case when R has prime characteristic, the closure of $\Sigma_{\mathrm{FO}}^{\mathrm{qf}}(R) = \Sigma_{\mathrm{FO}}(R)$ under first-order oracle queries amounts to showing that nesting of solvability quantifiers can be reduced to a single quantifier. It follows that $\mathrm{FOS}_{\mathrm{R}}$ has a strong normal form: one application of a solvability quantifier to a *quantifier-free* formula suffices.

5.1 Closure under first-order operations

Let R be a fixed commutative ring of characteristic m. In this section we prove the closure of $\Sigma_{\mathrm{FO}}^{\mathrm{qf}}(R)$ and $\Sigma_{\mathrm{FO}}(R)$ under first-order operations. To this end, we need to establish a couple of technical results. Of particular importance is the following key lemma, which gives a simple normal form for linear equation systems: up to quantifier-free reductions, we can restrict ourselves to linear systems over rings $\mathbb{Z}_m$, where the constant term of every equation is $1 \in \mathbb{Z}_m$. The proof of the lemma crucially relies on the fact that the ring R is fixed.

▶ **Lemma 13** (Normal form for linear equation systems). *There is a quantifier-free interpretation $\mathcal{I}$ of $\tau_{les}(\mathbb{Z}_m)$ in $\tau_{les}(R)$ so that for all $\tau_{les}(R)$-structures $\mathbf{S}$ it holds that*

- *$\mathcal{I}(\mathbf{S})$ is an equation system $(A, \mathbf{b})$ over $\mathbb{Z}_m$, where A is a $\{0,1\}$-matrix and $\mathbf{b} = \mathbf{1}$; and*
- *$\mathbf{S} \in \mathrm{SLV}(R)$ if, and only if, $\mathcal{I}(\mathbf{S}) \in \mathrm{SLV}(\mathbb{Z}_m)$.*

Proof. We describe $\mathcal{I}$ as the composition of three quantifier-free transformations: the first one maps a system $(A, \mathbf{b})$ over R to an equivalent system $(B, \mathbf{c})$ over $\mathbb{Z}_m$, where m is the characteristic of R. Secondly, $(B, \mathbf{c})$ is mapped to an equivalent system $(C, \mathbf{1})$ over $\mathbb{Z}_m$. Finally, we transform $(C, \mathbf{1})$ into an equivalent system $(D, \mathbf{1})$ over $\mathbb{Z}_m$, where D is a $\{0,1\}$-matrix. The first transformation is obtained by adapting the proof of Theorem 2. It can be seen that first-order quantifiers and fixed-point operators are not needed if R is fixed.

For the second transformation, suppose that B is an $I \times J$ matrix and $\mathbf{c}$ a vector indexed by I. We define a new linear equation system $\mathbf{T}$ which has in addition to all the variables that occur in $\mathbf{S}$, a new variable v_e for every $e \in I$ and a new variable w_r for every $r \in R$. For every element $r \in \mathbb{Z}_m$, we include in $\mathbf{T}$ the equation $(1-r)w_1 + w_r = 1$. It can be seen that this subsysem of equations has a unique solution given by $w_r = r$ for all $r \in \mathbb{Z}_m$. Finally, for every equation $\sum_{j \in J} B(e,j) \cdot x_j = \mathbf{c}(e)$ in $\mathbf{S}$ (indexed by $e \in I$) we include in $\mathbf{T}$ the two equations $v_e + \sum_{j \in J} B(e,j) \cdot x_j = 1$ and $v_e + w_{\mathbf{c}(e)} = 1$.

Finally, we translate the system $\mathbf{T} : C\mathbf{x} = \mathbf{1}$ over $\mathbb{Z}_m$ into an equivalent system over $\mathbb{Z}_m$ in which all coefficients are either 0 or 1. For each variable v in $\mathbf{T}$, the system has the m distinct variables $v_0, \ldots, v_{m-1}$ together with equations $v_i = v_j$ for $i \neq j$. By replacing all terms rv by $\sum_{1 \le i \le r} v_i$ we obtain an equivalent system. However, in order to establish our original claim we need to rewrite the auxiliary equations of the form $v_i = v_j$ as a set of equations whose constant terms are equal to 1. To achieve this, we introduce a new variable v_j^- for each v_j, and the equation $v_j + v_j^- + w_1 = 1$. Finally, we rewrite $v_i = v_j$ as $v_i + v_j^- + w_1 = 1$. The resulting system is equivalent to $\mathbf{T}$ and has the desired form. ◀

▶ **Corollary 14.** *$\Sigma_{\mathrm{FO}}^{qf}(R) = \Sigma_{\mathrm{FO}}^{qf}(\mathbb{Z}_m)$, $\Sigma_{\mathrm{FO}}(R) = \Sigma_{\mathrm{FO}}(\mathbb{Z}_m)$ and $\Sigma_{\mathrm{FO}}^{T}(R) = \Sigma_{\mathrm{FO}}^{T}(\mathbb{Z}_m)$.*

It is a basic fact from linear algebra that solvability of a linear equation system $A \cdot \mathbf{x} = \mathbf{b}$ is invariant under applying elementary row and column operations to the augmented coefficient matrix $(A \mid \mathbf{b})$. Over fields, this insight justifies the method of Gaussian elimination, which transforms the augmented coefficient matrix of a linear system into row echelon form. Over the integers, a generalisation of this method can be used to transform a linear system into Hermite normal form. The following lemma shows that a similar normal form exists over chain rings. The proof uses the fact that in a chain ring R, divisibility is a total preorder.

▶ **Lemma 15** (Hermite normal form). *For every $k \times \ell$-matrix A over a chain ring R, there exists an invertible $k \times k$-matrix S and an $\ell \times \ell$-permutation matrix T so that*

$$SAT = \begin{pmatrix} Q \\ \mathbf{0} \end{pmatrix} \quad \text{with} \quad Q = \begin{pmatrix} a_{11} & \cdots & \star \\ 0 & \ddots & \vdots \\ \mathbf{0} & 0 & a_{kk} \end{pmatrix},$$

where $a_{11} \mid a_{22} \mid a_{33} \mid \cdots \mid a_{kk}$ and for all $1 \le i, j \le k$ it holds that $a_{ii} \mid a_{ij}$.

Now we are ready to prove the closure of $\Sigma_{\mathrm{FO}}^{\mathrm{qf}}(R)$ and $\Sigma_{\mathrm{FO}}(R)$ under first-order operations. First of all, it can be seen that conjunction and universal quantification can be handled easily by combining independent subsystems into a single system. Thus, the only non-trivial part of the proof is to establish closure under complementation. To do that, we describe an appropriate reduction that translates from non-solvability to solvability of linear systems.

First of all, we consider the case where R has characteristic $m = p$ for a prime p. In this case we know that $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(R) = \Sigma^{\mathrm{qf}}_{\mathrm{FO}}(\mathbb{Z}_p)$ and $\Sigma_{\mathrm{FO}}(R) = \Sigma_{\mathrm{FO}}(\mathbb{Z}_p)$ by Corollary 14, where $\mathbb{Z}_p$ is a finite field. Over fields, the method of Gaussian elimination guarantees that a linear equation system $(A, \mathbf{b})$ is not solvable if, and only if, for some vector $\mathbf{x}$ we have $\mathbf{x} \cdot (A \mid \mathbf{b}) = (0, \ldots, 0, 1)$. In other words, the vector $\mathbf{b}$ is not in the column span of A if, and only if, the vector $(0, \ldots, 0, 1)$ is in the row span of $(A \mid \mathbf{b})$. This shows that $(A \mid \mathbf{b})$ is not solvable if, and only if, the system $((A \mid \mathbf{b})^T, (0, \ldots, 0, 1)^T)$ is solvable. In other words, over fields this reasoning translates the question of non-solvability to the question of solvability. In the proof of the next lemma, we generalise this approach to chain rings, which enables us to translate from non-solvability to solvability over all rings of prime-power characteristic.

▶ **Lemma 16** (Non-solvability over chain rings). *Let $(A, \mathbf{b})$ be a linear equation system over a chain ring R with maximal ideal πR and let n be the nilpotency of π. Then $(A, \mathbf{b})$ is not solvable over R if, and only if, there is a vector $\mathbf{x}$ such that $\mathbf{x} \cdot (A \mid \mathbf{b}) = (0, \ldots, 0, \pi^{n-1})$.*

Proof. If such a vector $\mathbf{x}$ exists, then $(A, \mathbf{b})$ is not solvable. On the other hand, if no such $\mathbf{x}$ exists, then we apply Lemma 15 to transform the augmented matrix $(A \mid \mathbf{b})$ into Hermite normal form $(A' \mid \mathbf{b}')$ with respect to A (that is, $A' = SAT$ as in Lemma 15 and $\mathbf{b}' = S\mathbf{b}$). We claim that for every row index i, the diagonal entry a_{ii} in the transformed coefficient matrix A' divides the i-th entry of the transformed target vector $\mathbf{b}'$. Towards a contradiction, suppose that there is some a_{ii} not dividing $\mathbf{b}'_i$. Then a_{ii} is not a non-unit in R and can be written as $a_{ii} = u\pi^t$ for some unit u and $t \geq 1$. By Lemma 15, it holds that a_{ii} divides every entry in the i-th row of A' and thus we can multiply the i-th row of the augmented matrix $(A' \mid \mathbf{b}')$ by an appropriate non-unit to obtain a vector of the form $(0, \ldots, 0, \pi^{n-1})$, contradicting our assumption. Hence, in the transformed augmented coefficient matrix, diagonal entries divide *all* entries in the same row, which implies solvability of $(A \mid \mathbf{b})$. ◀

Along with our previous discussion, Lemma 16 now yields the closure of $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(R)$ and $\Sigma_{\mathrm{FO}}(R)$ under complementation if R has prime-power characteristic. For a linear systems $(A, \mathbf{b})$ over a non-local ring $\mathbb{Z}_m$ (i.e. m is not a prime power), we can consider the decomposition of $\mathbb{Z}_m$ into a direct sum of local rings and apply the Chinese remainder theorem.

▶ **Theorem 17.** *$\Sigma^{qf}_{\mathrm{FO}}(R)$, $\Sigma_{\mathrm{FO}}(R)$ and $\Sigma^{T}_{\mathrm{FO}}(R)$ are closed under first-order operations.*

5.2 Solvability over rings of prime characteristic

From now on we assume that the commutative ring R is of prime characteristic p. We prove that in this case, the three reduction classes $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(R)$, $\Sigma_{\mathrm{FO}}(R)$ and $\Sigma^{\mathrm{T}}_{\mathrm{FO}}(R)$ coincide. First of all, we note that, by definition, we have $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(R) \subseteq \Sigma_{\mathrm{FO}}(R) \subseteq \Sigma^{\mathrm{T}}_{\mathrm{FO}}(R)$. Also, since we know that solvability over R can be reduced to solvability over $\mathbb{Z}_p$ (Corollary 14), it suffices for our proof to show that $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(\mathbb{Z}_p) \supseteq \Sigma^{\mathrm{T}}_{\mathrm{FO}}(\mathbb{Z}_p)$. Furthermore, by Theorem 17 it follows that $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(\mathbb{Z}_p)$ is closed under first-order operations, so it only remains to prove closure under oracle queries. Recalling that the original motivation for this study was to establish normal forms for logics with solvability quantifiers, it can be seen that proving closure under oracle queries corresponds to showing that for every formula of $\mathrm{FOS}_{\mathrm{R}}$ with nested solvability quantifiers, where R has prime characteristic, there is an equivalent $\mathrm{FOS}_{\mathrm{R}}$-formula with no nested solvability quantifiers. Since $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(R)$ is closed under first-order operations, any

FO-definable query is contained in $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(R)$; thus, we can conclude that every $\mathrm{FOS}_{\mathrm{R}}$-formula is equivalent to the single application of a solvability quantifier to a quantifier-free formula.

More specifically in terms of the classes $\Sigma^{\mathrm{qf}}_{\mathrm{FO}}(\mathbb{Z}_p)$, it can be seen that proving closure under oracle queries amounts to showing that nesting of linear equation systems can be reduced to a single system only. To formalise this, let $\mathcal{I}(\vec{x},\vec{y})$ be a quantifier-free interpretation of $\tau_{\mathrm{les}}(\mathbb{Z}_p)$ in σ with parameters $\vec{x},\vec{y}$ of length k and l, respectively. We extend the signature σ to $\sigma_X := \sigma \cup \{X\}$ and restrict our attention to those σ_X-structures $\mathbf{A}$ (with domain A) where the relation symbol X is interpreted as $X^{\mathbf{A}} = \{(\vec{a},\vec{b}) \in A^{k\times l} \mid \mathcal{I}(\vec{a},\vec{b})(\mathbf{A}) \in \textsc{Slv}(\mathbb{Z}_p)\}$. Then it remains to show that for any quantifier-free interpretation $\mathcal{O}$ of $\tau_{\mathrm{les}}(\mathbb{Z}_p)$ in σ_X, there is a quantifier-free interpretation of $\tau_{\mathrm{les}}(\mathbb{Z}_p)$ in σ that describes linear equation systems equivalent to $\mathcal{O}$. Hereafter, for any σ_X-structure $\mathbf{A}$ and tuples $\vec{a}$ and $\vec{b}$, we will refer to $\mathcal{O}(\mathbf{A})$ as an "outer" linear equation system and refer to $\mathcal{I}(\vec{a},\vec{b})(\mathbf{A})$ as an "inner" linear equation system. By applying Lemma 13 and Theorem 17, it is sufficient to consider the case where for σ_X-structures $\mathbf{A}$, $\mathcal{O}(\mathbf{A})$ describes a linear system $(M,\mathbf{1})$, where M is the $\{0,1\}$-matrix of the relation $X^{\mathbf{A}}$. For an illustration of this setup, see Figure 2.

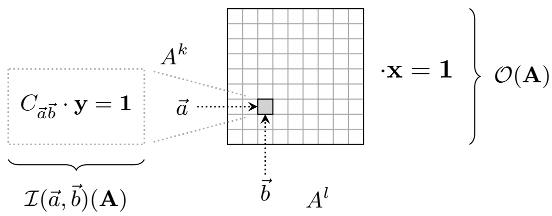

Figure 2 Each entry $(\vec{a},\vec{b})$ of the coefficient matrix of the outer linear equation system $\mathcal{O}(\mathbf{A})$ is determined by the corresponding inner linear system $C_{\vec{a}\vec{b}} \cdot \mathbf{y} = \mathbf{1}$ described by $\mathcal{I}(\vec{a},\vec{b})(\mathbf{A})$: this entry is 1 if $\mathcal{I}(\vec{a},\vec{b})(\mathbf{A})$ is solvable and 0 otherwise.

▶ **Theorem 18** (Closure under oracle queries). *For $\mathcal{I}$, $\mathcal{O}$ as above, there exists a quantifier-free interpretation $\mathcal{K}$ of $\tau_{les}(\mathbb{Z}_p)$ in σ such that for all σ_X-structures $\mathbf{A}$ it holds that $\mathcal{O}(\mathbf{A}) \in \textsc{Slv}(\mathbb{Z}_p)$ if, and only if, $\mathcal{K}(\mathbf{A}) \in \textsc{Slv}(\mathbb{Z}_p)$.*

Proof. For a σ-structure $\mathbf{A}$, let M_o denote the $\{0,1\}$-coefficient matrix of the outer linear equation system $\mathcal{O}(\mathbf{A})$. Then for $(\vec{a},\vec{b}) \in A^{k\times l}$ we have $M_o(\vec{a},\vec{b}) = 1$ if, and only if, the inner linear system $\mathcal{I}(\vec{a},\vec{b})(\mathbf{A})$ is solvable. By identifying the variables of $\mathcal{O}(\mathbf{A})$ by $\{v_{\vec{b}} \mid \vec{b} \in A^l\}$, we can express the equations of $\mathcal{O}(\mathbf{A})$ as $\sum_{\vec{b}\in A^l} M_o(\vec{a},\vec{b}) \cdot v_{\vec{b}} = 1$, for $\vec{a} \in A^k$.

We begin to construct the system $\mathcal{K}(\mathbf{A})$ over the set of variables $\{v_{\vec{a},\vec{b}} \mid (\vec{a},\vec{b}) \in A^{k\times l}\}$ by including the equations $\sum_{\vec{b}\in A} v_{\vec{a},\vec{b}} = 1$ for all $\vec{a} \in A^k$. Our aim is to extend $\mathcal{K}(\mathbf{A})$ by additional equations so that in every solution to $\mathcal{K}(\mathbf{A})$, there are values $v_{\vec{b}} \in \mathbb{Z}_p$ such that for all $\vec{a} \in A^k$, we have $v_{\vec{a},\vec{b}} = M_o(\vec{a},\vec{b}) \cdot v_{\vec{b}}$. Assuming this to be true, it is immediate that $\mathcal{O}(\mathbf{A})$ is solvable if, and only if, $\mathcal{K}(\mathbf{A})$ is solvable, which is what we want to show.

In order to enforce the condition "$v_{\vec{a},\vec{b}} = M_o(\vec{a},\vec{b}) \cdot v_{\vec{b}}$" by *linear* equations, we need to introduce a number of auxilliary linear subsystems to $\mathcal{K}(\mathbf{A})$. The reason why we cannot express this condition directly by a linear equation is because $M_o(\vec{a},\vec{b})$ is determined by solvability of the inner system $\mathcal{I}(\vec{a},\vec{b})(\mathbf{A})$. Therefore, if we were to treat both the elements of $M_o(\vec{a},\vec{b})$ and the $v_{\vec{b}}$ as individual variables, then that would require to express the *non-linear* term $M_o(\vec{a},\vec{b}) \cdot v_{\vec{b}}$. To overcome this issue, we introduce new subsystems in $\mathcal{K}(\mathbf{A})$ to ensure that for all $\vec{a},\vec{b},\vec{c} \in A$:

$$\textbf{if } v_{\vec{a},\vec{b}} \neq 0 \textbf{ then } M_o(\vec{a},\vec{b}) = 1; \text{ and} \tag{$*$}$$

$$\textbf{if } v_{\vec{a},\vec{b}} \neq v_{\vec{c},\vec{b}} \textbf{ then } \{M_o(\vec{a},\vec{b}), M_o(\vec{c},\vec{b})\} = \{0,1\}. \tag{$\dagger$}$$

Assuming we have expressed $(*)$ and $(\dagger)$, it can be seen that solutions of $\mathcal{K}(\mathbf{A})$ directly translate into solutions for $\mathcal{O}(\mathbf{A})$ and vice versa. To express $(*)$ we proceed as follows: for each $(\vec{a},\vec{b}) \in A^{k\times l}$ we introduce $\mathcal{I}(\vec{a},\vec{b})(\mathbf{A})$ as an independent linear subsystem in $\mathcal{K}(\mathbf{A})$ in which we additionally add to each single equation the term $(v_{\vec{a},\vec{b}}+1)$. Now, if in a solution of $\mathcal{K}(\mathbf{A})$ the variable $v_{\vec{a},\vec{b}}$ is evaluated to 0, then the subsystem corresponding to $\mathcal{I}(\vec{a},\vec{b})(\mathbf{A})$ is trivially solvable (recall, that the target vector is $\mathbf{1}$). However, if a non-zero value is assigned to $v_{\vec{a},\vec{b}}$, then this value is a unit in $\mathbb{Z}_p$ and thereby a solution for $\mathcal{K}(\mathbf{A})$ necessarily contains a solution of the subsystem $\mathcal{I}(\vec{a},\vec{b})(\mathbf{A})$; that is, we have $M_o(\vec{a},\vec{b}) = 1$.

For (†) we follow a similar approach. For fixed tuples $\vec{a}$, $\vec{b}$ and $\vec{c}$, the condition on the right-hand side of (†) is a simple Boolean combination of solvability queries. Hence, by Theorem 17, this combination can be expressed by a single linear equation system. Again we embed the respective linear equation system as a subsystem in $\mathcal{K}(\mathbf{A})$ where we add to each of its equations the term $(1 + v_{\vec{a},\vec{b}} - v_{\vec{c},\vec{b}})$. With the same reasoning as above we conclude that this imposes the constraint (†) on the variables $v_{\vec{a},\vec{b}}$ and $v_{\vec{c},\vec{b}}$, which concludes the proof. ◀

▶ **Corollary 19.** *If R has prime characteristic, then $\Sigma^{qf}_{\mathrm{FO}}(R) = \Sigma_{\mathrm{FO}}(R) = \Sigma^{T}_{\mathrm{FO}}(R)$.*

As explained above, our results have some important consequences. For a prime p, let us denote by FOS_p first-order logic extended by quantifiers deciding solvability over $\mathbb{Z}_p$, similar to what we have discussed before. Corresponding extensions of first-order logic by rank operators over prime fields (FOR_p) were studied by Dawar et al. [8]. Their results imply that $\mathrm{FOS}_p = \mathrm{FOR}_p$ over ordered structures, and that both logics have a strong normal form over ordered structures, i.e. that every formula is equivalent to a formula with only one application of a solvability or rank operator, respectively [21]. Corollary 19 allows us to generalise the latter result for FOS_p to arbitrary structures.

▶ **Corollary 20.** *Every $\phi \in \mathrm{FOS}_p$ is equivalent to a formula with a single solvability quantifier.*

6 Discussion

Motivated by the question of finding extensions of FPC to capture larger fragments of PTIME, we have analysed the (inter-)definability of solvability problems over various classes of algebraic domains. Similar to the notion of rank logic [8] one can consider *solvability logic*, which is the extension of FPC by (generalised Lindström) quantifiers that decide solvability of linear equation systems. In this context, our results from §3 and §4 can be seen to relate fragments of solvability logic obtained by restricting quantifiers to different algebraic domains, such as Abelian groups or commutative rings. We have also identified many classes of algebraic structures over which the solvability problem reduces to the very basic problem of solvability over cyclic groups of prime-power order. This raises the question, whether a reduction even to groups of prime order is possible. In this case, solvability logic would turn out to be a fragment of rank logic.

With respect to specific algebraic domains, we proved that FPC can define a linear order on the class of all k-generated local rings, i.e. on classes of local rings for which every maximal ideal can be generated by k elements, where k is a fixed constant. Together with our results from §4, this can be used to show that all natural problems from linear algebra over (not necessarily local) k-generated rings reduce to problems over ordered rings under FP-reductions. An interesting direction of future research is to explore how far our techniques can be used to show (non-)definability in fixed-point logic of other problems from linear algebra over rings.

Finally, we mention an interesting topic of related research, which is the logical study of *permutation group membership problems* (GM for short). An instance of GM consists of a set Ω, a set of generating permutations $\pi_1, \ldots, \pi_n$ on Ω and a target permutation π, and the problem is to decide whether π is generated by $\pi_1, \ldots, \pi_n$. This problem is known to be decidable in polynomial time (indeed it is in NC [4]). We can show that all the solvability problems we have studied in this paper reduce to GM under first-order reductions (basically, an application of Cayley's theorem). In particular this shows that GM is not definable in FPC. By extending fixed-point logic by a suitable operator for GM we therefore obtain a logic which extends rank logics and in which all studied solvability problems are definable. This logic is worth a further study as it can uniformly express all problems from (linear) algebra that have been considered so far in the context of understanding the descriptive complexity gap between FPC and PTIME.

References

1 V. Arvind and T. C. Vijayaraghavan. Classifying problems on linear congruences and abelian permutation groups using logspace counting classes. *Comp. Compl.*, 19:57–98, 2010.
2 M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*, volume 29. Addison-Wesley, 1969.
3 A. Atserias, A. Bulatov, and A. Dawar. Affine systems of equations and counting infinitary logic. *Theoretical Computer Science*, 410:1666–1683, 2009.
4 L. Babai, E. Luks, and A. Seress. Permutation groups in NC. In *STOC '87*, page 409–420. ACM Press, 1987.
5 G. Bini and F. Flamini. *Finite Commutative Rings and Their Applications*. Kluwer Academic Publishers, 2002.
6 J-Y. 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. Generalized quantifiers and logical reducibilities. *J. Logic Comp.*, 5(2):213, 1995.
8 A. Dawar, M. Grohe, B. Holm, and B. Laubner. Logics with Rank Operators. In *LICS '09*, pages 113–122. IEEE Computer Society, 2009.
9 H.-D. Ebbinghaus and J. Flum. *Finite model theory*. Springer-Verlag, 2nd edition, 1999.
10 E. Grädel et. al. *Finite Model Theory and Its Applications*. Springer-Verlag, 2007.
11 Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. *Inf. Comput.*, 178:253–262, October 2002.
12 M. Grohe. Fixed-point logics on planar graphs. In *LICS '98*, pages 6—15, 1998.
13 M. Grohe. The quest for a logic capturing PTIME. In *LICS '08*, pages 267–271, 2008.
14 M. Grohe. Fixed-point definability and polynomial time on graph with excluded minors. In *LICS '10*, pages 179 – 188, 2010.
15 M. Grohe and J. Mariño. Definability and descriptive complexity on databases of bounded tree-width. In *ICDT '99*, volume 1540, pages 70–82. Springer-Verlag, 1999.
16 B. Holm. *Descriptive complexity of linear algebra*. PhD thesis, Univ. of Cambridge, 2010.
17 N. Immerman. Relational queries computable in polynomial time. *Inf. and Control*, 68:86–104, 1986.
18 P. Lindström. First order predicate logic with generalized quantifiers. *Theoria*, 32:186–195, 1966.
19 B. R. McDonald. *Finite rings with identity*. Dekker, 1974.
20 M. Otto. *Bounded Variable Logics and Counting — A Study in Finite Models*, volume 9 of *Lecture Notes in Logic*. Springer-Verlag, 1997.
21 W. Pakusa. Finite model theory with operators from linear algebra. Staatsexamensarbeit, RWTH Aachen University, 2010.
22 M. Y. Vardi. The complexity of relational query languages. In *STOC '82*, pages 137–146. ACM Press, 1982.