Wied Pakusa

Finite Model Theory with Operators from Linear Algebra

Contents

Introduction

"Model theory is the branch of mathematical logic which deals with the relation between a formal language and its interpretations, or models", [17]. In the classical studies of model theory, first-order logic is probably the most relevant formal language. The investigated models of interest are most typically structures of infinite cardinality. Seminal results include the theorems of Löwenheim and Skolem, the compactness, and the completeness theorem. However, with growing importance of computer science the research on properties of *finite* structures has attracted much interest. Many problems originating in computer science have elegant formalizations in the language of model theory. This connection allows the application of well-established methods from model theory in various fields like database theory, (dynamic) complexity theory, automata and formal language theory, and in the field of artificial intelligence. Unless explicitly mentioned otherwise, throughout this thesis, we are concerned with finite structures.

Finite model theory arose as the specialization of model theoretic studies to the class of finite structures. In particular, model theorists focus on questions concerning the definability of various classes of structures. However, restricted to the finite, many of the well-established tools from classical model theory fail, e.g. including both the compactness and the completeness theorem for first-order logic. For this reason, new techniques have been developed for investigating the expressive power of logics over finite structures. These rely much more on combinatorial and game theoretical arguments than the classical methods. Besides first-order logic, various kinds of fixed point logics and infinitary logics gained increasing significance in the studies of finite model theory.

One major line of research is known as *descriptive complexity theory*. In this field, one studies relationships between logical definability and algorithmic computability. The theorem of Trakhtenbrot, stating that finite satisfiability for first-order logic is undecidable, can be seen as a first result in this regard. One of the key aims is to understand to what extent classifications stemming from traditional complexity theory can be linked to model classes of formal languages. Model theorists search for logics that *correspond to* complexity classes in the following sense: A logic $\mathcal{L}$ corresponds to a complexity class $\mathcal{C}$ if each class of structures definable in $\mathcal{L}$ is decidable in complexity $\mathcal{C}$ and vice versa. The notion of *correspondence*, or more commonly *capturing*, was made precise [40], and much effort has been spent to find logics that capture prominent complexity classes. Such characterizations are very useful since they provide a machine independent view on the

complexity and the structure of the algorithmic problems. Furthermore, they give deep insights into both, the logic and the corresponding complexity class. In particular, the logical characterization allows to apply methods from finite model theory to obtain new algorithmic insights.

Until today, capturing results are known for NP and co-NP, and all levels of the polynomial time hierarchy above these classes. For example, NP is captured by the existential fragment of second-order logic. This characterization was established by Fagin [32], and probably it is the most important initial results from the field. So far, no logic has been found which captures a complexity class below the class NP. Especially, one of the main unanswered questions remains: is there a logic that captures PTIME? Gurevich conjectured that no such logic exists. It should be very hard to prove his conjecture since it implies that PTIME $\neq$ NP. On the other hand, if one refutes his conjecture, the separation of PTIME and NP reduces to the separation of two logics over the domain of finite structures. Hence, in both cases we would make progress on settling the most prominent open problem from algorithmic complexity theory. This dependency illustrates the strong connections between both areas of research.

The quest to find a logic for PTIME has yielded a broad family of new logics that have been investigated as possible candidates. Probably *fixed point logics* such as *least fixed point logic* LFP, *inflationary fixed point logic* IFP and *partial fixed point logic* PFP are most important. These logics add different concepts of recursion to first-order logic through providing fixed points of definable operators. Many properties that require a global view on the structures are undefinable in first-order logic. In contrast, such properties like alternating reachability are definable in fixed point logics. It turned out that at least on the domain of ordered structures fixed point logics such as LFP and IFP are capable of defining all PTIME-decidable properties. This fact is known as the Immerman-Vardi theorem [68, 49]. Furthermore, the logic PFP captures PSPACE on the domain of ordered structures [1]. However, for both results it is crucial that the structures come with built-in linear orders. If this is not provided, one can find simple classes which are not definable in fixed point logic, but decidable in LOGSPACE. For instance, the class of all finite structures with universes of even cardinality has this property.

The linear order is important in a special concern. If we want to consider relational structures as inputs to algorithmic machines, it is necessary to agree on a *representation scheme* of structures by finite words. However, each known encoding scheme for general structures relies on the presence of some linear order over the universe. In particular, if we want to encode a structure without an intrinsic ordering, we first have to choose some arbitrary one. As a consequence, we only consider *order invariant queries*, i.e. algorithmic problems whose outcome is independent of the concrete order chosen for the encoding.

We proceed to explain for which reasons the linear order is vital to the aforementioned capturing results. First of all, linearly ordered structures are *rigid*, which means that

they do not possess any nontrivial automorphisms. Beyond that, if an ordering on the universe is given, first-order logic is capable of defining an order on each fixed power of the universe. This order can be engaged to obtain data structures which are used for simulating algorithms by logical formulas. Moreover, assumed we have agreed on a representation scheme, in the presence of a linear order the encoding of the structure is unique and first-order definable. These two insights are normally the central components of proofs showing that a logic captures a special complexity class.

Besides fixed point recursion, another well-studied approach is to enrich first-order logic by operators which compute different kinds of *transitive closure*. The most fundamental logics in this concern are given by the extensions of first-order logic by operators for *deterministic transitive closure* FO+DTC, for *symmetric transitive closure* FO+STC and for normal *transitive closure* FO+TC. Restricted again to the domain of ordered structures, FO+DTC captures LOGSPACE, FO+STC captures SLOGSPACE and FO+TC captures NLOGSPACE [50]. Hence, separating FO+DTC and FO+TC on the domain of ordered structures means to separate LOGSPACE from NLOGSPACE. Note however that on arbitrary finite structures the logics were separated [36].

Locality is inherent to first-order definable queries [30] and in particular first-order logic lacks a mechanism of recursion. As we have discussed, this defect is tackled by fixed point logics and logics with operators for various kinds of transitive closure. Beyond that, on arbitrary finite structures, a fundamental shortcoming of most familiar logics is the lack of even simple counting mechanisms. Consequently, commonly cited classes which are undefinable in fixed point logics are often based on counting properties. As mentioned above, the class of structures having a universe of even cardinality is contained in LOGSPACE, but it cannot be defined in any of the aforementioned logics.

For this reason, Immerman [49] proposed to extend logics by counting quantifiers. Least fixed point logic with counting seemed to be a promising candidate for a logic capturing polynomial time, until Immerman refuted his own proposal a short time later. In their famous work [16] Cai et al. presented a class of graphs which is decidable in PTIME, but not definable in fixed point logic with counting. It turned out that the methodical foundations of their proof can be engaged to obtain further classes which are undefinable in FP+C, cf. [7, 23, 41, 44]. Vital to their approach is the embedding of FP+C into the finite variable fragment of infinitary logic extended by counting quantifiers $\mathsf{C}^{\omega}_{\infty\omega}$. Logical equivalence with respect to the k-variable fragment of $\mathsf{C}^{\omega}_{\infty\omega}$, denoted by $\mathsf{C}^{k}_{\infty\omega}$, is captured by a *model comparison game* in the style of the classical Ehrenfeucht and Fraïssé games. These *pebble games* have been successfully used for establishing undefinability results and structural hierarchies for many logics.

In some sense, the query of Cai et al. can be identified as an abstract counting property as well. However, the ingenious part of their construction constitute highly symmetric graph gadgets which successfully prevent definability in FP+C. Although very elegant, for

a long time it seemed as if their class is somewhat artificial. Surprisingly, recent results by Atserias et al. [7] and Dawar et al. [27] revealed that their construction is strongly entangled with the very natural problem of deciding solvability of linear equation systems. Atserias et al. and Dawar et al. were not only able to show that FP+C is unable to express solvability of linear systems, but also that the query of Cai et al. can be reduced to this problem. As a consequence, they proposed to extend fixed point logic with operators that are able to determine the rank of definable matrices over finite fields. These rank operators reveal themselves as a natural generalization of the usual counting mechanisms available in FP+C. Rather than counting elements in definable relations, rank operators enable to determine the dimension of definable vector spaces. Inflationary fixed point logic extended by rank operators appears to be very powerful, and so far no examples are known yielding a separation from PTIME.

This situation motivates to investigate various operators from linear algebra as extensions for logics. Noteworthy, it turns out that many queries of linear algebra are already definable in FP+C. This includes matrix problems as multiplication, inversion, determinant or singularity [12, 7, 27]. In the logical setting, matrices are encoded as relations over the universe of structures. Thus, in general they are defined over *unordered* sets. As a consequence, we are only interested in matrix queries which are independent of the special ordering of rows and columns. For instance, questioning whether a matrix is in row echelon form is not possible for unordered matrices. In contrast, matrix rank over fields is well-defined since it is invariant against permutations of rows and columns.

This thesis reviews and broadens the achieved results concerning the relevance of linear algebra in descriptive complexity theory. The intrinsic complexity of most problems of linear algebra crucially depends on the kind of algebraic domain they are given over. For instance, computing the determinant of a matrix with entries in the two-element field $\mathbb{F}_2$ is equivalent to the problem of deciding singularity; a connection which clearly fails if we consider matrices over larger fields. The question whether a linear equation system has a solution can be formulated as a simple equality involving the matrix rank over fields. Recall that a linear equation system $A \cdot \bar{x} = b$ over a field is solvable iff $rk(A) = rk(A|b)$. By our knowledge, a similar characterization is not known for more general domains, e.g. finite rings. The results of Atserias et al. [7] demonstrate that solvability of linear equation systems cannot be defined in FP+C no matter which finite abelian group one chooses as the underlying domain. It is commonplace that this query is decidable in PTIME. Hence, decreasing the gap between FP+C and PTIME requires to analyze logical extensions which are at least able to define this query over all finite abelian groups.

We proceed to illustrate the starting points for the following investigations. So far, most research in the area has focused on problems of linear algebra defined over finite fields, although the present results suggest to widen the scope of algebra in descriptive complexity theory. We propose to generalize the point of view by taking commutative

rings as algebraic structures into account. Each abelian group can be embedded into a commutative ring and of course any field is a commutative ring as well. On the other hand, the intuitive meaning of matrix rank, as a numerical parameter, is hard to understand with respect to its structural meaning. Known examples which demonstrate the power of rank operators are actually based on linear equation systems. Thus, it seems reasonable to study the descriptive power of linear systems in its own right. Recent studies in algorithmic complexity theory also focus on the classifications of problems of linear algebra, see e.g. [6, 51, 3, 35, 46, 47]. In particular, it is known that solvability of linear equation systems can be decided in PTIME for any finite ring. Our hope is that there are other equivalent concepts whose structural meanings are more transparent.

With these considerations in mind, we analyze operators and problems of linear algebra defined over arbitrary finite commutative rings. First of all, for many queries from linear algebra we prove that known definability results for FP+C remain valid over finite rings. We investigate extensions of FP+C by new operators from linear algebra and present examples illustrating their expressive power. Figuring out relations for different kinds of underlying rings remains a steady issue throughout this thesis. For instance, take two fields of different characteristic and consider in each case the problem of deciding solvability of linear equation systems. As we will see, it seems unlikely that these two problems are equivalent in the view of descriptive complexity theory. Anyhow, for the case of linear equation systems, we establish a simple complete class of finite commutative rings. Moreover, we contrast different concepts to enrich FP+C with operators from linear algebra. Especially, we relate extensions by operators which decide solvability of linear systems, similarity or equivalence of matrices and the rank of definable matrices. By engaging ideas from algorithmic complexity theory and algebra we order the resulting extensions with respect to their expressive power.

Outline

In Chapter 1 we recall some preliminaries from the relevant areas of logic, descriptive complexity theory, combinatorics and linear algebra. Chapter 2 explores capabilities and limitations of FP+C with respect to queries of linear algebra. First of all, we agree in Section 2.1 on a uniform way to encode (unordered) matrices over arbitrary finite rings in a structural setting. In the following Sections 2.2, 2.3 and 2.4, we review results identifying a remarkable amount of problems of linear algebra which are expressible in FP+C. This includes queries like (iterated) matrix multiplication, singularity, determinant, characteristic and minimal polynomial. We are able to generalize many of the known results, i.e. we prove that they hold for matrices over arbitrary finite rings. In the case of singularity for example, we combine the existent ideas with more involved arguments from algebra. In particular, we significantly make use of decompositions of finite commutative rings. Subsequent to the positive findings, Section 2.5 reviews the fundamental result of [7] showing that solvability of linear equation systems cannot be defined in FP+C. We identify more classes sharing this property in Section 2.6. These findings motivate to analyze extensions of FP+C by various operators from linear algebra.

In Chapter 3 we study corresponding logical extensions by operators capable of deciding solvability of linear equation systems (Section 3.1), extensions by operators capable of deciding similarity and equivalence of matrices (Section 3.2), and finally extensions by operators capable of computing the rank of definable matrices (Section 3.3). The latter were already studied by Dawar et al. [27], and if we restrict to finite fields, they subsume the other extensions. However, in the general case, i.e. for extensions by operators capable of deciding the aforementioned queries over finite rings, many relations remain unclarified. In particular, we are not aware of algorithms computing the rank of matrices over arbitrary rings in polynomial time. We make some contributions towards relating the new operators for different rings, and we present a simple class of finite rings which is complete for solvability of linear equation systems in the following sense: if we solely add operators for this class of rings, we already obtain the full expressiveness of the extension by all operators. Hereafter, Section 3.4 introduces suitable infinitary logics and pebble games.

In Chapter 4 we review further results from Dawar et al. [27]. These were originally formulated for rank logics, but it turns out that the proofs directly apply for all other extensions introduced in Chapter 3. In Section 4.1 we demonstrate strictness of the arity hierarchies for the newly introduced operators from linear algebra. Furthermore, Dawar et al. proved that extensions of first-order logic by rank operators capture logspace modulo counting classes on the domain of ordered structures. In Section 4.2 we explain that this remains true for all other kinds of operators. In particular, we obtain equivalence of the affected extensions on the domain of ordered structures.

Chapter 1.

Preliminaries

This chapter briefly recalls well-known definitions and basic results from the fields of mathematical logic, finite model theory, combinatorics, and linear algebra. As a matter of fact, this chapter is mainly based on standard literature. We simultaneously fix notations, which will be used throughout this thesis. For more precise and detailed explanations we refer to [37, 55, 62].

1.1. Structures and Logics

A relational *vocabulary* or *signature* τ is a finite set $\{R_1, \ldots, R_k\}$ where each R_i is a relation symbol of arity r_i. A *τ-structure* is a tuple $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, \ldots, R_k^{\mathfrak{A}})$ such that A is a nonempty set, called the *universe* of $\mathfrak{A}$, and $R_i^{\mathfrak{A}}$ is an r_i-ary relation on A, i.e. $R_i^{\mathfrak{A}} \subseteq A^{r_i}$. Unless otherwise stated, we only consider *finite structures*, i.e. structures over a finite universe. The class of finite structures is denoted by $\mathit{fin}[\tau]$. All notions like *isomorphisms, partial isomorphisms, substructures, embeddings* etc. are defined as usual. A *(model) class* $\mathcal{C}$ of τ-structures is a subclass $\mathcal{C} \subseteq \mathit{fin}[\tau]$ that is closed under isomorphism, and a *domain* is a subclass $\mathcal{D} \subseteq \bigcup_\tau \mathit{fin}[\tau]$ such that the class $\mathcal{D}[\tau] := \mathcal{D} \cap \mathit{fin}[\tau]$ is a model class for all τ.

A *k-ary query* on a class $\mathcal{C}$ of τ-structures is a mapping Q defined on $\mathcal{C}$ such that $Q(\mathfrak{A})$ is a k-ary relation on A for all $\mathfrak{A} \in \mathcal{C}$ and Q is preserved under isomorphisms, i.e. for all $\mathfrak{A}, \mathfrak{B} \in \mathcal{C}$ and isomorphisms $h : \mathfrak{A} \xrightarrow{\sim} \mathfrak{B}$ we have $Q(\mathfrak{B}) = h(Q(\mathfrak{A}))$. Furthermore, a *Boolean query* on a class $\mathcal{C}$ is a subclass $Q \subseteq \mathcal{C}$ such that for all isomorphic $\mathfrak{A}, \mathfrak{B} \in \mathcal{C}$ we have $\mathfrak{A} \in Q$ iff $\mathfrak{B} \in Q$. We say that a k-ary query Q on a class $\mathcal{C}$ of τ-structures is definable in a logic $\mathcal{L}$ if an $\mathcal{L}$-formula $\varphi(x_1, \ldots, x_n)$ such that $Q(\mathfrak{A}) = \varphi^{\mathfrak{A}}$ for all $\mathfrak{A} \in \mathcal{C}$ exists. For a Boolean query Q on $\mathcal{C}$ we accordingly require the existence of a sentence φ with $Q = \{\mathfrak{A} \in \mathcal{C} : \mathfrak{A} \models \varphi\}$. For logics $\mathcal{L}_1$ and $\mathcal{L}_2$ we say that $\mathcal{L}_2$ is *at least as expressive as* $\mathcal{L}_1$ (on finite structures), denoted by $\mathcal{L}_1 \leq \mathcal{L}_2$, if every query on $\mathit{fin}[\tau]$ that is definable in $\mathcal{L}_1$ is also definable in $\mathcal{L}_2$. If $\mathcal{L}_1 \leq \mathcal{L}_2$ and $\mathcal{L}_2 \leq \mathcal{L}_1$, we say that the logics are *expressively equivalent* (on finite structures) and write $\mathcal{L}_1 \equiv \mathcal{L}_2$.

By $\mathsf{FO}[\tau]$ we denote *first-order logic* over the signature τ. $\mathsf{L}^{\omega}_{\infty\omega}$ denotes the finite variable fragment of *infinitary logic* $\mathsf{L}^{\infty}_{\infty\omega}$. Restricting the set of variables to $x_1, \ldots, x_k$ in formulas

of $\mathsf{L}^{\omega}_{\infty\omega}$ results in the k-variable fragment of infinitary logic, denoted by $\mathsf{L}^{k}_{\infty\omega}$. Similarly, the extension of $\mathsf{L}^{\omega}_{\infty\omega}$ by counting quantifiers $\exists^{\geq i}$, for all $i \in \omega$, denoted by $\mathsf{C}^{\omega}_{\infty\omega}$, has a k-variable fragment $\mathsf{C}^{k}_{\infty\omega}$. If we augment first-order logic with the capability to compute least fixed points of monotone definable operators, we obtain the well-studied fixed point logic LFP. Another important fixed point logic is IFP, whereat *inflationary fixed points* take the place of least fixed points. In fixed point logics, usually second order variables are used to define operators. However, for queries we restrict to formulas without free second order variables. It is known that $\mathsf{LFP} \equiv \mathsf{IFP} \leq \mathsf{L}^{\omega}_{\infty\omega}$, cf. [53]. Furthermore, *simultaneous inflationary fixed points* expressed by systems of definable operators can be translated into pure LFP formulas. We simply write FP for the fixed point logic that extends IFP and is capable to handle fixed points for systems of operators. As pointed out, for every formula in FP there is an equivalent formula in LFP. For further details and for definitions of other occurring logics as *second-order logic* SO, different transitive closure logics $\mathsf{FO{+}DTC}$, $\mathsf{FO{+}STC}$, $\mathsf{FO{+}TC}$, *partial fixed point logic* PFP, and so on, we refer to the introductory cited literature.

FO, FP and even $\mathsf{L}^{\omega}_{\infty\omega}$ lacks the possibility to define very simple counting queries, as e.g. deciding whether the cardinality of the universe is even. Hence, Immerman proposed extensions fixing this shortcoming [49]. The two most basics are *first-order logic with counting* $\mathsf{FO{+}C}$ and *fixed point logic with counting* $\mathsf{FP{+}C}$. These logics are two-sorted, meaning that terms and variables are typed with respect to two different sorts. Those terms and variables of the first sort are the usual ones, i.e. they range over the universe of the model. Objects of the second sort are interpreted by values from the arithmetic $\mathfrak{N} = (\omega, +, \cdot, \leq, 0, 1)$. Both types are linked through *counting terms*. In order to formally define the semantics for these logics, we have to extend our (one-sorted) models $\mathfrak{A}$ to auxiliary two-sorted structures $\mathfrak{A}^{+}$.

Definition 1.1.1. To any one-sorted structure $\mathfrak{A} \in \mathit{fin}[\tau]$ we associate the extended two-sorted structure $\mathfrak{A}^{+} := \mathfrak{A} \cup (\omega, +, \cdot, \leq, 0, 1)$, i.e. the disjoint union of $\mathfrak{A}$ with the standard arithmetic.

In two-sorted logics we use Latin letters x,y,z,... to denote variables ranging over the universe (the first sort) and Greek letters $\lambda, \mu, \nu, \ldots$ for variables ranging over the *numerical domain* (the second sort).

Full first-order logic on structures $\mathfrak{A}^{+}$ is undecidable. For this reason, we require that each occurring numerical variable is bounded by a specific term. In this way, numerical variables can only take values which are polynomially bounded in the size of the input structure. Hence, we obtain logics whose data complexity is contained in PTIME.

Definition 1.1.2. Let $\mathcal{L}$ be one of aforementioned logics. Then $\mathcal{L}^+$ is the associated two-sorted logic evaluated in extended models $\mathfrak{A}^+$ with the restriction that each occurrence of a numeric variable in formulas (either quantified or in the range of a second-order variable during a fixed point process) is bounded by a numeric term.

Let $\mathsf{FO}{+}\mathsf{C}$ denote *first-order logic with counting*, i.e. the extension of FO^+ resulting from the closure under *counting terms*. The counting terms are formed according to the following rule: for each formula $\varphi(x) \in \mathsf{FO}{+}\mathsf{C}$ where x is a free variable of the first sort, a counting term is given by $\#x\varphi(x)$. For a model $\mathfrak{A}$ the value of this term interpreted in $\mathfrak{A}$ is the number of different elements $a \in A$ that satisfy $\mathfrak{A} \models \varphi(a)$. The set of free variables of the term is determined by $\mathit{free}(\varphi) \setminus \{x\}$.

For *(inflationary) fixed point logic with counting*, denoted by $\mathsf{FP}{+}\mathsf{C}$, we further add the capability of defining inflationary fixed points as well. As in the case of FP^+, fixed points can be defined for operators of mixed type. To be more precise, suppose that $\psi(R,\bar{x},\bar{\mu})$ is a formula of vocabulary $\tau \cup \{R\}$, where $\bar{x} = x_1 \dots x_k$, $\bar{\mu} = \mu_1 \dots \mu_l$ and R is a second-order variable of mixed arity (k,l). This means that R is required to be interpreted by sets $R \subseteq A^k \times \omega^l$. Given a tuple $\bar{t} = t_1 \dots t_l$ of numeric terms that are supposed to bound the value of variables in $\bar{\mu}$, and a $k+l$ tuple $(\bar{u},\bar{\nu})$ of appropriate terms,

$$\Big[\mathbf{ifp}\, R\bar{x}\bar{\mu}_{\leq \bar{t}} \,.\, \psi(R,\bar{x},\bar{\mu})\Big]\,(\bar{u},\bar{\nu})$$

is a formula in $\mathsf{FP}{+}\mathsf{C}$ of vocabulary τ. The semantics are defined in the usual way.

A general comment is in place regarding the notion of queries. For all kinds of numeric two-sorted logics we only consider formulas without free numeric variables for this purpose. This convention allows a meaningful comparison of expressive power with respect to usual one-sorted logics. It is a well-known fact that $\mathsf{FP} \leq \mathsf{L}^{\omega}_{\infty\omega}$, and one can similarly show $\mathsf{FP}{+}\mathsf{C} \leq \mathsf{C}^{\omega}_{\infty\omega}$, cf. [39]. Both relationships are of great importance since certain model comparison games in the style of Ehrenfeucht and Fraïssé are known to capture logical equivalence in these infinitary logics, cf. Section 1.3.

We recall the notion of *logical interpretations* for a logic $\mathcal{L}$. The underlying idea is similar to many-one reductions known from complexity theory. Intuitively, an interpretation logically defines new structures out of given ones. In particular, the new structures may be structures over some different vocabulary. Stated otherwise, interpretations define a mapping transforming one structure into another via logically definable operations.

The syntactic part of an $\mathcal{L}$-interpretation is a sequence of $\mathcal{L}$-formulas. These formulas define the new structures out of the given ones via their evaluations. The crucial point is that many relevant logics $\mathcal{L}$ have convenient closure properties with respect to interpretations. Given an $\mathcal{L}$-interpretation, one can translate each sentence stating facts about the interpreted structures into an *equivalent* sentence which refers to the original structures. We assume in the following let $\mathcal{L}$ be one of the logics FO, $\mathsf{L}^{\omega}_{\infty\omega}$, $\mathsf{C}^{\omega}_{\infty\omega}$, FP or $\mathsf{FP}{+}\mathsf{C}$.

Definition 1.1.3. Let σ, τ be two vocabularies. Assume $\tau = \{R_1, \ldots, R_m\}$ where each R_i has arity r_i. A *k-dimensional $\mathcal{L}[\sigma,\tau]$-interpretation* $\mathcal{I}$ is given by a sequence of formulas in $\mathcal{L}[\sigma]$ consisting of

- $\delta(\bar{x})$, called the *domain formula*,
- $\varepsilon(\bar{x}, \bar{y})$, called the *equality formula*, and,
- for every relation symbol $R_i \in \tau$, a formula $\varphi_i(\bar{x}_1, \ldots, \bar{x}_{r_i})$.

Here $\bar{x}, \bar{y}, \bar{x}_i$ are disjoint tuples of k pairwise distinct first-order variables. Formulas defining the interpretation $\mathcal{I}$ may contain additional free first-order variables $\bar{z}$, called the *parameters* of $\mathcal{I}$.

Let $\mathcal{I}(\bar{z}) = \langle \delta, \varepsilon, (\varphi_R)_{R\in\tau} \rangle$ be a k-dimensional $\mathcal{L}[\sigma,\tau]$-interpretation with parameters $\bar{z}$. Let $\mathfrak{A}$ be a σ-structure with elements $\bar{c} \in A$ which are designated as an assignment for the parameters of $\mathcal{I}$. Whenever the binary relation $\varepsilon^{\mathfrak{A}}(\bar{c})$ is a congruence on the τ-structure $(\delta^{\mathfrak{A}}(\bar{c}),(\varphi_R^{\mathfrak{A}}(\bar{c}))_{R\in\tau})$, we denote with $\mathcal{I}(\mathfrak{A},\bar{c})$ the corresponding quotient structure. We can translate each formula $\psi \in \mathcal{L}[\tau]$ into a formula $\psi^{\mathcal{I}} \in \mathcal{L}[\sigma]$ by standard syntactic manipulations, e.g. by replacing each first-order variable by k-tuples of new ones, by relativizing quantifiers $Q\bar{x}$ to $\delta(\bar{x})$, by substituting equalities $\bar{x} = \bar{y}$ by $\varepsilon(\bar{x},\bar{y})$, and by replacing atomic formulas $R(\bar{x}_1, \ldots, \bar{x}_i)$ by $\varphi_R(\bar{x}_1, \ldots, \bar{x}_i)$.

Lemma 1.1.4. $(\mathfrak{A},\bar{c}) \models \psi^{\mathcal{I}}$ *iff* $\mathcal{I}(\mathfrak{A},\bar{c}) \models \psi$.

If we omit the specification of δ or ε in an interpretation $\mathcal{I}$, then we tacitly assume that they are trivial, meaning that $\delta(\bar{x})$ is valid or $\varepsilon(\bar{x},\bar{y})$ is equivalent to $\bar{x} = \bar{y}$, respectively.

1.2. Descriptive Complexity Theory

The field of descriptive complexity is concerned with relationships between the classical theory of algorithmic resources and the expressive power of logics. A central goal is to understand to what extent algorithmic complexity classes correspond to structural classes defined by sentences of different logics. In the following we formalize the notion of a logic that *captures* a complexity class.

Definition 1.2.1. For any vocabulary τ let $\tau_<$ be the extension by a new binary relation symbol $< \notin \tau$. The class of *ordered* τ-structures, $ord[\tau]$, is defined as

$$ord[\tau] := \{(\mathfrak{A}, <) \in fin[\tau_<] : \mathfrak{A} \in fin[\tau] \text{ and } < \text{ is a linear order on } A\}.$$

For any vocabulary we fix a natural *encoding scheme* that associates with any ordered structure $(\mathfrak{A}, <) \in \mathit{ord}[\tau]$ a finite string $\langle \mathfrak{A}, < \rangle \in \{0,1\}^\star$, see e.g. [37]. This scheme makes it possible to encode structures by finite words. For any class $\mathcal{C} \subseteq \mathit{fin}[\tau]$ we define the *machine representation* of $\mathcal{C}$, denoted by $\langle \mathcal{C} \rangle$, as

$$\langle \mathcal{C} \rangle := \{\langle \mathfrak{A}, < \rangle : \mathfrak{A} \in \mathcal{C} \text{ and } < \text{ is a linear order on } A\}.$$

With this preparation it makes sense to ask whether a class of finite structures is contained in a complexity class like NP or PTIME. On the other hand, we can assign the class consisting of corresponding word structures to each set of finite words. In this way we establish a direct correspondence between the class of relational finite structures and the class of languages over the finite alphabet $\{0,1\}$.

Definition 1.2.2. Let $\mathcal{L}$ be a logic, Comp a complexity class and $\mathcal{D}$ a domain of finite structures. We say that $\mathcal{L}$ *(effectively) captures* Comp *on* $\mathcal{D}$ if

(1) there is a computable function that associates with each sentence ψ in $\mathcal{L}[\tau]$ an algorithm M, which witnesses that $\{\mathfrak{A} \in \mathcal{D}[\tau] : \mathfrak{A} \models \psi\} \in \mathsf{Comp}$, and

(2) for every model class $\mathcal{C} \subseteq \mathcal{D}[\tau]$ whose membership problem is in Comp, there exists a sentence $\psi \in \mathcal{L}[\tau]$ such that $\mathcal{C} = \{\mathfrak{A} \in \mathcal{D}[\tau] : \mathfrak{A} \models \psi\}$.

If we do not explicitly specify the domain, we are concerned with the domain of *all* finite structures. Moreover, if the logic $\mathcal{L}$ satisfies condition (1) on the domain of all finite structures, we write $\mathcal{L} \leq \mathsf{Comp}$. If on the other hand condition (2) is satisfied, we write $\mathsf{Comp} \leq \mathcal{L}$. Consequently, if $\mathcal{L}$ captures Comp on the domain of all finite structures, the appropriate notation is $\mathcal{L} = \mathsf{Comp}$. We summarize important capturing results for the well-known complexity classes. The *domain of ordered structures* is the union over all model classes $\mathit{ord}[\tau]$.

Theorem 1.2.3.

(i) (Fagin) Existential SO *captures* NP *(on the domain of all finite structures).*

(ii) (Immerman) FO+DTC *captures* LOGSPACE *on ordered structures.*

(iii) (Immerman) FO+TC *captures* NLOGSPACE *on ordered structures.*

(iv) (Immerman, Vardi) FP *captures* PTIME *on ordered structures.*

(v) (Abiteboul, Vianu, Vardi) PFP *captures* PSPACE *on ordered structures.*

That FP+C $\leq$ PTIME is easy to see, and through the famous result of Cai et al. [16] we know that FP+C $\lneq$ PTIME. In particular, the availability of a linear order is crucial to the capturing results stated in the above theorem. In fact they fail on the domain of finite structures. It is one of the major open problems if there is a logic that captures PTIME. Remarkably, Dawar [22] showed that in the case there is a logic capturing PTIME, then there is also a natural one, i.e. an extension of FO by an uniform sequence of generalized Lindström quantifiers. On the other hand, if one can prove that no logic captures PTIME, this result would imply PTIME $\neq$ NP, since NP is captured by the existential fragment of second order logic.

1.3. Graphs, Logics and Games

Directed graphs are $\{E\}$-structures $\mathcal{G} = (V,E)$, where E is a binary relation, and *undirected graphs* are directed graphs with a symmetric edge relation E and without selfloops. If we speak of *graphs* only, then we usually refer to undirected graphs. For a comprehensive introduction into basic and more involved concepts of graph theory we refer to [28].

In this thesis we consider the notion of *treewidth* for undirected graphs. This measure of graph complexity has attracted much attention. One of the reasons for its importance is, that many NP-hard graph problems (and even some PSPACE-hard ones) become tractable on classes of graphs with bounded treewidth [13]. Treewidth can be characterized in various equivalent ways. We provide an algebraic and a game theoretic approach, which are probably the two best-known ones.

Definition 1.3.1. Let $\mathcal{G} = (V, E)$ be an undirected graph. A *tree decomposition of* $\mathcal{G}$ is an undirected tree $\mathcal{T} = (T, E_T)$ where T is a family of subsets of V, i.e. $T \subseteq \mathcal{P}(V)$ and

(a) $\bigcup T = V$, and

(b) for all $(u,v) \in E$ there is some $X \in T$ so that $\{u,v\} \subseteq X$, and

(c) for every vertex $v \in V$ the set $\{X \in T : v \in X\}$ is connected in $\mathcal{T}$.

Nodes in the tree $\mathcal{T}$ are called *bags* as they intuitively collect vertices of the graph $\mathcal{G}$. The *width* of the tree decomposition $\mathcal{T} = (T, E_T)$ is $(\max\{|X| : X \in T\} - 1)$, and the *treewidth of* $\mathcal{G}$, denoted by $tw(\mathcal{G})$, is defined to be the minimal width for which a tree decomposition of $\mathcal{G}$ exists.

Seymour and Thomas [64] established a game characterizing the notion of treewidth. The *cops and robber game* with k cops over $\mathcal{G}$ is played by two players, player I (the cops) and player II (the robber). Here, k is a parameter of the game. The rules are as follows: the cops possess k pebbles which they can place on vertices of the graph. The robber

has one pebble which is moved through the graph via edges. In each move the cops first choose a pebble. This pebble is either currently not placed on a vertex of the graph, or it is removed from its current position w. Afterwards, but in the same move, the cops determine a vertex v as the new position for their pebble. Then, the robber moves his pebble along some path to a new vertex, which may also be the previous one. The chosen path has to be cop-free, whereas the vertices v and w count as cop-free for the actual turn. The cops win a play iff they can reach a position in which the robber cannot move anymore. All other plays, i.e. precisely all infinite ones, are won by the robber.

Seymour and Thomas proved that a graph $\mathcal{G}$ has treewidth k iff the cops have a winning strategy in the game with $k+1$ pebbles, but the robber wins the game if the cops are limited to k pebbles.

Another instance in which games have been successfully applied is *model comparison*. We are interested in games capturing logical equivalence for $\mathsf{L}^k_{\infty\omega}$ and $\mathsf{C}^k_{\infty\omega}$ in particular. In the style of classical *Ehrenfeucht and Fraïssé games*, they are played by two players, Spoiler and Duplicator, on two relational structures $\mathfrak{A}$ and $\mathfrak{B}$. The *k-pebble bijection game* captures logical equivalence for $\mathsf{C}^k_{\infty\omega}$. After its introduction we point out necessary changes for obtaining the appropriate game for the logic $\mathsf{L}^k_{\infty\omega}$.

There are k pairs of corresponding pebbles $(x_1,y_1),\ldots,(x_k,y_k)$ which can be placed on elements in A and B, respectively. Formally, the positions are partial mappings $h : \{1,\ldots,k\} \to A\times B$. The initial position is $h=\emptyset$ when no pebbles are on the structures yet. Let the current position be h. In each move, Spoiler first chooses a pair i of corresponding pebbles. Duplicator has to respond with a bijection $f : A \to B$. The move ends with Spoiler placing the selected pair of pebbles on a pair of elements (a,fa). Accordingly, the new position is given by

$$h'(j) = \begin{cases} h(j), & j \neq i \\ (a,fa), & j = i. \end{cases}$$

If Duplicator cannot response to Spoilers move, or if $\mathit{range}(h')$ is not a partial isomorphism of $\mathfrak{A}$ and $\mathfrak{B}$, the game ends and she loses. She wins, if she never loses, i.e. when she can force that each play has an infinite duration. Hella [44] proved that for all $k \geq 1$ and all pairs of structures $\mathfrak{A}$ and $\mathfrak{B}$ Duplicator has a winning strategy in the k-pebble bijection game iff no sentence in $\mathsf{C}^k_{\infty\omega}$ can distinguish between $\mathfrak{A}$ and $\mathfrak{B}$.

In order to capture logical equivalence of $\mathsf{L}^k_{\infty\omega}$, the rules have to be adapted so that Duplicator becomes able to hide her bijection, i.e. Spoiler has to choose an element in A without knowing the corresponding $fa \in B$ which Duplicator will select in response.

1.4. Linear Algebra

We summarize basic definitions and results from linear algebra which are common knowledge to a large extent. More special notions are taken from the monographs [52, 59]. The set of natural numbers is denoted by ω, the field of rationals by $\mathbb{Q}$, and the ring of integers by $\mathbb{Z}$. For all $m \geq 2$ let $\mathbb{Z}_m$ be the residue ring of $\mathbb{Z}$ modulo the principal ideal $m\mathbb{Z}$. The unique finite field of characteristic p over p^n elements is denoted by $\mathbb{F}_{p^n}$.

Problems from the field of linear algebra are expressed as matrices with entries in commutative rings. These rings possess the minimum requirements for algebraic structure needed in our logical framework. For instance, in noncommutative rings it is impossible to formulate queries as *the product over a given finite set of ring elements equals one*. Throughout this thesis all considered rings are commutative and contain a neutral multiplicative, i.e. a unity.

Definition 1.4.1. Let $\mathcal{R} = (R,+,\cdot)$ be a commutative ring (with unity) and I,J two finite sets. An *(unordered) $I \times J$ matrix over $\mathcal{R}$* is a mapping $M\colon I \times J \to R$. For the matrix M we set $m_{ij} := M(i,j)$ and adapt usual notations, e.g. we write $M = (m_{ij})_{i\in I, j\in J}$.

If $|I| = 1$ we call M an *(unordered) J column (vector) over $\mathcal{R}$* and similarly if $|J| = 1$ we say that M is an *(unordered) I row (vector) over $\mathcal{R}$*. In this case we identify the domain of M with the sets J or I, respectively.

For unordered $I \times J$ matrices over a ring $\mathcal{R}$ we define matrix addition as expected. The definition of a suitable matrix product is a straightforward adaption as well. For the sake of illustration, let M be an $I \times J$, and let N be an $J \times K$ matrix over $\mathcal{R}$. We define the product matrix $M \cdot N$ to be the $I \times K$ matrix L, with

$$l_{ik} := \sum_{j\in J} m_{ij} \cdot n_{jk}, \text{ for all } i \in I, k \in K.$$

Obviously, the set of $I \times I$ matrices over $\mathcal{R}$ forms a ring with respect to matrix addition and multiplication. We skip the formal introduction of other well-known concepts like *matrices of unity*, *transposed matrices*, *matrix trace*, the *determinant* and so on, since they can also be defined for unordered matrices, mostly by straightforward adaptations of their usual formulations.

However, one has to be careful in some cases. A *square matrix* of *dimension* $n \in \omega$ is an $I \times I$ matrix for a finite set I of cardinality n. A square matrix is called *singular* if it has no inverse, or , stated equivalently, if its determinant has no inverse in $\mathcal{R}$. Note that it would also be reasonable to call an $I \times J$ matrix square whenever $|I| = |J|$. Though, this latter approach is not equivalent to the former one. Observe for instance that the determinant of an $I \times J$ matrix with $|I| = |J|$ can be defined only up to sign, whereas the determinant of an $I \times I$ matrix is determined as a unique ring element. Moreover, it is not

reasonable to talk about the trace of some $I \times J$ matrix even in the case where $|I| = |J|$. For square matrices as we have introduced them, matrix trace is perfectly defined.

In the literature other matrix properties are often considered exclusively for matrices over stronger algebras, e.g. fields. The matrix rank (in its usual definition as the dimension of the column or row space) is an important example. At the same time its notion is of central interest within this thesis. However, its common definition relies on the concept of linear dependency, which itself presupposes appropriate vector spaces containing the rows and columns of the matrix. Nevertheless, matrix rank can be generalized by considering the rows and columns of the matrix as elements in a *free module* over $\mathcal{R}$. For modules linear dependency is formalized in the same way as it is for vector spaces. Spoken informally, a module can be thought of as a vector space over a ring, though properties vary significantly. For instance, a module may not have a basis. To be more precise, a *module* $\mathcal{M}$ over the ring $\mathcal{R}$ is an algebraic structure $\mathcal{M} = (M, +, \cdot)$, where $+ : M \times M \to M$ is an addition and $\cdot : \mathcal{R} \times M \to M$ is a scalar multiplication, so that $(M,+)$ is an abelian group and for all $r, r' \in \mathcal{R}$, m,$m' \in M$ we have $1m = m$ and

(1) $r(r')m = (rr')m$, and

(2) $(r + r')m = rm + r'm$ and $r(m + m') = rm + rm'$.

The module $\mathcal{M}$ is called *free* if it is representable as a direct sum which only contains as summands the ring $\mathcal{R}$ itself.

Definition 1.4.2. Let $\mathcal{R}$ be a commutative ring with unity and let I be some finite set. The set of all I rows forms a free module $\mathcal{R}^I$ over $\mathcal{R}$, whereby addition is matrix addition and scalar multiplication is component wise ring multiplication in $\mathcal{R}$.

After this definition we are ready to introduce the concept of *matrix rank* formally. According to the preceding definition, we can decompose each $I \times J$ matrix M into a set of I row vectors or J column vectors. These are elements of the modules $\mathcal{R}^I$ or $\mathcal{R}^J$, respectively. Using this fact, we formalize *linear dependency* for rows and columns in the same way as it is done for vector spaces. We define the *row rank* and the *column rank* of M to be the size of a maximal subset of linear independent rows or columns, respectively. Unless stated otherwise, we conduct our investigations with this definition of matrix rank.

Remarkably, the notion of matrix rank over commutative rings lacks many useful properties that it possesses over fields. One can for instance find non-equivalent formulations for its notion in the literature. Especially, common criteria for solvability of linear equation systems fail or have to be reformulated. For our definition, further properties fail. The row rank, for instance, does not equal the column rank in general. To observe this,

consider the finite commutative ring $\mathcal{R} = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and the matrix

$$M = \begin{pmatrix} (1,0,0) & (0,0,1) \\ (0,1,0) & (1,0,0) \\ (0,0,1) & (0,1,0) \end{pmatrix}.$$

One can check that its columns are linear independent, whereas each row is annihilated by a single element. Hence, the column rank equals two but the row rank equals zero.

Despite that, both values are at least invariant against row and column permutations as it is required in our logical framework. We agree that within this thesis, whenever we speak of matrix rank we actually refer to the column rank. It is common place that differences between both values disappear over fields.

Theorem 1.4.3 ([59])**.** *Let A be an $I \times J$ matrix over a field $\mathcal{F}$. Then the column rank of A is equal to the row rank of A.*

Furthermore, the rank of A is also the maximal integer $t \geq 1$ so that there is a nonsingular $t \times t$ submatrix of A. We conclude that for the case $I = J$, the matrix A has full rank iff it is invertible.

Let b be an I column vector over $\mathcal{R}$. In this case the linear equation system (A,b) is solvable iff $rk(A) = rk((A|b))$.

We emphasize that the above theorem fails over rings. Actually, much research is going on about this concern. For instance, Elizarov [31] recently established a remarkable amount of necessary conditions for solvability of linear equation systems with respect to a different notion of rank and various kinds of commutative rings. More details and further approaches to matrix rank over rings can be found in the monograph [59].

Chapter 2.

Linear Algebra and Counting Logics

In this chapter we analyze the descriptive complexity of classical problems from linear algebra. In particular, we are interested in properties which are decidable in PTIME. Consequently, our focus lies on the logic FP+C, which is known to capture PTIME on a great variety of important structural classes. Grohe [38] has recently shown that FP+C captures PTIME on every class of graphs with excluded minors, e.g. on the class of all planar graphs or on each class of graphs with bounded treewidth. It turns out that many problems of linear algebra can be expressed in FP+C. Examples include iterated matrix multiplication and matrix inversion. In contrast, strongly related problems such as solvability of linear equation systems, are located in PTIME $\setminus$ FP+C. Noteworthy, from the perspective of algorithmic complexity these problems are equivalent.

Almost all problems that occur in linear algebra are questions about matrices over specific domains. Varying the underlying domain usually has crucial influence on the complexity of the given problem. Most frequently the ring of integers, the field of rationals and general finite fields are studied as important instances in the area of algorithmic complexity theory. For the case of finite domains we prefer to choose the most general framework. In consequence, we consider matrices defined over finite commutative rings. In Section 2.1, we first agree on a uniform encoding by finite structures. Equipped with this representation scheme, Section 2.2 starts to explore basic queries for which an FP+C definition, based on simple matrix arithmetic, exists. We extend many of the known results for the case of matrices over finite rings. Sections 2.3 and 2.4 establish FP+C definitions for the characteristic and the minimal polynomial. We infer definability results for the matrix inverse, the adjugate and the determinant of a matrix.

In contrast to the positive results, Section 2.5 gives reasons why one of the most classical problems of linear algebra, namely deciding solvability of linear equation systems, cannot be defined in FP+C. To get a clearer view on the structural properties of this problem and to derive a deeper understanding of its descriptive complexity, Section 2.6 establishes a collection of different classes which reduce to solvability of linear equation systems via first-order interpretations.

2.1. Encoding Matrices over Different Domains

We introduce the technical framework for encoding matrices as relations in finite structures. This way we can talk about problems from linear algebra in a logical setting. Actually, all relevant problems from linear algebra are representable by appropriate matrices. Relevant *numerical* logics, such as e.g. FP+C, are interpreted over extended two-sorted structures $\mathfrak{A}^+$, which include an ordered numerical domain (cf. Section 1.1). As a matter of fact, our discussion comprises the usage of numerical elements in matrix encodings. If we define queries, we either assume that structures are equipped with an intrinsic numerical domain, or we stick to an encoding which does not make use of numerical elements.

According to Definition 1.4.1, unordered matrices are defined as a mapping over the Cartesian product of two finite sets. In order to index the rows and the columns of a matrix, our encoding scheme makes use of elements (or even tuples of elements) from the universe of the underlying structure. Since we deal with arbitrary finite structures, we agree that such sets are not linearly ordered in any intrinsic way. Hence we stick to the notion of *unordered* matrices in general, and we only consider properties of, or operations on matrices which are invariant under row and column permutations. This includes matrix singularity, matrix multiplication, matrix determinant and matrix rank for instance.

Our encoding is strongly based on methods used in [12, 27, 24]. As we are concerned with *finite* model theory, our main interest manifests in matrices taking entries in *finite* rings. Nevertheless, we also prepare ways for dealing with matrices over $\mathbb{Z}$ and $\mathbb{Q}$. The main idea can be illustrated as follows: Let $\mathcal{G} = (V,E)$ be a finite graph. We consider its *adjacency matrix* $M_{\mathcal{G}}$ as an unordered matrix over the two-element field $\mathbb{F}_2$. Formally it is given as the (unordered) $V \times V$ matrix $M_{\mathcal{G}}$ over $\mathbb{F}_2$ which is defined by

$$M_{\mathcal{G}}(a,b) = \begin{cases} 0, & (a,b) \notin E, \\ 1, & (a,b) \in E. \end{cases}$$

In this sense the finite graph $\mathcal{G}$ *encodes* the matrix $M_{\mathcal{G}}$. The same considerations apply to formulas. Let $\varphi(u,v)$ be a formula in some logic $\mathcal{L}$ of vocabulary τ. We assume that its free variables are among the first-order variables u and v. For any τ-structure $\mathfrak{A}$ the formula φ defines a graph over A via its expansion, i.e. the graph $(A, \varphi^{\mathfrak{A}})$. This means that φ also defines an $A \times A$ matrix $M_{\varphi}^{\mathfrak{A}}$ over $\mathbb{F}_2$, which is the adjacency matrix associated to the graph $(A, \varphi^{\mathfrak{A}})$.

Our aim is to generalize this basic idea in two concerns. First of all, we extend the encoding for the representation of matrices defined over arbitrary finite rings $\mathcal{R}$. The adjacency matrix of a graph can also be regarded as a matrix over the ring $\mathcal{R}$ with the agreement that its entries are the elements $0,1 \in \mathcal{R}$. The problem is that we are still restricted to matrices with only two different entries.

The obvious solution is to enhance the vocabularies. We use designated relation symbols for all single elements in the ring $\mathcal{R}$. Assume for instance that we want to encode a matrix over the four-element field $\mathbb{F}_4$. Usually this field is constructed as $\mathbb{F}_2[z]/(z^2+z+1)$. According to this definition we denote its elements by $0, 1, z, z+1$. Recall how field operations are defined for this representation, e.g. $z \cdot (z+1) = 1$ and $1 + (z+1) = z$. We fix τ as the vocabulary containing three binary relation symbols E_1, E_z, E_{z+1} and consider a τ-structure $\mathfrak{A}$. Each of the three restrictions of $\mathfrak{A}$ to one of its single relations is a graph with vertex set A. The associated adjacency matrices have entries 0,1 $\in \mathbb{F}_4$. Let $M_1^{\mathfrak{A}}$, $M_z^{\mathfrak{A}}$, and $M_{z+1}^{\mathfrak{A}}$ denote these matrices. By composing the three adjacency matrices with their corresponding ring elements we finally arrive at the $A \times A$ matrix $M^{\mathfrak{A}}$ over $\mathbb{F}_4$ which is the matrix encoded by $\mathfrak{A}$:

$$M^{\mathfrak{A}}(a,b) := M_1^{\mathfrak{A}}(a,b) + z \cdot M_z^{\mathfrak{A}}(a,b) + (z+1) \cdot M_{z+1}^{\mathfrak{A}}(a,b).$$

In exactly the same manner, sequences of formulas $\varphi_1(u,v), \varphi_z(u,v), \varphi_{z+1}(u,v)$ define matrices over $\mathbb{F}_4$ in every structure interpreting them. As previously mentioned, we consider a further generalization of the matrix representation. In Chapter 3 we investigate various logical extensions by operators from linear algebra. These operators express properties of definable matrices. To obtain sensible logics which are e.g. closed with respect to logical interpretations, it is reasonable to include operators of *unbounded arity*. It is even necessary, as Section 4.1 demonstrates. Consequently, these operators decide properties of matrices which are defined over *tuples* of elements. We speak of matrices having *dimension* (k,l) if their rows and columns are indexed by tuples of length k and l, respectively. Up to this point we have only considered matrices of dimension (1,1). Assume we want to encode a matrix over $\mathbb{F}_4$ of dimension (1,2), i.e. we have single elements to index the rows, and tuples of length two that index the columns. We declare three ternary relation symbols E_1, E_z and E_{z+1} to form a vocabulary τ. Let $\mathfrak{A}$ be a τ-structure. By identifying the ternary relations in $\mathfrak{A}$ as binary relations over the set $A \cup A^2$, we obtain an extended version of adjacency matrices. For $\star \in \{1, z, z+1\}$, we set

$$M_\star^{\mathfrak{A}}(a,bc) = \begin{cases} 0, & \text{if } (a,b,c) \notin E_\star^{\mathfrak{A}} \\ 1, & \text{if } (a,b,c) \in E_\star^{\mathfrak{A}}. \end{cases}$$

Accordingly, $\mathfrak{A}$ encodes the $A \times A^2$ matrix $M^{\mathfrak{A}}$ over $\mathbb{F}_4$ defined as

$$M^{\mathfrak{A}}(a,bc) := M_1^{\mathfrak{A}}(a,bc) + z \cdot M_z^{\mathfrak{A}}(a,bc) + (z+1) \cdot M_{z+1}^{\mathfrak{A}}(a,bc).$$

In the same way a sequence of formulas $\varphi_1(u,vw), \varphi_z(u,vw), \varphi_{z+1}(u,vw)$ gives rise to a matrix over $\mathbb{F}_4$ of dimension (1,2) in every structure via expansion. We define the illustrated encodings more formally. To abbreviate the set of possible matrix dimensions, we define for integers $s \geq 2$

$$\hat{s} = \{(v,w) : v,w \geq 1, v + w = s\}.$$

Finite Rings Our first concern is to introduce a uniform encoding appropriate for general finite rings $\mathcal{R}$. Let $s \geq 2$ and let $(v,w) \in \hat{s}$ be a matrix dimension. We fix an enumeration of the ring elements of $\mathcal{R}$ as $a_1, \ldots, a_k$ and a signature $\tau_{\mathcal{R}}^{v,w}$, which consists of designated relation symbols $M_{a_i}^{\mathcal{R},v,w}$ where each is of arity s.

Let $\mathfrak{A}$ be a $\tau_{\mathcal{R}}^{v,w}$-structure. For tuples $\bar{a} \in A^v, \bar{b} \in A^w$ choose $I \subseteq \{1, \ldots, k\}$ as the smallest set satisfying that whenever $i \notin I$ then $\mathfrak{A} \not\models M_{a_i}^{\mathcal{R},v,w}(\bar{a},\bar{b})$. Thus, I is the set of indices $1 \leq i \leq k$ for which the ring element $a_i \in \mathcal{R}$ has to be considered when obtaining the matrix entry at position $(\bar{a},\bar{b})$.

Use the set I to define the element $\mathcal{R}[\mathfrak{A},\bar{a},\bar{b}] := \sum_{i \in I} a_i \in \mathcal{R}$. That way each finite structure $\mathfrak{A}$ of signature $\tau_{\mathcal{R}}^{v,w}$ encodes an $A^v \times A^w$ matrix over $\mathcal{R}$, denoted by $M_{\mathfrak{A}}$:

$$M_{\mathfrak{A}}(\bar{a}, \bar{b}) := \mathcal{R}[\mathfrak{A},\bar{a},\bar{b}].$$

In the same manner we proceed for formulas: let $\varphi = (\varphi_{a_i}(x_1^i, \ldots, x_s^i))_{1 \leq i \leq k}$ be a sequence of τ-formulas in some logic $\mathcal{L}$ and let its free variables be among the first-order variables $x_1^1, \ldots, x_s^k$. In any τ-structure $\mathfrak{A}$ and for any dimension $(v,w) \in \hat{s}$, the formula sequence φ encodes an $A^v \times A^w$ matrix over $\mathcal{R}$. This matrix $M_{\mathfrak{A}}^{\varphi}$ is defined through the expansion of φ in $\mathfrak{A}$, i.e. it is the matrix encoded by the structure

$$(A, (\varphi_{a_i}^{\mathfrak{A}})_{1 \leq i \leq k}) \in \mathit{fin}[\tau_{\mathcal{R}}^{v,w}].$$

To emphasize that φ should represent a matrix of dimension $(v,w) \in \hat{s}$, we notate

$$\left(\varphi_{a_i}(x_1^i, \ldots, x_s^i)\right)_{1 \leq i \leq k} = \left(\varphi_{a_i}(x_1^i \cdots x_v^i, x_{v+1}^i \cdots x_s^i)\right)_{1 \leq i \leq k}.$$

The presented encoding was also used by Dawar and Holm [24] and implicitly in [7]. It does not rely on numeric elements and it is applicable for all finite rings.

If we deal with logics interpreted over extended structures $\mathfrak{A}^+$, like e.g. $\mathsf{FP{+}C}$, we can make the representation of ring elements more explicit by identifying them with an initial segment of the natural numbers. Following this approach, ring elements are, in a certain sense, available in the structures itself, meaning that they can be identified with values of numerical terms. As a matter of fact, matrices become definable by single numerical terms. Using FO^+-interpretations, one can easily switch between both encodings. We omit technical details for the general case in order to avoid overburdening the notation.

In the special case of quotient rings $\mathbb{Z}_m$ however, this encoding is more natural than the generic one. This is because the addition and multiplication available in the arithmetic of the extended structures can directly be engaged as ring addition and multiplication for the ring itself: we only have to reduce results modulo m. By this means, matrix definitions become more compact and readable. Dawar et al. [27] introduced this encoding for prime fields $\mathbb{F}_p$ but it is convenient for the general case, i.e. for arbitrary $m \geq 2$. In this encoding we also use numerical elements to index rows and columns.

Quotient Rings over the Integers Assume $m \geq 2$, $s \geq 2$, and a matrix dimension $(v,w) \in \hat{s}$ are given. Let τ be a vocabulary and let $\chi(\bar{v})$ be a numeric τ-term defined in some logic $\mathcal{L}$, like e.g. FO^+ or $\mathsf{FP}{+}\mathsf{C}$, which is interpreted in extended structures $\mathfrak{A}^+$. Its free variables should be among the first-order variables $\bar{v}$. We require $|\bar{v}| = s$ and allow each first-order variable to be typed, i.e. each variable can range over the universe or the numeric domain of the two-sorted models.

Let $\bar{v} = x_1 \dots x_l \eta_{l+1} \dots \eta_v y_1 \dots y_k \nu_{k+1} \dots \nu_w$, where all the x_i, y_i are universe variables and the η_i, ν_i are ranging over the arithmetic. According to our convention from Section 1.1, we require numeric variables to be bounded by a numeric term. Let $\bar{t}_\eta$ and $\bar{t}_\nu$ be tuples of numeric terms designated to bound the variables in $\bar{\eta}$ and $\bar{\nu}$, respectively. We indicate that we have agreed on this setting by writing $\chi(\bar{v}) = \chi(\bar{x}\bar{\eta}_{\leq \bar{t}_\eta}, \bar{y}\bar{\nu}_{\leq \bar{t}_\nu})$.

In a given τ-structure $\mathfrak{A}$ the term $\chi(\bar{v})$ defines a matrix as follows: Rows are indexed by tuples in $A^l \times \omega^{v-l}$ and columns by tuples from $A^k \times \omega^{w-k}$, whereby the numeric components in the tuples are bounded by the values of the terms $\bar{t}_\eta$ and $\bar{t}_\nu$ in $\mathfrak{A}$. The entries of the matrix are the values of $\chi(\bar{v})$ modulo m interpreted in $\mathfrak{A}$ at a given position. To be precise, let $\bar{q} = (q_{l+1}, \dots, q_v) \in \omega^{v-l}$ and $\bar{r} = (r_{k+1}, \dots, r_w) \in \omega^{w-k}$ be the unique tuples of natural numbers satisfying $\mathfrak{A} \models \bar{t}_\eta = \bar{q}$ and $\mathfrak{A} \models \bar{t}_\nu = \bar{r}$, respectively. We set

$$Q := \{(n_{l+1}, \dots, n_v) \in \omega^{v-l} \,:\, n_i \leq q_i \text{ for } l+1 \leq i \leq v\}, \text{ and}$$
$$R := \{(n_{k+1}, \dots, n_w) \in \omega^{w-k} \,:\, n_i \leq r_i, \text{ for } k+1 \leq i \leq w\}.$$

Then $\chi(\bar{v})$ defines in $\mathfrak{A}$ the $(A^l \times Q) \times (A^k \times R)$ matrix $M^\chi_\mathfrak{A}$ over the ring $\mathbb{Z}_m$, defined by

$$M^\chi_\mathfrak{A}(\bar{a}\bar{n},\bar{b}\bar{m}) := \chi^\mathfrak{A}(\bar{a}\bar{n}\bar{b}\bar{m}) \mod m, \text{ for } (\bar{a},\bar{n}) \in A^l \times Q, (\bar{b},\bar{m}) \in A^k \times R.$$

The usage of numeric variables makes the encoding incomparable with the generic one. If we abandon this option, it is easy to give FO^+-interpretations which translate one encoding into the other. We tacitly switch between them whenever it seems useful.

Integers and Rationals Finally, we want to discuss possibilities to handle matrices with entries in $\mathbb{Q}$ and therewith in $\mathbb{Z}$. In contrast to finite rings, each encoding based on a finite set of relation symbols or formulas is not meaningful. Actually, each set of matrices over $\mathbb{Q}$ whose entries form a finite set of rationals can be encoded in this way. However, neither would this technique lead to a uniform representation for matrices over the rationals nor would it assure closure under logical definability of simple operations like, e.g. matrix addition or multiplication.

We consider structures that include an ordered numerical domain as a second sort. Either this arithmetic is inherent to the structure itself, or it is available due to dealing with numerical logics. The obvious idea is to use a numeric term for defining matrices over $\mathbb{Z}$ and two numeric terms (numerator and denominator) to define matrices over $\mathbb{Q}$.

However, in the logics we are interested in the size of matrix entries would be polynomially bounded with respect to the cardinality of the universe. To avoid this restriction, Blass et al. proposed to represent entries of integer matrices by their binary expansions [12]. We introduce their setting for rational matrices, see also [27].

By handling numerators and denominators of entries separately it suffices to deal with integer matrices since a matrix over $\mathbb{Q}$ can be expressed by two matrices over $\mathbb{Z}$. So let $\varphi(\bar{x},\bar{y},\nu_{\leq t})$ be a formula in some logic $\mathcal{L}$ over a signature τ which is interpreted in extended two-sorted structures $\mathfrak{A}^+$. Let the set of free variables in φ be among the first-order (universe) variables $\bar{x}$ and $\bar{y}$ and the numeric variable ν. We assume that ν is bounded by a numeric term t and choose $s \geq 2$ such that $(|\bar{x}|,|\bar{y}|) = (v,w) \in \hat{s}$. Let $\mathfrak{A}$ be some τ-structure. For tuples $\bar{a} \in A^v, \bar{b} \in A^w$ let the set $C[\mathfrak{A},\bar{a},\bar{b}]$ be defined as

$$C[\mathfrak{A},\bar{a},\bar{b}] := \{\gamma \in \omega \,:\, \gamma < t^{\mathfrak{A}},\, \mathfrak{A} \models \varphi(\bar{a},\bar{b},\gamma)\}.$$

The set $C[\mathfrak{A},\bar{a},\bar{b}]$ collects those natural numbers γ for which the coefficient of 2^γ in the binary expansion for the matrix entry at position $(\bar{x},\bar{y})$ should be one. The sign of this entry is encoded by the value $t^{\mathfrak{A}}$. Accordingly, we declare φ to encode the $A^v \times A^w$ matrix $M^\varphi_{\mathfrak{A}}$ over $\mathbb{Z}$ defined by

$$M^\varphi_{\mathfrak{A}}(\bar{a},\bar{b}) := \left(\sum_{\gamma \in C[\mathfrak{A},\bar{a},\bar{b}]} 2^\gamma\right) \cdot \begin{cases} -1, & \text{if } \mathfrak{A} \models \varphi(\bar{a},\bar{b},t^{\mathfrak{A}}) \\ 1, & \text{else.} \end{cases}$$

The arithmetic, or the numerical domain, allows us to represent integer matrices which have entries of exponential size (measured in the cardinality of the universe). Once again we stress that in queries the numerical domain has to be inherent to the structures itself.

Finally, we present a normal form for the uniform encoding. Consider a finite ring $\mathcal{R}$ for which we have agreed on an enumeration of the ring elements as $a_1, \ldots, a_k$. Let $(\varphi_{a_i}(x_1,\ldots,x_s))_{1\leq i\leq k}$ be a sequence of formulas in some logic $\mathcal{L}$ which encode a matrix. Let further $\mathcal{L}$ be closed under first-order operations. It is a simple observation that there is an equivalent encoding $(\psi_{a_i}(x_1,\ldots,x_s))_{1\leq i\leq k}$ with the following *uniqueness property*: there is precisely one $1 \leq i \leq k$ so that $\mathfrak{A} \models \psi_{a_i}(\bar{a})$ for all structure $\mathfrak{A}$ and tuples $\bar{a} \in A$. This is because for all $a_i \in R$ there are only finitely many different ways to generate a_i as a sum out of the other elements due to the finiteness of $\mathcal{R}$.

2.2. Simple Matrix Arithmetic

In this section we study fundamental queries related to simple matrix arithmetic. This includes operations like matrix addition, matrix multiplication and the trace of a square matrix. We argue that fixed point logics can define iterative versions of these operations,

and we explain how these basic results can be exploited to derive logical descriptions of more sophisticated problems as singularity of matrices.

We start with matrix addition: clearly this operation can be handled even in FO for any finite ring. Consider the case of matrices over $\mathbb{Q}$. They are represented by binary expansions of numerators and denominators. If a logic allows fixed point recursion over the numerical sort, we can define addition of two rationals given their binary expansions, since so every polynomial time property over the ordered numerical domain of the structure is definable.

Proposition 2.2.1. *Matrix addition over finite rings and $\mathbb{Q}$ can be defined in* FP+C.

In contrast to matrix addition, the logical definability of matrix multiplication is slightly more involved. Let A be an $I \times J$ matrix and B an $J \times K$ matrix. In order to determine the entries of $A \cdot B$, one has to sum up products of the form $a_{ij} \cdot b_{jk}$. The single products can obviously be handled like in the case of matrix addition. The difficulty manifests in the summation over the whole set. The straightforward approach of summing up the products one after the other is not definable in any logic, since this would require an order on the index sets. Blass et al. [12] solved this problem for $\mathbb{F}_2$. Generalizing their idea proves that matrix multiplication can be defined for any finite ring in FP+C.

Theorem 2.2.2. *Let $\mathcal{R} = (R, +, \cdot)$ be a finite ring, τ a vocabulary and let two sequences of τ-formulas $(\varphi_a(\bar{x},\bar{y}))_{a\in R}$ and $(\psi_a(\bar{y},\bar{z}))_{a\in R}$ of* FP+C *be given. Then there is a sequence of* FP+C*-formulas $(\vartheta_a(\bar{x},\bar{z}))_{a\in R}$ such that for all structures $\mathfrak{A}$ we have $M^{\vartheta}_{\mathfrak{A}} = M^{\varphi}_{\mathfrak{A}} \cdot M^{\psi}_{\mathfrak{A}}$.*

Proof. For each $a \in R$ we find a numeric term $\chi_a(\bar{x},\bar{z})$ which takes for tuples $\bar{a},\bar{c} \in A$ in a structure $\mathfrak{A}$ the following value: $\chi^{\mathfrak{A}}(\bar{a},\bar{c})$ is the multiplicity of the element a appearing as a summand in the calculation for the entry $(M^{\varphi}_{\mathfrak{A}} \cdot M^{\psi}_{\mathfrak{A}})(\bar{a},\bar{c})$.

The crucial point is that in a finite ring each element induces a finite cyclic subgroup with respect to ring addition. From elementary group theory we know that this subgroup is isomorphic to $(\mathbb{Z}_k,+)$ for some $k \leq |R|$. Thus, we can assume that each of the numeric terms $\chi_a(\bar{x},\bar{z})$ takes values bounded by $|R|$, namely by reducing their values modulo the appropriate k. We are left with a constant number of different tuples $(\chi^{\mathfrak{A}}_a(\bar{a},\bar{c}))_{a\in R}$ which can be handled easily. □

We proceed with the discussion of matrices over $\mathbb{Q}$ and corresponding properties definable in FP+C. In particular, we can omit technical details concerning polynomial time arithmetic of rationals in binary representation. Assume that two logical definitions of matrices over $\mathbb{Q}$ are given by sequences of FP+C-formulas $(\varphi_n(\bar{x},\bar{y},\nu_{\leq s^{\varphi}}),\varphi_d(\bar{x},\bar{y},\nu_{\leq t^{\varphi}}))$ and $(\psi_n(\bar{y},\bar{z},\nu_{\leq s^{\psi}}),\psi_d(\bar{y},\bar{z},\nu_{\leq t^{\psi}}))$. In order to simplify the argumentation, it is convenient to reduce this problem to a problem for matrices over $\mathbb{Z}$. One can define in FP+C (the binary expansion of) the product of all integers with the following property: the binary

expansion has a length smaller than the value of the term $\max(t^\varphi, t^\psi)$, and the integer is at the same time present as a denominator of one of the matrix entries. Hence, also the matrices resulting by scalar multiplication with this integer can be defined in FP+C from the ones given. Both resulting definitions encode matrices over $\mathbb{Z}$. As we will see, the matrix product of two matrices over $\mathbb{Z}$ is FP+C definable and so is the product of the original matrix by restoring the denominator as the square of the integer defined before. Considering these explanations we agree that it is sufficient to deal with matrices over $\mathbb{Z}$.

Let $\varphi(\bar{x},\bar{y},\nu_{\leq t})$ and $\psi(\bar{y},\bar{z},\nu_{\leq s})$ be two formulas. We reuse the idea of Theorem 2.2.2, i.e. we apply the counting mechanism from FP+C to find a numeric term $\chi(\bar{x},\bar{z},\nu)$ such that for all structures $\mathfrak{A}$ and $\bar{a},\bar{c} \in A$ we have

$$(M^\varphi_\mathfrak{A} \cdot M^\psi_\mathfrak{A})(\bar{a},\bar{c}) = \sum_{\gamma \leq \max(t,s)^\mathfrak{A}} \chi^\mathfrak{A}(\bar{a},\bar{c},\gamma) \cdot 2^\gamma. \tag{2.2.1}$$

The length of the binary encodings of entries in the product matrix can be bounded by the numeric term $r := (\sharp x(x = x) + t + s)$. Thus, we conclude that there is an FP+C formula $\vartheta(\bar{x},\bar{z},\nu_{\leq r})$ defining the same matrix as $\chi(\bar{x},\bar{z},\nu)$ but in the usual binary encoding.

Theorem 2.2.3 ([27])**.** *The product of* FP+C *definable matrices over* $\mathbb{Q}$ *is again an* FP+C *definable matrix over* $\mathbb{Q}$*.*

A closely related problem concerns raising a definable matrix to a non-constant power. This power may be given as a numeric term χ. Since the problem directly reduces to iterated matrix multiplication, the previous results indicate that FP+C is able to express matrix powering via fixed point recursion. Provided that the matrix has entries in some finite ring $\mathcal{R} = (R,+,\cdot)$, we can easily follow this way. If its entries are elements in $\mathbb{Q}$ or $\mathbb{Z}$, we have to ensure the existence of an appropriate numeric term which bounds the length of the binary expansions corresponding to entries in the resulting matrix. For illustration, consider an FP+C matrix encoding over $\mathbb{Z}$, i.e. an FP+C-formula $\varphi(\bar{x},\bar{y},\nu_{\leq t})$. One easily verifies that it suffices to choose $[(|\bar{y}| \cdot (\chi - 1)) \cdot \log(\text{card}) + t \cdot \chi]$, where $\text{card} := \sharp x(x = x)$.

Corollary 2.2.4. *Given an* FP+C *representation of a (square) matrix over some finite ring* $\mathcal{R}$ *or over* $\mathbb{Q}$ *and a numeric term* χ*, one can find an* FP+C *formula encoding the* χ*-power of the given matrix.*

Blass et al. [12] investigated the same problem for powers that are even exponential in the size of the input structure. Again, these powers are defined by an FP+C formula in their binary expansions. Using the well-known method of *repeated squaring* they established an FP+C definition for this query. Based on this result they proved that over finite fields singularity of matrices is definable in FP+C. We sketch the main ideas and extend them along the way to handle even matrices over arbitrary finite rings.

Let $\mathcal{R}$ be a finite ring and I some finite set. Denote by $\mathrm{GL}_I(\mathcal{R})$ the set of all $I \times I$ matrices M over $\mathcal{R}$ so that $det(M)$ is invertible in $\mathcal{R}$. It is common knowledge that this set forms a group with respect to matrix multiplication, which is known as the *general linear group over* $\mathcal{R}$. The crucial point is to gain knowledge about the cardinality of this group, which clearly depends on $|I|$. Note that an $I \times I$ matrix M is nonsingular iff $M^{|\mathrm{GL}_I(\mathcal{R})|} = 1$, which is a direct consequence of Lagrange's Theorem. We require an important result from commutative ring theory which can be found in [10]. A ring is called *local* if it contains exactly one maximal ideal, e.g. each field is a local ring. For more details on local rings we refer to [33].

Theorem 2.2.5. *Let $\mathcal{R} = (R, +, \cdot)$ be a finite commutative ring and I a finite set.*

Then there is a unique decomposition of $\mathcal{R}$ as a direct sum of local rings. In fact if $P_1, \ldots, P_m$ is a list of all prime ideals in $\mathcal{R}$, then there exists $t \geq 1$ such that

$$\mathcal{R} \cong (\mathcal{R}/P_1^t) \oplus \cdots \oplus (\mathcal{R}/P_m^t).$$

Furthermore, we have $\mathrm{GL}_I(\mathcal{R}) \cong \mathrm{GL}_I(\mathcal{R}/P_1^t) \oplus \cdots \oplus \mathrm{GL}_I(\mathcal{R}/P_m^t)$.

Thus, it suffices to analyze the cardinality of $\mathrm{GL}_I(\mathcal{R})$ for local rings $\mathcal{R}$. The next result is formulated as an exercise in [59].

Theorem 2.2.6. *Let $\mathcal{R} = (R, +, \cdot)$ be a local finite commutative ring with the unique maximal ideal m and let I be a finite set. We denote the field $\mathcal{R}/m$ by $\mathcal{F}$ and its cardinality by $k := |\mathcal{F}|$. Then we have*

$$|\mathrm{GL}_I(\mathcal{F})| = k^{|I|^2} \cdot \prod_{i=0}^{|I|-1} (1 - k^{i-|I|}) \quad \text{and} \quad |\mathrm{GL}_I(\mathcal{R})| = |R|^{|I|^2} \cdot \prod_{i=0}^{|I|-1} (1 - k^{i-|I|}).$$

Proof. The first equation can be explained as follows: Since $\mathcal{F}$ is a field, an $I \times I$ matrix over $\mathcal{F}$ is invertible iff its columns are linearly independent. Each set of i linearly independent column vectors gives rise to k^i different linear combinations which can be generated. Thus, there remain $(k^{|I|} - k^i)$ many possible columns which are independent of the given ones. This counting argument shows that

$$\begin{aligned} |\mathrm{GL}_I(\mathcal{F})| &= (k^{|I|} - 1) \cdot (k^{|I|} - k) \cdot (k^{|I|} - k^2) \cdots (k^{|I|} - k^{|I|-1}) \\ &= \prod_{i=0}^{|I|-1} (k^{|I|} - k^i) = \prod_{i=0}^{|I|-1} k^{|I|}(1 - k^{i-|I|}) = k^{|I|^2} \prod_{i=0}^{|I|-1} (1 - k^{i-|I|}). \end{aligned}$$

Now consider the canonical surjective group homomorphism $\pi : \mathrm{GL}_I(\mathcal{R}) \to \mathrm{GL}_I(\mathcal{F})$. There are $|m|^{|I|^2}$ different $I \times I$ matrices over $(1 - m)$, hence $|\ker(\pi)| = |m|^{|I|^2}$. The fundamental homomorphism theorem implies

$$\frac{|\mathrm{GL}_I(\mathcal{R})|}{|m|^{|I|^2}} = |\mathrm{GL}_I(\mathcal{F})|,$$

which proves the second claim since $|\mathcal{F}| \cdot |m| = |R|$. □

Let an FP+C matrix encoding over some finite ring $\mathcal{R} = (R, +, \cdot)$ be given, i.e. a sequence of FP+C-formulas $(\varphi_a(\bar{x},\bar{y}))_{a\in R}$ such that $|\bar{x}| = |\bar{y}| =: s$. The aforementioned theorems assert that there is an FP+C formula $\eta(\nu)$ and a numeric term t such that for all structures $\mathfrak{A}$ the evaluation $\eta^{\mathfrak{A}}(\nu_{\leq t})$ determines the binary expansion of $|\mathrm{GL}_{A^s}(\mathcal{R})|$. Furthermore, by using the technique of repeated squaring and e.g. a simultaneous fixed point definition, one can show that there are FP+C formulas $(\psi_a(\bar{x},\bar{y},\mu_{\leq t}))_{a\in R}$ so that for all structures $\mathfrak{A}$ and $c \leq t^{\mathfrak{A}}$ we have $M_{\mathfrak{A}}^{\psi(c,\cdot,\cdot)} = (M_{\mathfrak{A}}^{\varphi})^{2^c}$. Combining these two facts establishes the desired existence of FP+C formulas, say $(\vartheta_a(\bar{x},\bar{y},\mu_{\leq t}))_{a\in R}$, with

$$M_{\mathfrak{A}}^{\vartheta} = (M_{\mathfrak{A}}^{\varphi})^{|\mathrm{GL}_{A^s}(\mathcal{R})|}.$$

This procedure is clearly applicable for other integers than $|\mathrm{GL}_{A^s}(\mathcal{R})|$ whose binary representation is definable in FP+C in the indicated sense. Especially, we can define the inverse of a matrix in $\mathrm{GL}_{A^s}(\mathcal{R})$ simply by taking it to the power $|\mathrm{GL}_{A^s}(\mathcal{R})| - 1$. The following theorem summarizes the achieved results.

Theorem 2.2.7. *Let an* FP+C *matrix encoding over a finite ring* $\mathcal{R} = (R, +, \cdot)$ *be given as* $(\varphi_a(\bar{x},\bar{y}))_{a\in R}$ *where* $|\bar{x}| = |\bar{y}|$. *Further let* $\eta(\nu_{\leq t})$ *be an* FP+C *formula defining in each structure* $\mathfrak{A}$ *a natural number* $k_{\mathfrak{A}}$ *via its binary expansion. Then one can find* FP+C *formulas* $(\psi_a(\bar{x},\bar{y}))_{a\in R}$ *such that* $M_{\mathfrak{A}}^{\psi} = (M_{\mathfrak{A}}^{\varphi})^{k_{\mathfrak{A}}}$ *for all structures* $\mathfrak{A}$.

Moreover, there is a sequence of FP+C *formulas* $(\vartheta_a(\bar{x},\bar{y}))_{a\in R}$ *so that for all* $\mathfrak{A}$ *we have* $M_{\mathfrak{A}}^{\vartheta} = 0$ *whenever* $M_{\mathfrak{A}}^{\vartheta} \notin \mathrm{GL}_{A^s}(\mathcal{R})$ *and* $M_{\mathfrak{A}}^{\varphi} \cdot M_{\mathfrak{A}}^{\vartheta} = 1$ *otherwise.*

The approach for matrix inversion used above is not applicable for matrices over $\mathbb{Q}$ or $\mathbb{Z}$, since their general linear groups are infinite. Anyhow, there is a way to define the inverse of matrices in these cases. This will be discussed in Section 2.3.

We add a short remark concerning matrix traces. For each matrix it is possible to define the matrix containing only its diagonal. This can be achieved by rewriting each single formula $\varphi(\bar{x},\bar{y})$ in a given representation into the formula $\bar{x} = \bar{y} \wedge \varphi(\bar{x},\bar{y})$. Hence, it is possible to define the trace as this reduces to matrix multiplication of the diagonal matrix and the matrix filled with ones.

Proposition 2.2.8. *Given an* FP+C *representation of a (square) matrix over a finite ring* $\mathcal{R}$ *or over* $\mathbb{Q}$, *one can find* FP+C *formulas encoding the trace of the matrix.*

Another relevant query in this context is the class of *nilpotent* matrices. An $I \times I$ matrix A is nilpotent if there is an $m \in \omega$ such that $A^m = 0$. Let $n = |I|$. For matrices A that are defined over fields one can show that A is nilpotent iff $A^n = 0$. Hence, FP+C is capable to define nilpotency of matrices over fields. The same is true for matrices over $\mathbb{Z}$, and moreover there is an interesting connection to graph theory in this case. Consider A

as being the adjacency matrix over $\mathbb{Z}$ of some directed graph $\mathcal{G}$. It is an easy observation that the entries in A^m correspond to the total number of different ways connecting two vertices in $\mathcal{G}$. For this reason, the matrix A is nilpotent iff the graph $\mathcal{G}$ is acyclic. This equivalence fails if we consider nilpotency over rings of finite characteristic.

2.3. Characteristic Polynomial and Determinant

We investigate definabilty of the characteristic polynomial in FP+C. In particular, we can establish FP+C-formulas for many other notions like the determinant or the inverse from a definition of this polynomial. We first recall its definition. Let A be an $I \times I$ matrix over a commutative ring $\mathcal{R}$, where $n := |I|$. The *characteristic polynomial of* A, denoted by $\chi_A \in \mathcal{R}[X]$, is given by the identity $\chi_A = \det(XE_I - A)$, where E_I denotes the $I \times I$ identity matrix over $\mathcal{R}$ and X is an indeterminate. The following theorem summarizes some useful facts about this polynomial.

Theorem 2.3.1. *Let A be an $I \times I$ matrix over a commutative ring $\mathcal{R}$, where $n := |I|$ and let $\chi_A(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$. Then we have $\chi_A(A) = 0$ by the theorem of* Cayley-Hamilton.

Furthermore, for all $1 \leq i \leq n$ the coefficient a_i is given as $(-1)^i$ times the sum over determinants of all principal submatrices of dimension i. In particular, it follows that $a_n = (-1)^n det(A)$ and $a_1 = -tr(A)$.

Theorem 2.3.1 implies that an FP+C definition of the characteristic polynomial provides FP+C formulas defining the inverse, the adjugate, the trace and the determinant of a matrix. In this sense knowledge about the characteristic polynomial is very profitable. In a first step we show that an FP+C definition of the characteristic polynomial is possible whenever the matrix has entries in $\mathbb{Z}$ or $\mathbb{Q}$.

The underlying idea is due to Rossman [11] who also showed how to proceed for matrices over finite fields. He suggested the application of a well-known parallel algorithm developed by Csanky [21]. Following his approach, Dawar et al. [27] showed that the algorithm can also be formulated in FP+C.

The main advantage of Csanky's algorithm is its applicability in the logical setting. This is due to the fact that no matrix manipulations or calculations are involved which require a systematic treatment of arbitrary big submatrices. In contrast, compare Csanky's algorithm e.g. to the algorithm of Berkowitz [8, 69]. However, the algorithm has also its disadvantages, mainly manifested in the application of divisions. For this reason a generalization which allows to handle matrices over arbitrary finite rings is hard to establish. The algorithm itself is applicable for rings $\mathcal{R}$ in which division by $|I|!$ is possible. In our framework the size of the matrix depends on the size of the finite structure encoding it, thus it seems that we can only handle rings with characteristic zero. But as already

pointed out, in some cases there are ways to circumvent this restriction. We explore these cases systematically after the treatment for matrices over $\mathbb{Z}$ and $\mathbb{Q}$. Csanky's algorithm is based on the following fact.

Theorem 2.3.2 ([59])**.** *Let A be an $I \times I$ matrix over a ring $\mathcal{R}$ in which division by $|I|!$ is possible, and assume $\chi_A(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$, where $n = |I|$.*

Then $a_1 = -tr(A)$, $a_n = (-1)^n det(A)$ and for $2 \leq k \leq n$ we have

$$\begin{aligned} a_k &= (-1)^k \frac{1}{k} \left[a_{k-1} tr(A) + a_{k-2} tr(A^2) + \cdots + a_1 tr(A^{k-1}) + tr(A^k) \right] \\ &= (-1)^k \frac{1}{k} \sum_{i=1}^{k} a_{k-i} tr(A^i). \end{aligned}$$

Thus, the task of determining the coefficients of the characteristic polynomial can be reduced to find traces of all matrix powers up to $|I|$ combined with some easy polynomial time calculations in the ring. Corollary 2.2.4 and Proposition 2.2.8 show that the first task can be handled in FP+C. For matrices over $\mathbb{Q}$ the remaining calculations can be carried out over the numerical domain and thus be defined in FP+C. This proves the following theorem.

Theorem 2.3.3. *Given an* FP+C *representation of a (square) matrix over $\mathbb{Z}$ or over $\mathbb{Q}$ one can find* FP+C *formulas encoding the characteristic polynomial of the matrix. In particular one obtains* FP+C *formulas defining its determinant, inverse and adjugate.*

The question remains how to proceed for matrices having their entries in some finite ring. As already pointed out we are unable to answer this question in general yet. Recall from Theorem 2.2.5 that any finite (commutative) ring is the direct sum of local rings. As a consequence, we can constrain our observations to local rings. For special kinds of local rings we are able to adapt Csanky's algorithm.

First of all let $p \geq 2$ be a prime, $e \geq 1$ and let $\mathbb{Z}_{p^e}$ be the local ring of residue classes of integers modulo p^e. Consider the canonical ring epimorphism $\pi : \mathbb{Z} \to \mathbb{Z}_{p^e}$. This epimorphism allows to transfer all calculations formulated for the ring $\mathbb{Z}_{p^e}$ into corresponding calculations carried out in the ring $\mathbb{Z}$. Afterwards it is possible to coherently restore the proper result in $\mathbb{Z}_{p^e}$ by engaging π again. Since the coefficients of the characteristic polynomial can be obtained solely by means of both ring operations, we are able to proceed as follows: Given a matrix over $\mathbb{Z}_{p^e}$, switch to the canonical matrix over $\mathbb{Z}$. Now determine the coefficients of the characteristic polynomial of this matrix and reduce the results again according to π. In this way one obtains the characteristic polynomial of the original matrix. It is clear that all described steps can be defined in FP+C.

The foregoing considerations include the case of all prime fields. We switch to arbitrary finite fields at this point. Such fields are given by $\mathbb{Z}_p[X]/(f)$ where $p \geq 2$ is a prime and

$f \in \mathbb{Z}_p[X]$ is a monic irreducible polynomial. The canonical epimorphism $\pi : \mathbb{Z} \to \mathbb{Z}_p$ extends to an epimorphism $\pi : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ via reduction of coefficients. If we choose a monic polynomial $g \in \pi^{-1}(f)$ we obtain an epimorphism $\sigma : \mathbb{Z}[X]/(g) \to \mathbb{Z}_p[X]/(f)$ by setting $\sigma(p + (g)) = \pi(p) + (f)$. To see that σ is well defined note that for any polynomial $h \in \mathbb{Z}[X]$ we have $g \mid h$ iff $f \mid \pi(h)$. Thus, we can follow the same lines as above, i.e. given a matrix over an arbitrary finite field, switch to a matrix over $\mathbb{Z}[X]/(g)$, determine its characteristic polynomial, and reduce the result again via σ to obtain the desired polynomial of the original matrix. We can work in $\mathbb{Z}[X]$ due to the canonical epimorphism $\mathbb{Z}[X] \to \mathbb{Z}[X]/(g)$ too.

However, the only infinite domains yet considered were $\mathbb{Z}$ and $\mathbb{Q}$. So we still have to argue that the established results concerning FP+C definability can be transferred to the case of matrices over $\mathbb{Z}[X]$. Since we want to use Csanky's algorithm over $\mathbb{Z}[X]$, this primarily includes definability results for powers of matrices and their traces. To avoid overburdening the notation we skip a formal introduction of an encoding for such matrices. Actually it should be clear that polynomials in $\mathbb{Q}[X]$ can be encoded by FP+C formulas if they have a degree which is polynomially bounded in the size of the structure. For example we could just list the binary expansions of their coefficients. Furthermore in this encoding all PTIME manipulations can be defined in FP+C.

For matrices over $\mathbb{Z}[X]/(g)$ entries can be chosen to be polynomials in $\mathbb{Z}[X]$ whose degree is bounded by the degree of f, which is a constant. Rising such a matrix to a power which is polynomially bounded in the cardinality of the structure, leads to a matrix whose entries are polynomials in $\mathbb{Z}[X]$, whose degree is polynomially bounded in the size of the input structure as well. With this knowledge and by reusing adapted ideas of Theorem 2.2.3 and Corollary 2.2.4, we can accept that FP+C is capable of defining the required objects and operations to perform Csanky's algorithm over $\mathbb{Z}[X]$. Finally, we reduce the coefficients of the resulting polynomial modulo g and afterwards modulo p. This way we obtain coefficients of the characteristic polynomial of the original matrix.

Theorem 2.3.4. *Assume we have given an* FP+C *encoding of a (square) matrix over some finite ring $\mathcal{R}$ whose unique decomposition into local rings consists of finite fields and rings $\mathbb{Z}_{p^e}$ for primes $p \geq 2$ and integers $e \geq 1$.*

Then there are FP+C *formulas encoding the characteristic polynomial of the matrix. As a consequence, there are* FP+C *formulas that define the determinant, inverse and adjugate of the given matrix.*

It remains unanswered whether the same result holds for general rings, and in particular whether FP+C is capable to define the determinant of a matrix over all finite rings. Theorem 2.2.7 states that singularity for matrices can be defined in FP+C for arbitrary finite rings. Thus, there is only a small gap that remains between *non-invertible determinant* and *determinant equals r* for some $r \in R$. We suppose that this gap can be closed.

2.4. Minimal Polynomial

In contrast to the characteristic polynomial, the minimal polynomial for matrices over commutative rings $\mathcal{R}$ is undefined. This is due to the fact that $\mathcal{R}[X]$ is not a principal ideal domain, i.e. in general the ideal in $\mathcal{R}[X]$ which contains all polynomials annihilating the matrix is not generated by a single polynomial. Furthermore, proofs showing the uniqueness of the minimal polynomial are based on the euclidean division algorithm, which naturally requires $\mathcal{R}[X]$ to be an euclidean domain. As a result, in this section we are only interested in square matrices over finite fields $\mathcal{F}$. Recall that the minimal polynomial of an $I \times I$ matrix A over the field $\mathcal{F}$ is the unique monic polynomial $\mu_A(X) \in \mathcal{F}[X]$ which has minimal degree and annihilates the matrix. To be more precise, it is the polynomial $\mu_A(X) = X^m + c_{m-1}X^{m-1} + c_{m-2}X^{m-2} + \cdots + c_1X + c_0$ so that $\mu_A(A) = 0$ and for any polynomial $p(X) \in \mathcal{F}[X]$ of degree $< m$ we have $p(A) \neq 0$. In the following, we achieve an FP+C definition of this polynomial for any matrix definable in FP+C.

The idea is to express the problem of determining its coefficients as the solution of a linear equation system [46]. Let $\vec{v}_i$ be the $|I|^2$ column vector which results if we arrange the columns of A^i among each other for $i \leq |I|$. To be precise let $\vec{v}_i$ be the $I \times I$ column defined by $\vec{v}_i(a,b) = A^i(b,a)$. With this notation we can express the coefficients of the minimal polynomial μ_A as the unique non trivial solution $(c_m,c_{m-1},\ldots,c_0)$ of the linear equation system

$$c_m\vec{v}_m + c_{m-1}\vec{v}_{m-1} + \cdots + c_1\vec{v}_1 + c_0 = 0,\ c_m = 1,$$

for the minimal $m \leq |I|$ such that a solution exists.

Suppose we have given an FP+C encoding of a (square) matrix over a field $\mathcal{F}$ which can either be finite or equal to $\mathbb{Q}$. Corollary 2.2.4 shows that it is possible to define each of the equation systems for increasing $m \leq |I|$ in FP+C using a fixed point induction. Thus, if it is possible to define solutions of these linear system in FP+C we have found an FP+C definition for the minimal polynomial. In Section 2.5 we will see that FP+C cannot define solvability of general linear equation systems. However, this behaves differently for the special kind of systems we consider here. Suppose the system is represented as a matrix with entries in $\mathcal{F}$. One observes that the columns of the corresponding matrix are indexed by elements from the numerical domain. The crucial point is that the order on the columns also defines a canonical order on the set indexing the rows of the matrix. The following theorem exploits this observation and thus describes a general method to solve linear equation systems which have this shape.

Theorem 2.4.1. *Let $(\varphi_a(\bar{x},\bar{y}))_{a\in\mathcal{F}}$ be an FP+C encoding of a matrix over some finite field $\mathcal{F}$ such that the variables in $\bar{y}$ are unexceptionally ranging over the numerical sort. Furthermore, let $(\psi_a(\bar{x}))_{a\in\mathcal{F}}$ be an FP+C representation of a column having its entries in*

the field $\mathcal{F}$. Then there is a tuple of FP+C *formulas $(\vartheta_a(\bar{y}))_{a\in\mathcal{F}}$ representing a column over $\mathcal{F}$ such that for all structures $\mathfrak{A}$*

$$M^{\vartheta}_{\mathfrak{A}} \neq 0 \text{ iff the system } M^{\varphi}_{\mathfrak{A}} \cdot \vec{x} = M^{\psi}_{\mathfrak{A}} \text{ is (non-trivial) solvable.}$$

Furthermore if $M^{\vartheta}_{\mathfrak{A}} \neq 0$, then ϑ encodes a solution for the linear system $(M^{\varphi}_{\mathfrak{A}},M^{\psi}_{\mathfrak{A}})$, i.e. $M^{\varphi}_{\mathfrak{A}} \cdot M^{\vartheta}_{\mathfrak{A}} = M^{\psi}_{\mathfrak{A}}$. The analog claim is true for linear systems over $\mathbb{Q}$.

Proof. In this setting a solution is a column which is indexed by tuples ranging over the numerical sort, i.e. we have a unique representation of each solution. In a first step we agree that the augmented matrix $(M^{\varphi}_{\mathfrak{A}}|M^{\psi}_{\mathfrak{A}})$ is given by a suitable FP+C representation which only uses numerical variables to index the columns. We switch to a matrix representation which also uses numerical variables to index the rows and in which solutions of the original linear equation systems are preserved. We claim that the order on the columns induces a total preorder on the tuples indexing the rows. Consider the lexicographic ordering given by the order on the column tuples and some order on the elements from the field. In the case of finite fields we can fix such an ordering a priori, whereas in the case of $\mathbb{Q}$ we use e.g. the natural one. The corresponding equivalence relation precisely merges tuples of elements which index identical rows in the matrix.

Of course, it does not change the solvability of the given equation system if we restrict to a matrix with exactly one representative from each of these equivalence classes. So far, we have already defined a linear order on these equivalence classes, so we can switch to a matrix indexed completely over the numerical sort and then use any polynomial time algorithm to derive a solution of the reduced linear equation system in FP+C. The claim follows since the set of solutions of the reduced and the original system coincide. □

Theorem 2.4.2. *For any* FP+C *encoding of a matrix with entries in a finite field or in $\mathbb{Q}$ there are* FP+C *formulas defining the minimal polynomial of the encoded matrix.*

It would be profitable to obtain further knowledge about the relationship between the degree of the minimal polynomial and corresponding structural graph properties. The proof of the preceding theorem shows the following: for each directed graph we can define a total preorder on tuples of vertices in FP+C whereas the width of this preorder is the degree of the minimal polynomial of the adjacency matrix. The question remains whether we can exploit this fact to define relevant graph properties.

2.5. Linear Equation Systems

For problems from linear algebra we obtained many positive results with respect to FP+C definability. At first glance it may seem that FP+C is capable of handling all relevant queries from the field. However, it will turn out that the very fundamental problem

of deciding solvability of linear equation systems is not definable in FP+C. This result remains true no matter which finite commutative ring we take as a basis. In this section we review the proof which is originally due to Atserias et al. [7]. In Section 2.6 we will make further profit of their work by identifying more undefinable problems as similarity of matrices. Altogether we establish a remarkable collection of problems from linear algebra which are all located in PTIME $\setminus$ FP+C.

The main steps are as follows: With $\mathcal{R} = (R, +, \cdot)$ we fix some finite ring and assume its universe is given by $R = \{a_1, \ldots, a_m\}$. Throughout our argumentation we are interested in cubic, i.e. 3-regular, connected graphs $\mathcal{G} = (V,E)$ which possess a sufficient amount of vertices for the ring $\mathcal{R}$, i.e. we assume $|V| > |R|$. Let $u \in V$ be a designated vertex. For each ring element $a \in R$ we define a structure $\mathcal{G}_a^u$ encoding a linear equation system over the ring $\mathcal{R}$. The construction ensures that this system has a solution iff $a = 0$. If we start with sufficiently complex graphs $\mathcal{G}$ instead, then for any $a \in R$ the structures $\mathcal{G}_a^u$ and $\mathcal{G}_0^u$ cannot be distinguished by sentences in $\mathsf{C}_{\infty\omega}^k$. The same holds for sentences of FP+C if we base the construction on a class of graphs with unbounded complexity.

According to [7] we use the notion of *treewidth* as an appropriate measure of graph complexity (cf. Section 1.3). Equation systems will frequently be identified by the structures encoding them. We first introduce the linear system $\mathcal{G}_a^u$ and then argue how to encode it as a finite structure. For convenience consider edges as undirected tuples $e = \{v,w\}$. For each vertex $v \in V$, each element $b \in R$, and each edge $e \in vE$ we define a variable $x_b^{v,e}$. Altogether we have $3|R||V|$ different variables taking values in $\mathcal{R}$. For each $v \in V \setminus \{u\}$, each set $\{e_1,e_2,e_3\} = vE$ and all $b_1,b_2,b_3 \in R$ the system $\mathcal{G}_a^u$ includes the equation

$$x_{b_1}^{v,e_1} + x_{b_2}^{v,e_2} + x_{b_3}^{v,e_3} = b_1 + b_2 + b_3. \tag{2.5.1}$$

For the designated vertex u the system contains for each set of edges $\{e_1,e_2,e_3\} = uE$ and each tuple of elements $b_1,b_2,b_3 \in R$ the equation

$$x_{b_1}^{u,e_1} + x_{b_2}^{u,e_2} + x_{b_3}^{u,e_3} = b_1 + b_2 + b_3 + a. \tag{2.5.2}$$

We stick to the convention from [7] and call these kinds of equations *vertex equations*. Furthermore, the system $\mathcal{G}_a^u$ contains *edge equations* which we include for every edge $e = \{v_1,v_2\} \in E$ and each pair $b_1, b_2 \in R$ as

$$x_{b_1}^{v_1,e} + x_{b_2}^{v_2,e} = b_1 + b_2. \tag{2.5.3}$$

The system can be represented by a corresponding coefficient matrix and a column vector. Hence, we can define it in our generic encoding, but the very special form of the system (consisting of at most three variables per equation only with coefficients 0 and 1) suggests a more economic way. We fix a vocabulary $\tau = \{E_b^r : b \in R, r = 2, 3\}$ where each relation symbol E_b^r is of arity r. We encode $\mathcal{G}_a^u$ as a τ-structure over the universe of all

variables, i.e. over $X := \{x_b^{v,e} : b \in R, v \in V, e \in E\}$. For $x,y,z \in X$ let $(x,y) \in E_b^2$ and $(x,y,z) \in E_b^3$ iff $x+y=b$ or respectively $x+y+z=b$ are equations in the linear system. We analyze the solvability of the arose system.

Lemma 2.5.1. *The equation system $\mathcal{G}_a^u$ is solvable iff $a=0$.*

Proof. One verifies that setting $x_b^{v,e} = b$ solves the equation system $\mathcal{G}_0^u$. So let $a \neq 0$ and consider the subsystem S_0 of all equations involving only variables $x_0^{v,e}$, i.e. those who have as index the element $0 \in \mathcal{R}$. If one sums up over the left hand sides of all equations in S_0 of type (2.5.1) and (2.5.2), one can pair for each edge $e=(v,w)$ the variables $x_0^{v,e}$ and $x_0^{w,e}$; in this way covering all of them. Thus, equations (2.5.3) force the total sum to equal zero. On the other hand, summing up the right hand sides of all equations of type (2.5.3) we definitely obtain a. Hence, the subsystem S_0 is not solvable. □

As pointed out, for graphs $\mathcal{G}$ which have sufficient complexity the equation systems $\mathcal{G}_0^u$ and $\mathcal{G}_a^u$ cannot be distinguished by sentences in $\mathsf{C}_{\infty\omega}^k$, i.e. $\mathsf{C}_{\infty\omega}^k$ cannot decide solvability of linear equation systems. The next lemma illustrates the structural reasons for this. The proof method is similar to one used by Cai et al. in [16] to separate FP+C from PTIME.

Lemma 2.5.2. *For every pair of vertices $u,u' \in V$ we have $\mathcal{G}_a^u \simeq \mathcal{G}_a^{u'}$.*

Proof. Recall that $\mathcal{G}$ is connected. Let $u = v_1 \xrightarrow{e_1} v_2 \xrightarrow{e_2} v_3 \xrightarrow{e_3} v_4 \cdots \xrightarrow{e_s} v_{s+1} = u'$ be a simple path in $\mathcal{G}$ connecting u and u'. We define a bijection $\eta : X \to X$ and show that it is an isomorphism between $\mathcal{G}_a^u$ and $\mathcal{G}_a^{u'}$. The intuitive idea is to move the overhang of value a which occur in equations at vertex u via the path to vertex equations corresponding to the vertex u'. We set $\eta(x_b^{v,e}) = x_b^{v,e}$ except

$$\text{for all } l \in \{1,\dots\ s\} \text{ we define } \eta(x_b^{v_l,e_l}) = x_{b+a}^{v_l,e_l} \text{ and}$$
$$\text{for all } l \in \{1,\dots,s\} \text{ we define } \eta(x_b^{v_{l+1},e_l}) = x_{b-a}^{v_l,e_l}.$$

One can check that η is a bijection. In order to show that η is an isomorphism we have to justify that all equations, i.e. relations E_b^r, are preserved. Due to η's definition this is true for all equations involving variables $x_b^{v,e}$ with $v \notin \{v_1,\dots,v_{s+1}\}$. For vertices $v_i \in \{v_2,\dots,v_s\}$ a vertex equations $x_{b_1}^{v_i,e_i} + x_{b_2}^{v_i,e_{i-1}} + x_{b_3}^{v_i,f} = b_1+b_2+b_3$ is mapped by η to the equation $x_{b_1+a}^{v_i,e_i} + x_{b_2-a}^{v_i,e_{i-1}} + x_{b_3}^{v_i,f} = b_1+b_2+b_3$. Furthermore, for the vertex u the equations $x_{b_1}^{u,e_1} + x_{b_2}^{u,f} + x_{b_3}^{u,g} = b_1+b_2+b_3+a$ are mapped to $x_{b_1+a}^{u,e_1} + x_{b_2}^{u,f} + x_{b_3}^{u,g} = b_1+b_2+b_3+a$ and similarly for the vertex u' equations $x_{b_1}^{u',e_s} + x_{b_2}^{u',f} + x_{b_3}^{u',g} = b_1+b_2+b_3$ are mapped to $x_{b_1-a}^{u',e_s} + x_{b_2}^{u',f} + x_{b_3}^{u',g} = b_1+b_2+b_3$.

In the end, we have to check that all edge equations are preserved. Again for edges which are not on the path from u to u' this is clear immediately, since η acts on all involved variables as the identity. Hence, consider any edge $e_l = \{v_l, v_{l+1}\}$. The equation

$x_{b_1}^{v_l,e_l} + x_{b_1}^{v_{l+1},e_l} = b_1 + b_2$ is mapped by η to $x_{b_1+a}^{v_l,e_l} + x_{b_1-a}^{v_{l+1},e_l} = b_1 + b_2$, which is truly an equation in $\mathcal{G}_a^{u'}$.

Altogether each equation in $\mathcal{G}_a^u$ is mapped by η to an equation in $\mathcal{G}_a^{u'}$ at which this correspondence is one-to-one. Since the total number of equations is equal in both systems the claim follows. □

Recall the rules of the cops and robber game and the rules of the k-pebble bijection game. The former is known to characterize the treewidth of a graph, whereas the latter one captures $\mathsf{C}_{\infty\omega}^k$ equivalence. Both games were introduced in Section 1.3 in detail. Let $k < tw(\mathcal{G})$. Our aim is to specify a winning strategy for Duplicator in the k-pebble bijection game played on $\mathcal{G}_a^u$ and $\mathcal{G}_0^u$ in order to prove the claimed equivalence $\mathcal{G}_a^u \equiv^{\mathsf{C}_{\infty\omega}^k} \mathcal{G}_0^u$. The crucial idea is to take advantage of a winning strategy of the robber in the cops and robber game played on $\mathcal{G}$. We prepare some additional notation which affects the choice of suitable bijections as responses to Spoiler's moves. For convenience define $\mathfrak{A} := \mathcal{G}_0^u$ and $\mathfrak{B} := \mathcal{G}_a^u$. Let X^v denote the set of variables that correspond to the vertex $v \in V$, i.e. define $X^v = \{x_b^{v,e} : b \in R, e \in vE\} \subseteq X$. Accordingly, by X^e we denote the set of variables corresponding to the edge $e \in E$.

Remember that $\mathcal{G}$ was chosen to be connected. Assume $f : \mathfrak{A} \to \mathfrak{B}$ is a bijection. We say that f is *good except at vertex* $v \in V$ if, intuitively, f acts very much like an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$, meaning that f preserves all equations except the vertex equations of vertex v. To make this intuition precise we formally require:

for all $w \in V$:	$f(X^w) = X^w$
for all $e \in E$:	$f(X^e) = X^e$
for all $x,y \in X$:	$\mathfrak{A} \models E_b^2(x,y)$ iff $\mathfrak{B} \models E_b^2(fx,fy)$
for all $x,y,z \in X \setminus X^v$:	$\mathfrak{A} \models E_b^3(x,y,z)$ iff $\mathfrak{B} \models E_b^3(fx,fy,fz)$
for all $x,y,z \in X^v$:	$\mathfrak{A} \models E_b^3(x,y,z)$ iff $\mathfrak{B} \models E_{b+a}^3(fx,fy,fz)$.

It can be said that f concentrates the differences between $\mathfrak{A}$ and $\mathfrak{B}$ in variables and equations corresponding to the vertex v. With respect to the equations of all other vertices f acts as an isomorphism. For instance, the identity bijection between $\mathfrak{A}$ and $\mathfrak{B}$ is good except at vertex u. Basically, the strategy of Duplicator in the k-pebble bijection game played on $\mathfrak{A}$ and $\mathfrak{B}$ is as follows: Duplicator always responds with a bijection that is good except at some vertex for which corresponding variables are unpebbled yet. In fact, Spoiler has to engage more than one pebble in order to uncover the differences at one vertex. Since Duplicator switches her bijection as soon as a variable for the vertex gets pebbled, she is able to hide the dissimilarity forever. The next lemma explains in which way this switching proceeds.

Lemma 2.5.3. *Let $f : \mathfrak{A} \to \mathfrak{B}$ be a bijection which is good except at some vertex v, and let $v = v_1 \xrightarrow{e_1} v_2 \xrightarrow{e_2} \cdots \xrightarrow{e_s} v_{s+1} = v'$ be a simple path in $\mathcal{G}$. Then there is a bijection $f' : \mathfrak{A} \to \mathfrak{B}$ which is good except at vertex v' and $f|_{X \setminus \bigcup_i X^{v_i}} = f'|_{X \setminus \bigcup_i X^{v_i}}$.*

Proof. The argument is similar to the proof of Lemma 2.5.2. We define $f'(x_b^{v_i,e_i}) = f(x_{b-a}^{v_i,e_i})$ and $f'(x_b^{v_{i+1},e_i}) = f(x_{b+a}^{v_i,e_i})$ for $1 \leq i \leq s$. For all remaining cases, f' is defined as f. One can verify that f' possesses the claimed properties. □

The previous lemma asserts the possibility to switch between different bijections along simple paths. The assignments for variables that correspond to vertices which are not on the path are left unchanged. We are ready to prove:

Lemma 2.5.4. *For any $k < tw(\mathcal{G})$ and any $u \in V$ we have*

$$\mathcal{G}_0^u \equiv^{\mathsf{C}^k_{\infty\omega}} \mathcal{G}_a^u.$$

Proof. We describe a winning strategy for Duplicator in the k-pebble bijection game played on $\mathfrak{A} := \mathcal{G}_0^u$ and $\mathfrak{B} := \mathcal{G}_a^u$. For this purpose we first initialize the cops and robber game played on $\mathcal{G}$ with k pebbles for the cops. We identify each of the k pairs of corresponding pebbles with one of the cops and assume that the robber makes his moves according to a fixed winning strategy. The positions in the two games are related as follows: The vertices in $\mathcal{G}$ occupied by the cops are precisely those for which a corresponding variable in X is pebbled. Furthermore, whenever the robber is at some vertex $v \in V$, then Duplicator chooses in her current move some bijection which is good except at vertex v. For convenience, we assume that the robber starts at node u, and therefore in the first round Duplicator answers with the identity bijection. Recall that this bijection is good except at vertex u. If Spoiler places the ith pair of pebbles on variables corresponding to some vertex v (the bijection guarantees that this vertex is unique), the position of the ith cop is updated.

Now, according to his winning strategy, the robber moves along a simple path to a new vertex v'. Thus, by Lemma 2.5.3, this path induces a new bijection which is good except at vertex v'. Since the robber is not allowed to a hit a cop on his way, this bijection agrees with the old one for all other variables, i.e. in particular it respects already pebbled variables. Since Duplicator can play like this forever, she has a strategy to win the game. □

Lemma 2.5.4 tells us that for any finite ring $\mathcal{R}$ the class

$$SLES(\mathcal{R}) := \{\mathfrak{A} = (A, \bar{M}, \bar{b}) \in \mathit{fin}[\tau_{\mathcal{R}}^{(1,1)} \uplus \tau_{\mathcal{R}}^{(1,0)}] \,:\, M_{\mathfrak{A}} \cdot \vec{x} = b_{\mathfrak{A}} \text{ is solvable}\},$$

cannot be defined in FP+C. A recent result of Arvind and Vijayaraghavan [5] shows that the class is contained in PTIME for any finite ring.

Theorem 2.5.5 ([7]). *For all finite rings $\mathcal{R}$ the class SLES($\mathcal{R}$) is not definable in* FP+C. *It follows that* FP+C $\subsetneq$ PTIME.

We observe that the equation systems used in the proof share some remarkable properties. Most outstanding is that every equation contains at most three different variables. This motivates the definition of the following class.

$$3\text{-}SLES(\mathcal{R}) := \{\mathfrak{A} \in SLES(\mathcal{R}) : \text{all equations in } \mathfrak{A} \text{ contain at most 3 variables}\}.$$

Theorem 2.5.6 ([7]). *For finite rings $\mathcal{R}$ the class 3-SLES($\mathcal{R}$) is not definable in* FP+C.

At this point some comments are in place concerning solvability of linear equation systems over the infinite rings $\mathbb{Z}$ and $\mathbb{Q}$. Surprisingly, for equation systems over $\mathbb{Q}$ one can show that FP+C is able to define their solvability. The argumentation is based on the following lemma.

Lemma 2.5.7 ([27], [60]). *Let M be an $I \times I$ matrix over $\mathbb{Q}$. Then we have*

$$rk(M) = rk(M^t M) = rk((M^t M)^2).$$

Furthermore, for all matrices satisfying this identity, we have that $\mathrm{rk}(M) = |I| - k$, where $k \geq 0$ is maximal such that X^k divides the characteristic polynomial χ_M of M.

Clearly, the transpose of a matrix is definable. Since matrix multiplication and the characteristic polynomial can also be defined in FP+C, the preceding lemma implies that FP+C is capable of defining the matrix rank for all matrices over $\mathbb{Q}$. Thus, by Theorem 1.4.3 we obtain the following result.

Theorem 2.5.8. *The class SLES($\mathbb{Q}$) is definable in* FP+C.

With this result in mind, one could be tempted to think that solvability of linear equation systems over $\mathbb{Z}$ can be defined in FP+C. This would suggest that reasons for the descriptive complexity are due to special properties of rings with finite characteristic. However, in Section 2.6 we prove FP+C undefinability over $\mathbb{Z}$.

Altogether we have seen that FP+C is capable of defining many important problems from linear algebra, but the previous results indicate an unsatisfiable gap between FP+C and PTIME. Other known classes in PTIME$\setminus$FP+C appear to be rather artificial, whereas solving linear equations is a classical PTIME property. The central aim of Chapter 3 is an analysis of different ways to enrich fixed point logics to make these queries definable.

2.6. Reducing Linear Equation Systems

We exploit the results from the preceding section in order to identify further problems which are as hard as deciding solvability of linear equation systems with respect to FP+C definability. More precisely, we establish logical reductions from the query $\mathit{SLES}(\mathcal{R})$ to other classes of structures $\mathcal{C}$. For this purpose recall the notion of logical interpretations from Section 1.1. If we obtain an FP+C-interpretation acting as a reduction from $\mathit{SLES}(\mathcal{R})$ to $\mathcal{C}$, we can conclude that $\mathcal{C}$ is not FP+C definable.

As a first query, we treat similarity of matrices which have entries in some finite field. The following reduction is based on an idea formulated in [47]. For any finite field $\mathcal{F}$, we introduce the Boolean query

$$\mathit{SIM}(\mathcal{F}) := \{\mathfrak{A} = (A,\bar{C},\bar{D}) \in \mathit{fin}[\tau_{\mathcal{F}}^{(1,1)} \dot\cup \tau_{\mathcal{F}}^{(1,1)}] \,:\, C_{\mathfrak{A}} \text{ is similar to } D_{\mathfrak{A}}\}.$$

A comment concerning the relevance of this query is in place. Actually, for any unordered square matrix, a special type of similarity is a lower bound for every query which is well-defined in our logical setting. To be precise, any matrix query should be invariant under *permutation similarity*. Two $I \times I$ matrices A and B over some ring $\mathcal{R}$ are called *(permutation) similar* if there is an invertible $I \times I$ (permutation) matrix P over $\mathcal{R}$ such that $A = PBP^{-1}$. Thus, an investigation of this class seems reasonable.

We proceed to show that $\mathit{SLES}(\mathcal{F})$ reduces to $\mathit{SIM}(\mathcal{F})$ by an FO interpretation. For this purpose, let $\mathfrak{A} = (A,\bar{M},\bar{b}) \in \mathit{fin}[\tau_{\mathcal{F}}^{(1,1)} \dot\cup \tau_{\mathcal{F}}^{(1,0)}]$ encode the linear system $M_{\mathfrak{A}} \cdot \bar{x} = b_{\mathfrak{A}}$. For the sake of simplicity, assume that matrices are encoded in normal form, cf. Section 2.1. We consider a two-dimensional interpretation, which is equality preserving and uses two parameters c and d. The domain formula is given by

$$\delta(x,y) := (x = c) \vee (x = d \wedge y = d).$$

The interpreted structure encodes the following two matrices C and D:

$$C = \begin{pmatrix} M_{\mathfrak{A}} & b_{\mathfrak{A}} \\ 0 \cdots 0 & 0 \end{pmatrix} \text{ and } D = \begin{pmatrix} M_{\mathfrak{A}} & 0 \\ 0 \cdots 0 & 0 \end{pmatrix}.$$

We use tuples $(c,\cdot), (c,\cdot)$ to address entries of the matrix $M_{\mathfrak{A}}$ and tuples $(c,\cdot), (d,d)$ for the column $b_{\mathfrak{A}}$. For illustration we present a formula $\varphi_0^C(xy,x'y')$ which defines the 0-entries for the matrix C:

$$\begin{aligned}\varphi_0^C(xy,x'y') := (x = d) \vee (x = c \wedge x' = c \wedge M_0^{\mathcal{F},1,1}(y,y')) \\ \vee (x = c \wedge x' = d \wedge y' = d \wedge b_0^{\mathcal{F},1,0}(y)).\end{aligned}$$

We have to guarantee that C and D are similar iff the equation system $M_{\mathfrak{A}} \cdot \bar{x} = b_{\mathfrak{A}}$ is solvable. Indeed, if $\bar{x}_0$ is a solution, we regard the invertible matrix

$$T := \begin{pmatrix} E & \bar{x}_0 \\ 0 \cdots 0 & -1 \end{pmatrix}, \text{ where } E \text{ is the identity matrix of suitable dimension.}$$

It can be shown that $CT = TD$, thus C and D are similar. On the other hand, if the system is not solvable, then surely the rank of the two matrices differs. This implies that they cannot be similar. In particular, note that checking similarity for matrices over fields is clearly a PTIME property [66].

Theorem 2.6.1. *For any finite field $\mathcal{F}$ the class SIM($\mathcal{F}$) is not definable in* FP+C.

We can apply the same interpretation once again. Consider the query

$$EQRANK(\mathcal{F}) := \{\mathfrak{A} = (A,\bar{C},\bar{D}) \in fin[\tau_{\mathcal{F}}^{(1,1)} \uplus \tau_{\mathcal{F}}^{(1,1)}] : C_{\mathfrak{A}} \text{ and } D_{\mathfrak{A}} \text{ have equal rank}\}.$$

By the explanations mentioned above it is clear that this class cannot be defined in FP+C as well. In both cases our arguments crucially rely on properties of the matrix rank which are valid only for matrices over fields. However, in Section 3.2 we see how to extend the results by involving more algebraic theory.

Theorem 2.6.2. *For any finite field $\mathcal{F}$ the class EQRANK($\mathcal{F}$) is not definable in* FP+C.

Next, we show that FP+C is unable to define to the query 3-*SAT*. This query is known to be complete for the complexity class NP, thus it is an expected result. We provide a first-order interpretation which acts as a reduction from the class 3-*SLES*($\mathbb{F}_2$) to 3-*SAT*.

First we fix an encoding of 3-*SAT* by finite structures. Let the signature be $\tau = \{N, C\}$, where N is a binary, and C a ternary relation symbol. We consider elements in the universe of τ-structures as propositional literals of the encoded formula. Each τ-structure $\mathfrak{A}$ encodes a formula in 3-CNF provided that

- $N^{\mathfrak{A}}$ is symmetric and irreflexive, and
- for all $a \in A$ there is precisely one $b \in A \setminus \{a\}$ such that $\mathfrak{A} \models Nab$.

We interpret tuples $(a,b) \in N^{\mathfrak{A}}$ to be inverse literals corresponding to the same variable. Tuples $(a,b,c) \in C^{\mathfrak{A}}$ are interpreted as a clause containing the literals a,b,c. The encoded formula, denoted by $\varphi_{\mathfrak{A}}$, is the conjunction over all existing clauses. The formula $\varphi_{\mathfrak{A}}$ is *satisfiable* if there is a mapping $I\colon A \to \{0,1\}$ such that $I(a) = 0$ iff $I(b) = 1$ for all $(a,b) \in N^{\mathfrak{A}}$, and $I \models \varphi_{\mathfrak{A}}$ in the usual sense. Following this conventions, we set

$$3\text{-}SAT := \{\mathfrak{A} = (A,N,C) \in fin[\tau] : \mathfrak{A} \text{ encodes a satisfiable formula } \varphi_{\mathfrak{A}}\}.$$

The underlying idea of the reduction is as follows: First of all, we identify each variable in the linear equation system over $\mathbb{F}_2$ with a designated propositional variable. This way we also understand the Boolean values, which are assigned to the propositional variables in the natural way as elements in the field $\mathbb{F}_2$. Altogether, we obtain a one-to-one correspondence between the assignments of the new propositional variables and the assignments of the original variables in the linear equation system.

So equations of the form $x+y+z=a$ that are part of the linear system are translated into a set of clauses. These clauses are built up by using the literals over the three associated variables. The resulting sets are of constant size and they are satisfiable iff there is an assignment for the corresponding variables over $\mathbb{F}_2$ that is valid with respect to the actual equation. For illustration, consider the case that $x+y+z=0$. The corresponding set of clauses is as follows:

$$\begin{array}{lll} x \to (y \vee z) & z \to (x \vee y) & (x \wedge y) \to \neg z \\ y \to (x \vee z) & (x \wedge z) \to \neg y & (y \wedge z) \to \neg x. \end{array}$$

Similarly, we handle the case $x+y+z=1$, and equations consisting of only two variables as well. Once again our interpretation is two-dimensional, and equality preserving. Apart from that it uses two parameters c and d. The domain formula is given by

$$\delta(x,y) := (x=c) \vee (x=d).$$

Tuples $(c,\cdot)$ are considered as the set of propositional variables with $(d,\cdot)$ being their negation, i.e. the formula defining the predicate N is given by

$$\varphi_N(xy,x'y') := (y=y') \wedge (x=c \to x'=d) \wedge (x=d \to x'=c).$$

Finally, we explain how to construct the formula $\varphi_C(x_1y_1,x_2y_2,x_3y_3)$. Its shape is

$$\varphi_C := \exists z \left[Mzy_1 \wedge Mzy_2 \wedge Mzy_3 \wedge \left(bz \to \bigvee \cdots \right) \wedge \left(\neg bz \to \bigvee \cdots \right) \right].$$

Clearly, the big disjunctions can be completed to define the appropriate set of clauses as described above. Altogether we derive:

Theorem 2.6.3. *The class 3-SAT is not definable in* FP+C.

We return to linear algebra and show that solvability of linear equation systems over the ring $\mathbb{Z}$ cannot be defined in FP+C. Systems like this can be represented in our usual encoding by a ternary relation M and a binary relation b, where the both latter components of M and b range over a designated numerical domain. However, as we want to define a query, we slightly adapt our convention. Actually, it suffices to include a preorder $\preceq$ in the structures. Its width, i.e. the length of the corresponding linear order on the associated equivalence then determines the possible size of integers that are possible matrix entries. For $\tau = \{M,b,\preceq\}$ define

$$\mathit{SLES}(\mathbb{Z}) := \{\mathfrak{A} = (A,M,b,\preceq) \in \mathit{fin}[\tau] \,:\, M_{\mathfrak{A}} \cdot \bar{x} = b_{\mathfrak{A}} \text{ is solvable}\}.$$

We present an FO interpretation reducing for all $m \geq 2$ the class $\mathit{SLES}(\mathbb{Z}_m)$ to $\mathit{SLES}(\mathbb{Z})$. The idea is based on the following observation.

Proposition 2.6.4. *$M_{\mathfrak{A}} \cdot \bar{x} = b_{\mathfrak{A}}$ is solvable over $\mathbb{Z}_m$ iff the system*

$$M_{\mathfrak{A}} \cdot \bar{x} + mE \cdot \bar{y} = b_{\mathfrak{A}}$$

is solvable over $\mathbb{Z}$, where E denotes the identity matrix of appropriate dimension, and $\bar{y}$ is a vector of new variables with $|bx| = |\bar{y}|$.

Thus, by the foregoing examples it is clear that the intended reduction can be realized by a first-order interpretation. The only difficulty is to interpret an appropriate preorder in the given structure. Since m is fixed and we have to encode integers only up to m this can be done, e.g. by using a k-dimensional interpretation such that sufficiently many equality types are available.

Theorem 2.6.5. *The class SLES($\mathbb{Z}$) is not definable in* FP+C.

Recall that this result contrasts to the case of linear equation systems over $\mathbb{Q}$, as Theorem 2.5.8 points out. Moreover, solvability over $\mathbb{Z}$ can be characterized in terms of solvability over the residue rings. In [54] it is shown that $M_{\mathfrak{A}} \cdot \bar{x} = b_{\mathfrak{A}}$ is solvable over $\mathbb{Z}$ iff the system is solvable over $\mathbb{Z}_m$ for all $m \geq 2$. Altogether, solvability over $\mathbb{Z}$ is equivalent to solvability over $\mathbb{Z}_m$ for all $m \geq 2$. In means of FP+C definabilty, they differ significantly from the problem considered over $\mathbb{Q}$.

Chapter 3.

Operators from Linear Algebra

Our preceding considerations revealed interesting classes of problems from linear algebra which cannot be expressed in FP+C, but are decidable in polynomial time. These queries underline the fact that FP+C does not capture PTIME on the class of all finite structures, a result first shown by Cai et al. in their famous article [16]. With these results in mind, we explore ways to enrich FP+C with operators from linear algebra. We obtain logics which come closer to capturing PTIME and analyze their behavior for different classes of underlying rings. In particular, we investigate to what extent the expressive power of the various logics can be related.

The central problem in our precedent considerations was deciding solvability of linear equation systems. Hence, in Section 3.1 we introduce the logic FP+slv which is the minimal reasonable extension of FP+C with respect to this shortcoming. It is obtained by adding operators capable of deciding solvability of linear equation systems. Dawar et al. proved that the prominent CFI-query can be expressed in this logic, thereby demonstrating (beside the solvability query itself) that $\mathsf{FP+C} \leq \mathsf{FP+slv}$. With FP+sim, another extension is discussed in Section 3.2. This fixed point logic arises from FP+C by adding operators capable of deciding similarity of definable matrices. By refining ideas from the foregoing chapter, we can show that $\mathsf{FP+slv} \leq \mathsf{FP+sim}$. Recall that whenever two matrices are similar, they are also equivalent, but the converse is false in general. We investigate to what extent operators capable of deciding similarity are related to those capable of deciding equivalence.

At least over fields, the most comprehensive enrichment of FP+C which we analyze is achieved by adding operators capable of computing the matrix rank of definable matrices. Section 3.3 analyzes the resulting fixed point logic FP+rk, which was initially studied by Dawar et al. [27]. In Section 3.4, we introduce infinitary logics subsuming the above logics and present appropriate pebble games. These games capture equivalence in finite variable fragments. We point out that the underlying ring is an important parameter of the operators. Another relevant parameter is their arity for which a strict hierarchy can be obtained, cf. Chapter 4.

3.1. Solving Systems of Linear Equations

In Section 2.5 it became clear that FP+C lacks the possibility to express solvability of linear equation systems. This is true for linear equation systems over arbitrary finite rings. Thus, we are interested in extensions of FP+C in which this query is definable. The most direct way to achieve this is to adjoin an appropriate family of generalized Lindström quantifiers to FO+C or FP+C. For any finite ring $\mathcal{R}$ with elements $a_1,\ldots,a_m$, and each matrix dimension $(v,w) \in \hat{s}$, we introduce the class

$$slv_{\mathcal{R}}^{(v,w)} = \{\mathfrak{A} = (A,\bar{M},\bar{b}) \in fin[\tau_{\mathcal{R}}^{(v,w)} \dot\cup \tau_{\mathcal{R}}^{(v,0)}] \,:\, M_{\mathfrak{A}} \cdot \vec{x} = b_{\mathfrak{A}} \text{ is solvable over } \mathcal{R}\}.$$

Each of these classes gives rise to a Lindström quantifier $slv_{\mathcal{R}}^{(v,w)}$ of type $((v,w)^m, v^m)$ and arity s. By $slv_{\mathcal{R}}$ we denote the family of all quantifiers associated to a fixed ring $\mathcal{R}$, whereas the class of all quantifiers is denoted by slv.

The first question which arises concerns the relationship between FP+C and FP(slv). By the results of Section 2.5, we know that FP(slv) $\not\subseteq$ FP+C. Similarly, it seems to be hard to simulate the full counting mechanism provided by FP+C using only fixed point recursion in addition to slv-operators. Despite that, we show that modulo counting can be handled in FP(slv). For this purpose, let some FP(slv)-formula $\varphi(\bar{x})$ be given. Then for all $k \geq 2$ and $0 \leq a < k$ there is a sentence $\psi \in$ FP(slv) such that

$$\psi \equiv (\#\bar{x}\varphi(\bar{x}) = a \mod k).$$

First assume $a \neq 0$. We set $\nu_1(\bar{x},\bar{y}) := (\bigvee_i x_i \neq y_i) \wedge \varphi(\bar{x}) \wedge \varphi(\bar{y})$ and $\nu_i(\bar{x},\bar{y}) = 0$ for all $i \in \mathbb{Z}_k \setminus \{1\}$. Furthermore, let $\eta_{a-1}(\bar{x}) = \varphi(\bar{x})$ and $\eta_i(\bar{x}) = 0$ for all $i \in \mathbb{Z}_k \setminus \{a-1\}$. This defines a linear equation system $(\bar{\nu},\bar{\eta})$ over $\mathbb{Z}_k$ which is solvable for a given structure $\mathfrak{A}$ iff the number of different tuples $\bar{a} \in \varphi^{\mathfrak{A}}$ equals a modulo k. The case when $a = 0$ can be handled by excluding the other ones.

It remains unanswered whether more involved counting properties can be defined in FP(slv). In particular, this includes relations between different cardinalities of definable sets, e.g. the Rescher or Härtig quantifier. As already pointed out, this seems unlikely.

Definition 3.1.1. Let FO+slv and FP+slv denote the extensions of FO(slv) respectively FP(slv) which result from the closure under numerical and counting terms, precisely in the same way as FP+C and FO+C are defined as extensions of FP and FO.

Arvind and Vijayaraghavan [6] analyzed solvability of linear equation systems over finite rings from an algorithmic point of view. Their results imply that the problem is decidable in PTIME, so we have

$$\text{FO+slv} \leq \text{FP+slv} \leq \text{PTIME}.$$

We will now analyze the expressive power of the introduced extensions. Since for all finite rings $\mathcal{R}$ we have $SLES(\mathcal{R}) \in \mathsf{FO}{+}\mathsf{slv}$, one concludes that $\mathsf{FO}{+}\mathsf{slv} \not\subseteq \mathsf{FP}{+}\mathsf{C}$. Although it seems unlikely that the converse inclusion holds, by now this remains an open question. We begin to study graph accessibility problems:

Theorem 3.1.2. *[Dawar et al. [27]] For all finite rings $\mathcal{R}$ we have*

$$\mathsf{FO}{+}\mathsf{DTC} \lneq \mathsf{FO}{+}\mathsf{STC} \lneq \mathsf{FO}(slv_{\mathcal{R}}) \leq \mathsf{FO}{+}\mathsf{slv}.$$

Proof. The first strict inclusion is well-known (see e.g. [30, 36]), so we only have to show that $\mathsf{FO}{+}\mathsf{STC} \lneq \mathsf{FO}(slv_{\mathcal{R}})$. For a directed graph $\mathcal{G} = (V,E)$ we have to decide whether $(s,t) \in STC(E)$ for two designated vertices $s,t \in V$. We assign a variable x_u to each vertex $u \in V$ and consider the linear equation systems containing the equations $x_u = x_v$ for all $(u,v) \in E$. In addition, the system includes the two equations $x_s = 1$ and $x_t = 0$. The resulting system is solvable, iff s and t are not contained in the same connected component. It is simple to define this system in FO, even with the exclusive use of atomic formulas. □

Note that the same proof fails for full transitive closure, and in fact the relation between $\mathsf{FO}{+}\mathsf{TC}$ and $\mathsf{FO}{+}\mathsf{slv}$ remains unclear. We come back to this issue in Section 4.2, where we encounter a close connection to an open question from the area of algorithmic complexity theory. We illustrate the expressive power of $\mathsf{FO}{+}\mathsf{slv}$ with a further example: we show that the class of all bipartite graphs can be defined in $\mathsf{FO}{+}\mathsf{slv}$. For this purpose, we consider a variable x_v ranging over $\mathbb{Z}_2$ for each vertex $v \in V$, and define the equation $x_u + x_v = 1$ for each edge $(u,v) \in E$. The resulting system is solvable over $\mathbb{Z}_2$ iff the given graph is bipartite. This result is not surprising since the class of bipartite graphs is reducible to the problem of undirected graph accessibility via a first-order interpretation [4]. Hence, the result already follows from Theorem 3.1.2.

The most cited query showing the separation of $\mathsf{FP}{+}\mathsf{C}$ from PTIME is a class of graphs introduced by Cai et al. [16]. Nowadays, one typically refers to their construction as the CFI-construction and the resulting graphs are known as CFI-graphs. One of the main contributions of their approach are sophisticated graph gadgets with a high number of automorphisms. Starting from a class of graphs with sufficient complexity, these gadgets are designed to replace single vertices in the original graph. Depending on the way in which these gadgets are connected to each other, one obtains precisely two isomorphism classes of new graphs. It was shown that no sentence in $\mathsf{FP}{+}\mathsf{C}$ is able to separate these two isomorphism classes. In contrast, Cai et al. showed that they can be distinguished by a polynomial time algorithm. This way they obtained the indicated separation. Remarkably, using a first-order interpretation, the task of distinguishing between the two isomorphism types reduces to deciding solvability of a linear equation system over $\mathbb{F}_2$.

Thus, there is a sentence in $\mathsf{FO}(slv_{\mathbb{F}_2})$ which separates the two isomorphism classes. First of all we introduce the construction in detail. Our presentation follows [25] and [27].

Assume that $\mathcal{G} = (V,E)$ is an (undirected) connected graph with a minimal vertex degree of at least two. For each vertex v we define a set of new vertices $\hat{v}$. These sets form the graph gadgets intended to replace the vertices in $\mathcal{G}$. Let

$$\hat{v} := \{a_{vw}, b_{vw}, c_{vw}, d_{vw} : w \in vE\} \cup \{v^S : S \subseteq vE, |S| \text{ even}\}.$$

The vertices a_{vw}, b_{vw} are referred to as *outer vertices*, since they will connect the two gadgets corresponding to v and w. Vertices c_{vw}, d_{vw} are used to color outer nodes, i.e. to make the property of being an outer node first-order definable. Consequently, we refer to them as *color vertices*. Crucial to the construction is the definition of edges between the remaining vertices v^S - called the *inner vertices* - and the associated outer vertices.

For each (symmetric) set $X \subseteq E$ we define the CFI-graph $\mathcal{H}_X^{\mathcal{G}}$ as follows: The set of vertices is $V_X^{\mathcal{G}} := \bigcup_{v \in V} \hat{v}$, and the set of edges $E_X^{\mathcal{G}}$ is defined as the symmetric closure of the set containing the following edges:

$$\begin{aligned}
&\text{for } v \in V, w \in vE : (a_{vw}c_{vw}), (b_{vw}c_{vw}), (c_{vw}d_{vw}) \\
&\text{for } v \in V, S \subseteq vE, |S| \text{ even} : (a_{vw}v^S) \text{ if } (v,w) \in S \text{ and } (b_{vw}v^S) \text{ otherwise} \\
&\text{for } v \in V, w \in vE, (v,w) \notin X : (a_{vw}a_{wv}), (b_{vw}b_{vw}) \\
&\text{for } v \in V, w \in vE, (v,w) \in X : (a_{vw}b_{wv}), (a_{vw}b_{vw}).
\end{aligned}$$

We say that in $\mathcal{H}_X^{\mathcal{G}}$ the edges in X have been *twisted*. Cai et al. proved that for all possible sets $X,Y \subseteq E$ we have

$$\mathcal{H}_X^{\mathcal{G}} \cong \mathcal{H}_Y^{\mathcal{G}} \text{ iff } |X| \equiv |Y| \mod 2.$$

We conclude that for each graph $\mathcal{G}$ the corresponding CFI-graphs are divided into precisely two isomorphism classes. These are completely characterized by the parity of the total number of twisted edges. We fix a representative $\mathcal{H}_0^{\mathcal{G}}$ of the isomorphism class with an even number of twists, and a CFI-graph $\mathcal{H}_1^{\mathcal{G}}$ from the isomorphism class with an odd number of twists. Starting from a class of graphs with sufficiently growing complexity, Cai et al. showed that no sentence in $\mathsf{FP}+\mathsf{C}$ can separate both classes. Moreover, this is even true for sentences in $\mathsf{C}^{\omega}_{\infty\omega}$.

Theorem 3.1.3 (Cai et al. [16])**.** *There is a class of cubic connected graphs $\mathfrak{C}$ such that for all $k \geq 1$ there is a graph $\mathcal{G} \in \mathfrak{C}$ with*

$$\mathcal{H}_0^{\mathcal{G}} \equiv^{\mathsf{C}^k_{\infty\omega}} \mathcal{H}_1^{\mathcal{G}}.$$

The weakest notion of graph complexity known to be sufficient is treewidth, cf. [25]. Originally, Cai et al. used the notion of graph separators as a measure.

Theorem 3.1.4 (Dawar et al. [27]). *There is a sentence $\varphi \in \mathsf{FO}(slv_{\mathbb{F}_2})$ such that for all graphs $\mathcal{G}$ we have*

$$\mathcal{H}_0^{\mathcal{G}} \models \varphi \text{ and } \mathcal{H}_1^{\mathcal{G}} \not\models \varphi.$$

Proof. We construct a linear equation system over $\mathbb{F}_2$: for each pair of outer vertices a_{vw} and b_{vw} we introduce variables $x_{a_{vw}}$ and $x_{b_{vw}}$, and for each inner vertex v^S a variable x_{v^S}. Observe that there is a first-order formula which identifies outer and inner vertices that belong to the same gadget, and that furthermore, a first-order formula can distinguish between these two kinds of vertices. This fact is important in order to obtain a first-order definition of the following equation system.

For each pair of corresponding outer vertices a_{vw} and b_{vw}, our system includes the equation $x_{a_{vw}} + x_{b_{vw}} = 1$. Moreover, for every pair v,w of outer vertices that are connected, we include the equation $x_v + x_w = 0$, and for each inner vertex v^S we define the equation

$$\sum_{w \in S} x_{a_{vw}} + \sum_{w \in vE \setminus S} x_{b_{vw}} = \sum_{S \subseteq vE, |S| \text{ even}} x_{v^S}.$$

Finally we include the equation summing up all variables of inner vertices, i.e.

$$\sum_{v \in V, S \subseteq E(v), |S| \text{ even}} x_{v^S} = 0.$$

Consider an even CFI-graph $\mathcal{H}_0^{\mathcal{G}}$. By $x_{a_{vw}} = 1$, $x_{b_{vw}} = 0$, $x_{v^S} = 0$ for all $v \in V$, $w \in vE$, $S \subseteq vE, |S|$ even, a solution of the equation system is given. Now, assume that we are dealing with an odd CFI-graph $\mathcal{H}_1^{\mathcal{G}}$. For convenience let $\mathcal{H}_1^{\mathcal{G}} = \mathcal{H}_{(v,w)}^{\mathcal{G}}$ for some edge $(v,w) \in E$, and consider the following subset of equations in the system:

$$\text{for all } u \in V: \quad \sum_{w \in uE} x_{b_{uw}} = \sum_{S \subseteq uE, |S| \text{ even}} x_{u^S} \tag{3.1.1}$$

$$\text{for all } (u,u') \in E \setminus \{(v,w)\}: \quad x_{b_{uu'}} + x_{b_{u'u}} = 0 \tag{3.1.2}$$

$$\text{for } (v,w): \quad x_{a_{vw}} + x_{b_{wv}} = 0, x_{a_{vw}} + x_{b_{vw}} = 1 \tag{3.1.3}$$

$$\sum_{v \in V, S \subseteq E(v), |S| \text{ even}} x_{v^S} = 0. \tag{3.1.4}$$

By summing up the left hand sides of all equations (3.1.1) and pairing corresponding variables, one can reduce the result - with equations (3.1.2) - to $x_{b_{vw}} + x_{b_{wv}}$. We employ equations of type (3.1.3) to conclude that the left hand has to sum up to 1. In contrast, according to (3.1.4), the right hand side should sum up to 0, which means that the subsystem and thus the whole system is not solvable. Using the introductory remarks, one can check that the system can be defined by an first-order formula. □

We reconsider the relationship of quantifiers $slv_{\mathcal{R}}$ for different finite rings $\mathcal{R}$. In general we conjecture that they are incomparable whenever the characteristics of the underlying rings differ. It is an easy task to show that $\mathsf{FO}(slv_{\mathbb{Z}_{p^m}}) \leq \mathsf{FO}(slv_{\mathbb{Z}_{p^n}})$ for all $m \leq n$, and we believe that the converse inclusion does not hold. By now, we are not able to prove one of these two conjectures. However, we are able to show is that all open relations reduce to these two elementary kinds. To be more precise, let $slv_{\mathbb{Z}/\star}$ be the subclass of all Lindström quantifiers in *slv* capable of deciding solvability of linear equation systems over rings $\mathbb{Z}_{p^e}$ where $p \geq 2$ is a prime and ≥ 1 a natural number. Furthermore, let $\mathsf{FP{+}slv}^{\mathbb{Z}/\star}$ and $\mathsf{FO{+}slv}^{\mathbb{Z}/\star}$ be defined as $\mathsf{FP{+}slv}$ and $\mathsf{FO{+}slv}$, but restricted to quantifiers in $slv_{\mathbb{Z}/\star}$. By adapting the ideas of [6] to the logical setting we are able to show that

Theorem 3.1.5. $\mathsf{FO{+}slv} \equiv \mathsf{FO{+}slv}^{\mathbb{Z}/\star}$ *and* $\mathsf{FP{+}slv} \equiv \mathsf{FP{+}slv}^{\mathbb{Z}/\star}$.

Proof. We obtain a direct translation. Recall from Theorem 2.2.5 that any finite ring can be decomposed into local ones. Thus, it suffices to consider formulas

$$slv_{\mathcal{R}}\ [\bar{x}_1, \bar{y}_1, \ldots, \bar{x}_r, \bar{y}_r, \bar{z}_1, \ldots, \bar{z}_r\, (\varphi_1(\bar{x}_1,\bar{y}_1), \ldots, \varphi_r(\bar{x}_r,\bar{y}_r), \psi_1(\bar{z}_1), \ldots, \psi_r(\bar{z}_r))]\,,$$

for some finite local ring $\mathcal{R}$. Let the ring $\mathcal{R}$ contain $r = p^e$ elements $s_1, \ldots, s_r$, where p is prime and $e \geq 1$. By $\mathcal{R}^+$ we denote the additive abelian group of $\mathcal{R}$. The well-known structure theorem for finite abelian groups states that $\mathcal{R}^+ \cong \mathbb{Z}_{p^{e_1}} \oplus \mathbb{Z}_{p^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_l}}$ for some $e_1 \geq e_2 \geq \cdots \geq e_l \geq 1$ with $\sum_i e_i = e$. We consider the ring of group endomorphisms over $\mathcal{R}^+$, denoted by $End(\mathcal{R}^+)$, and assume that each $\Phi \in End(\mathcal{R}^+)$ is represented by an $l \times l$ matrix having $(\varphi_1^j, \ldots, \varphi_l^j)$ as jth column where

$$\Phi(0^{j-1},1,0^{l-j}) = \varphi_1^j \cdot (1,0^{l-1}) + \varphi_2^j \cdot (0,1,0^{l-2}) + \varphi_3^j \cdot (0,0,1,0^{l-3}) + \cdots + \varphi_l^j \cdot (0^{l-1},1).$$

In other words, we uniquely represent each endomorphism by listing the images of the generators from the cyclic groups with respect to the group decomposition and express these images again as a combination of the generators. The resulting matrices have entries in $\mathbb{Z}_{p^e}$. A result due to Shoda [65] characterizes the matrices in $\mathbb{Z}_{p^e}$ which represent endomorphisms over $\mathcal{R}^+$ in this sense. Furthermore, the set of these matrices becomes a ring with respect to usual matrix addition and multiplication if the entries in each row i are reduced modulo p^{e_i}. This ring coincides with $End(\mathcal{R}^+)$, cf. [6, 65].

The crucial point is that $\mathcal{R}$ can be embedded into the ring $End(\mathcal{R}^+)$. This way we can use the matrix representation of endomorphisms over $\mathcal{R}^+$ for the ring elements in $\mathcal{R}$. For each $a \in \mathcal{R}$ let $T_a \colon \mathcal{R} \to \mathcal{R}$ denote the left translation with a, i.e. define $T_a(r) := ar$. Then $\mathcal{R} \hookrightarrow End(\mathcal{R}^+), r \mapsto T_r$ is an embedding. Since $\mathcal{R}$ is fixed, all values e, e_i, r, l are fixed as well, thus we obtain first-order formulas encoding the equation system in the new representation. Note that we are now dealing with a matrix and a column vector which have $l \times l$ matrices over $\mathbb{Z}_{p^e}$ as entries. This equation system is equivalent to the

previous one if we adapt the variable range and the corresponding arithmetic operations. To obtain an equivalent system over $\mathbb{Z}_{p^e}$, we have to further convert the system.

First of all, assume that we adapt the variable range to $\mathbb{Z}_{p^e}$, also switching to the appropriate operations between $l \times l$ matrices over $\mathbb{Z}_{p^e}$ and elements in $\mathbb{Z}_{p^e}$. If we restrict the variable range to $\mathbb{Z}_{p^e}$, we ignore elements in $\mathcal{R}$ as possible candidates in solutions. This means that we expand the coefficient matrix as follows: each entry T_a is substituted by the tuple $(T_a \cdot T_{s_1}, \ldots, T_a \cdot T_{s_r})$, i.e. we expand each variable x that takes $l \times l$ matrices over $\mathbb{Z}_{p^e}$ as value by a tuple of new variables $(x_1, \ldots, x_r)$ which range over $\mathbb{Z}_{p^e}$. This means that each variable x becomes the linear combination of the x_is, i.e. $x = \sum_{i=1}^{r} x_i T_{r_i}$. If we stick to the appropriate matrix operations we obtain an equivalent system whose coefficients are $l \times l$ matrices over $\mathbb{Z}_{p^e}$ and whose variables in evaluations range over $\mathbb{Z}_{p^e}$. Again, the size of every object in this transformation is fixed by $\mathcal{R}$, thus the new system is first-order interpretable in the original one. Finally, we unfold all matrices in the above system. For each $(i,j) \in l \times l$ we regard the set of equations which correspond to entries in positions (i,j) in the $l \times l$ matrices in the system. Each of these entries corresponds to a set of equations over $\mathbb{Z}_{p^{e_i}}$, however multiplying each coefficient by p^{e-e_i} leads to an equivalent system over $\mathbb{Z}_{p^e}$. This last transformation can also be captured by a first-order formula since it mainly corresponds to a syntactic rewriting. □

We will now reconsider the extensions of first-order logic by *slv*-quantifiers in the view of circuit value problems. Let σ be some vocabulary containing only unary relation symbols. We define $\tau_\sigma := \{E, I_+, I_-, O\} \cup \sigma$, where E denotes a binary relation symbol (edge relation), and I^+, I^- and O are unary relation symbols (input gates true and false, and output gates). The predicates in σ are intended to identify the different types of gates. Formally, the semantic for gates of type $R \in \sigma$ is given by an evaluation function

$$I_\sigma^R \colon \{(v,w) \in \hat{n} : n \geq 1\} \to \{0,1\}.$$

This function determines the value of the gate if v inputs are false and w inputs are true. A (Boolean) *σ-circuit* is a τ_σ structure $\mathfrak{C} = (C, E^{\mathfrak{C}}, I_+^{\mathfrak{C}}, I_+^{\mathfrak{C}}, O^{\mathfrak{C}}, (R^{\mathfrak{C}})_{R\in\sigma})$ such that

- C is the disjoint union of $I_+^{\mathfrak{C}}$, $I_-^{\mathfrak{C}}$, $O^{\mathfrak{C}}$ and the sets $(R^{\mathfrak{C}})_{R\in\sigma}$,
- the vertices in $O^{\mathfrak{C}}$ have no successors but a unique predecessor,
- the nodes in $I_+^{\mathfrak{C}}, I_-^{\mathfrak{C}}$ are precisely the vertices without predecessors,
- every vertex in $\bigcup_{R\in\sigma} R^{\mathfrak{C}}$ has a predecessor and a successor,
- the graph $\mathfrak{C} = (C, E^{\mathfrak{C}})$ is connected and acyclic.

A circuit $\mathfrak{C}$ *evaluates to true* if there is a mapping $T\colon C \to \{0,1\}$ such that

$$\begin{aligned} \text{for } i \in I_+^{\mathfrak{C}} &: T(i) = 1 \\ \text{for } i \in I_-^{\mathfrak{C}} &: T(i) = 0 \\ \text{for } g \in R^{\mathfrak{C}}, R \in \sigma &: T(g) = I_\sigma^R \left(\#_v[g \in vE^{\mathfrak{C}}, T(v) = 0], \#_w[g \in wE^{\mathfrak{C}}, T(w) = 1]\right) \\ \text{for some } o \in O^{\mathfrak{C}} &: T(o) = 1. \end{aligned}$$

The *σ-circuit value problem (CVP)* is to decide whether a given σ-circuit evaluates to true. Recall that for circuits consisting solely of NAND gates the corresponding CVP is already complete for PTIME. Hence, it is unlikely that there is an FO+slv sentence defining this class. Our aim is to identify families of gates for which the corresponding CVP is definable in FO+slv. Natural candidates are MOD_k gates for $k \geq 2$. Their semantic is determined by

$$I^{\text{MOD}_k}(v,w) = \begin{cases} 0, & \text{if } v \equiv 0 \mod k \\ 1, & \text{if } v \not\equiv 0 \mod k. \end{cases}$$

Note that MOD_2 gates with two inputs are XOR gates. It follows that MOD_2 gates can express negation. The set of Boolean functions representable by circuits over XOR gates is a strict subclass of the set of all Boolean functions, whereas NAND is known to be functionally complete. However, MOD_3 gates already can simulate NAND gates.

It seems to be more appropriate to consider *arithmetic* circuits. In contrast to Boolean circuits these take, for instance, integers as inputs and outputs. Semantics for MOD_k gates are adapted in the natural way. We agree that evaluation functions for vocabularies containing arithmetic gates are of the form $I_\sigma^R\colon \bigcup_{k\geq 1} \omega^k \to \omega$. The evaluation function for MOD_k gates is then determined by

$$I^{\text{MOD}_k}(v_1,\ldots,v_k) = \sum_j v_j \mod k.$$

Evaluation in arithmetic circuits is defined in the same way as evaluation in Boolean circuits with obvious adaptations. Let σ be a vocabulary of arithmetic gates. The corresponding *arithmetic σ-circuit value problem* is to decide whether in a given arithmetic circuit at least one output evaluates to 1. For a fixed $k \geq 2$, we show that the arithmetic CVP for MOD_k gates can be formulated as a linear equation system over $\mathbb{Z}_k$. We denote this problem by $CVP(\mathbb{Z}_k)$.

Theorem 3.1.6. *Let $k \geq 2$ and let $\sigma = \{\text{MOD}_k\}$. Then the (arithmetic) σ-circuit value problem is definable in* FO+slv.

Proof. The translation into a linear system is straightforward. Let $\mathfrak{C}$ be an arithmetic circuit over MOD_k gates. For each vertex $v \in V$ we introduce a variable x_v ranging over $\mathbb{Z}_k$. The equation system over $\mathbb{Z}_k$ consists of the following equations:

$$\begin{aligned}
\text{for all } i \in I_+^{\mathfrak{C}}: &\quad x_i = 1\\
\text{for all } i \in I_-^{\mathfrak{C}}: &\quad x_i = 0\\
\text{for all } v \in \text{MOD}_k^{\mathfrak{C}}: &\quad x_v = \sum_{w, v \in wE^{\mathfrak{C}}} x_w\\
\text{for all } o \in O^{\mathfrak{C}}, w \in \text{MOD}_k^{\mathfrak{C}}, o \in wE^{\mathfrak{C}}: &\quad x_o = x_w\\
\text{for some } o \in O^{\mathfrak{C}}: &\quad x_o = 1.
\end{aligned}$$

The system is FO definable. It has a solution iff $\mathfrak{C}$ has an output that evaluates to 1. □

As indicated, the above theorem also includes the case of Boolean circuits over XOR gates. An open question is whether we can sharpen the result to circuits built over different types of MOD_k gates. Again, this seems unlikely since we can simulate a NAND gate by using for instance one MOD_2 and one MOD_3 gate:

$$[(2 + x + y) \mod 3] \mod 2 \equiv (x \text{ NAND } y).$$

Imhof [48] showed that the CVP for Boolean monotone circuits is complete for IFP if cycles are allowed. It is an open question whether a similar result can be established for extensions of FO by solve operators. One can prove that the introduced CVPs are complete problems for interesting logspace modulo counting classes. For primes p, these classes are captured by $\mathsf{FO{+}slv}_{\mathbb{F}_p}$ on the domain of ordered structures, cf. Section 4.2.

Chattopadhyay et al. [18] studied arithmetic circuits over modulo gates and obtained lower bounds for computing different functions. If we could strengthen our knowledge about the relationship between FO+slv and these circuits, it might be possible to exploit these lower bounds to obtain undefinability results for FO+slv. Hence, further investigations in this area seem profitable.

3.2. Similarity and Equivalence of Matrices

In Theorem 2.6.1 we constructed a first-order interpretation reducing solvability of linear equation systems to the problem of deciding similarity of two matrices. This result implies that the latter problem cannot be defined in FP+C either. The following extension of FP+C is motivated by this shortcoming. We introduce appropriate quantifiers for matrix similarity and relate the resulting extensions to FO+slv and FP+slv, respectively. Note that matrix similarity is a notion which only makes sense for square matrices. For any

finite ring $\mathcal{R}$ and each matrix dimension $(v,v) \in \hat{s}$ we define the Lindström quantifier

$$sim_{\mathcal{R}}^{(v,v)} = \{\mathfrak{A} = (A,\bar{M},\bar{N}) \in fin[\tau_{\mathcal{R}}^{(v,v)} \dot\cup \tau_{\mathcal{R}}^{(v,v)}] \,:\, M_{\mathfrak{A}} \text{ similar to } N_{\mathfrak{A}}\}.$$

We adapt the notation from the preceding section, i.e. we denote the class of all quantifiers corresponding to a certain ring $\mathcal{R}$ by $sim_{\mathcal{R}}$, and the whole family of quantifiers by *sim*. We are not aware of algorithms deciding similarity of matrices over arbitrary finite rings in polynomial time. Thus, we consider to restrict this query to matrices over finite fields. Let $sim^{\mathcal{F}_\star}$ be the collection of quantifiers $sim_{\mathcal{F}}$ for finite fields $\mathcal{F}$, i.e.

$$sim^{\mathcal{F}_\star} = \bigcup_{\mathcal{F} \text{ finite field}} sim_{\mathcal{F}}.$$

Definition 3.2.1. Let $\mathsf{FO}{+}\mathsf{sim}$ and $\mathsf{FP}{+}\mathsf{sim}$ denote the extensions of $\mathsf{FO}(sim)$ respectively $\mathsf{FP}(sim)$ by closure under the formation of numerical and counting terms.

Moreover, let $\mathsf{FO}{+}\mathsf{sim}^{\mathcal{F}_\star}$ and $\mathsf{FP}{+}\mathsf{sim}^{\mathcal{F}_\star}$ denote the restrictions of $\mathsf{FO}{+}\mathsf{sim}$ and $\mathsf{FP}{+}\mathsf{sim}$, which result from limiting the set of possible quantifiers to finite fields.

We analyze the data complexity of the introduced extensions: over (finite) fields one can decide whether two matrices are similar by comparing their Frobenius normal forms. Polynomial time algorithms able to compute this normal form are known, see e.g. [66]. However, to our knowledge an appropriate normal form for matrices over arbitrary rings has not yet been established. We conclude

Proposition 3.2.2. $\mathsf{FO}{+}\mathsf{sim}^{\mathcal{F}_\star} \leq \mathsf{FP}{+}\mathsf{sim}^{\mathcal{F}_\star} \leq \mathsf{PTIME}$.

We proceed to study the relationship between the quantifier classes *slv* and *sim*: the arguments used for proving Theorem 2.6.1 show that over fields, solvability of linear equation systems can be reduced to similarity of matrices via a first-order interpretation. We extend the argumentation to derive the following, more general result.

Theorem 3.2.3. $\mathsf{FO}{+}\mathsf{slv} \leq \mathsf{FO}{+}\mathsf{sim}$ *and* $\mathsf{FP}{+}\mathsf{slv} \leq \mathsf{FP}{+}\mathsf{sim}$.

Proof. For a finite ring $\mathcal{R}$ let an ($\mathsf{FO}{+}\mathsf{slv}$ or $\mathsf{FP}{+}\mathsf{slv}$) formula be given by

$$slv_{\mathcal{R}}\left[(\bar{x}_a,\bar{y}_a,\bar{z}_a)_{a\in\mathcal{R}}\,(\varphi_a(\bar{x}_a,\bar{y}_a),\psi_a(\bar{z}_a))_{a\in\mathcal{R}}\right].$$

Just as in the proof of Theorem 2.6.1, we conclude that there are formulas $(\vartheta_a,\eta_a)_{a\in\mathcal{R}}$ such that for any structure $\mathfrak{A}$ we have

$$M_{\mathfrak{A}}^{\vartheta} = \begin{pmatrix} M_{\mathfrak{A}}^{\varphi} & M_{\mathfrak{A}}^{\psi} \\ 0\cdots 0 & 0 \end{pmatrix} \text{ and } M_{\mathfrak{A}}^{\eta} = \begin{pmatrix} M_{\mathfrak{A}}^{\varphi} & 0 \\ 0\cdots 0 & 0 \end{pmatrix}.$$

If the system $(M_{\mathfrak{A}}^{\varphi},M_{\mathfrak{A}}^{\psi})$ is solvable, $M_{\mathfrak{A}}^{\vartheta}$ and $M_{\mathfrak{A}}^{\eta}$ are similar. To see this, let $\bar{x}_0$ be a solution. In this case the matrix

$$T := \begin{pmatrix} E & \bar{x}_0 \\ 0 \cdots 0 & -1 \end{pmatrix},$$

where E is a unity matrix of suitable dimension, is invertible and $M_{\mathfrak{A}}^{\vartheta} \cdot T = T \cdot M_{\mathfrak{A}}^{\eta}$.

Now, assume that the linear equation system $(M_{\mathfrak{A}}^{\varphi},M_{\mathfrak{A}}^{\psi})$ is not solvable. We require some more involved arguments than in the proof over fields, since matrix rank for matrices over rings behaves differently.

We introduce the notion of *McCoy rank*. Assume that A is an $I \times J$ matrix over a commutative ring $\mathcal{R}$ and b an I column vector over $\mathcal{R}$. For $1 \leq t \leq \min(|I|,|J|)$, we define the t-th *determinantal ideal* $F_t(A)$ as the ideal in $\mathcal{R}$ which is generated by all $t \times t$ subdeterminants of A. Furthermore, we set $F_0(A) = R$ and $F_t(A) = 0$ for all $t > \min(|I|,|J|)$. Then the McCoy rank $rk_m(A)$ of A is the largest integer $t \geq 0$ for which there is no element $0 \neq x \in \mathcal{R}$ so that $xF_t(A) = 0$. The McCoy rank is an important generalizations of the concept of matrix rank over rings, and its definition is equivalent to the common matrix rank over fields. In particular, in the case of homogeneous linear equation systems it characterizes solvability, see [59]. Nevertheless, for general systems no equivalent criterion seems to exists. However, for Noetherian full quotients rings (which include finite commutative rings), Ching [19] found the following sufficient criterion.

Let $D_t(A,b)$ be the ideal generated by all $t \times t$ subdeterminants of the augmented matrix $(A|b)$ which are not $t \times t$ subdeterminants of A. If $D_{rk_m(A)+1}(M,b) = \{0\}$, then the linear equation system $A\bar{x} = b$ has a solution [19]. In our case this criterion implies that $D_{rk_m(M_{\mathfrak{A}}^{\varphi})+1}(M_{\mathfrak{A}}^{\varphi},M_{\mathfrak{A}}^{\psi}) \neq \{0\}$. This means in particular that

$$F_{rk_m(M_{\mathfrak{A}}^{\varphi})+1}(M_{\mathfrak{A}}^{\vartheta}) \supsetneq F_{rk_m(M_{\mathfrak{A}}^{\varphi})+1}(M_{\mathfrak{A}}^{\eta}).$$

However, equivalent matrices have the same determinantal ideals [59], thus $M_{\mathfrak{A}}^{\vartheta}$ and $M_{\mathfrak{A}}^{\eta}$ cannot be equivalent, and thus not similar. □

If one substitutes matrix similarity by matrix equivalence in all foregoing definitions, one likewise obtains the extension $\mathsf{FO}{+}\mathsf{eqv}$, $\mathsf{FO}{+}\mathsf{eqv}^{\mathcal{F}_\star}$ and $\mathsf{FP}{+}\mathsf{eqv}$, $\mathsf{FP}{+}\mathsf{eqv}^{\mathcal{F}_\star}$. Over fields it is clear that the data complexity of these extensions is contained in PTIME since there are polynomial time algorithms for computing the Smith normal form. This is also true for the case of principal ideal rings [67].

Proposition 3.2.4. $\mathsf{FO}{+}\mathsf{eqv}^{\mathcal{F}_\star} \leq \mathsf{FP}{+}\mathsf{eqv}^{\mathcal{F}_\star} \leq \mathsf{PTIME}$.

Furthermore, the proof of Theorem 3.2.3 applies for matrix equivalence as well.

Theorem 3.2.5. $\mathsf{FO}{+}\mathsf{slv} \leq \mathsf{FO}{+}\mathsf{eqv}$ *and* $\mathsf{FP}{+}\mathsf{slv} \leq \mathsf{FP}{+}\mathsf{eqv}$.

Equivalence of matrices is a necessary condition for similarity, although it is not sufficient. In the following section we return to this issue and present a characterization of matrix similarity in terms of matrix equivalence. Admittedly, this characterization is only valid over fields. Thus, clarifying the general relationship between FP+sim and FP+eqv remains an open task.

3.3. Rank Operators

We follow the lines of Dawar et al. [27] and analyze logics that are extended by rank operators. These allow defining the rank of matrices as a numerical value. This way they are able to determine the maximum size of a subset of linear independent vectors. It will turn out that the rank is a powerful generalization of the usual counting mechanism.

Just as in the case of ordinary counting quantifiers, there are different ways to enrich our common logics. From the perspective of model theory, the most direct one would be to adjoin a family of generalized Lindström quantifiers. However, at least for FP+C, it has been shown [62] that formalizing the counting mechanism by extended two-sorted structures and counting terms gives rise to a more powerful extension. We strongly believe that this is true for rank operators as well. According to Dawar et al. we introduce the notion of *rank terms*. By these terms, the rank of a matrix can be defined as the numerical value in the second sort.

Let $\mathcal{R} = (R, +, \cdot)$ be a finite ring and let $\varphi = (\varphi_a(\bar{x}_a, \bar{y}_a))_{a \in R}$ be a sequence of formulas such that the tuples $\bar{x}_a, \bar{y}_a$ consist of first-order variables ranging over the universe. Recall that the matrix encoded by φ in a structure $\mathfrak{A}$ is denoted by $M^{\varphi}_{\mathfrak{A}}$. We proceed by defining the new numeric *rank term* $rk_{\mathcal{R}}(\varphi)$. Its free variables are precisely those which occur free in some of the formulas φ_a but which are not among $\bar{x}_a$,$\bar{y}_a$. In a given structure $\mathfrak{A}$, which interprets all other free variables, the value of this rank term is defined as the matrix rank of $M^{\varphi}_{\mathfrak{A}}$. In the following, we analyze the extensions of FO^+ and FP^+ which are closed under the formation of rank terms.

Definition 3.3.1. We define the logic FO+rk as the extension of FO^+ obtained by the closure under the formation of numeric rank terms $rk_{\mathcal{R}}(\cdot)$ for all finite rings $\mathcal{R}$ and the usual first-order operations. $\mathsf{FO{+}rk}^{\mathcal{F}_\star}$ denotes the restriction of FO+rk which results if we close FO^+ only under rank terms $rk_{\mathcal{F}}(\cdot)$ for finite fields $\mathcal{F}$.

Similarly, with FP+rk we define the minimal extension of FP^+ which is closed under the formation of numeric terms $rk_{\mathcal{R}}(\cdot)$ for finite rings $\mathcal{R}$ and under all FP^+ operations. $\mathsf{FP{+}rk}^{\mathcal{F}_\star}$ is defined analogous as an restriction of FP+rk.

Let $\mathcal{R}$ be a fixed finite ring. $\mathsf{FO{+}rk}_{\mathcal{R}}$ denotes the extension of FO^+ obtained by the closure under rank terms $rk_{\mathcal{R}}(\cdot)$. $\mathsf{FP{+}rk}_{\mathcal{R}}$ is defined analogous as an extension of FP^+.

Like in the case of matrix similarity and matrix equivalence, we defined rank logics in

two variants. They differ in the possibility to define matrix rank only for matrices over finite fields or also for matrices with entries in arbitrary finite rings. The reasons are the same, i.e. we do not know whether the rank of matrices over finite rings can be computed in polynomial time. For matrices over fields this is clearly true, e.g. by employing the Gaussian algorithm.

Proposition 3.3.2. $\mathsf{FO}{+}\mathsf{rk}^{\mathcal{F}_\star} \leq \mathsf{FP}{+}\mathsf{rk}^{\mathcal{F}_\star} \leq \mathsf{PTIME}$.

Ordinary counting terms can be translated into rank terms, since we have

$$\models [\sharp \bar{x}\varphi(\bar{x}) = rk_{\mathcal{R}}((\varphi_a(\bar{x},\bar{y}))_{a\in\mathcal{R}})]\,, \text{ where } \varphi_1 := [\bar{x} = \bar{y} \wedge \varphi(\bar{x})]\,, \varphi_a := 0 \text{ for } a \neq 1.$$

We will relate rank logics to the previously introduced extensions. Over finite fields, the rank quantifier can be used to decide solvability of linear equation systems, cf. Theorem 1.4.3. Beyond that, matrix similarity and matrix equivalence can be characterized by matrix rank as well. Again, this is true only for the case of matrices over fields.

Theorem 3.3.3. $\mathsf{FO}{+}\mathsf{sim}^{\mathcal{F}_\star} \leq \mathsf{FO}{+}\mathsf{eqv}^{\mathcal{F}_\star} \leq \mathsf{FO}{+}\mathsf{rk}^{\mathcal{F}_\star}$ *and the same inclusions hold for the corresponding fixed point logics.*

Proof. Consider for some finite field $\mathcal{F}$ a formula

$$eqv_{\mathcal{F}}\ \left[(\bar{x}_a, \bar{y}_a, \bar{v}_a, \bar{w}_a)_{a\in\mathcal{R}}\,(\varphi_a(\bar{x}_a,\bar{y}_a), \psi_a(\bar{v}_a,\bar{w}_a))_{a\in\mathcal{R}}\right].$$

Over fields, matrices are equivalent iff they have the same rank. Thus, the given formula is equivalent to

$$rk_{\mathcal{F}}\ [\bar{x}_a, \bar{y}_a(\varphi_a(\bar{x}_a,\bar{y}_a))_{a\in\mathcal{R}}] = rk_{\mathcal{F}}\ [\bar{v}_a, \bar{w}_a(\psi_a(\bar{v}_a,\bar{w}_a))_{a\in\mathcal{R}}]\,.$$

Matrix similarity is treated by Dixon's criterion [29]. Consider a formula

$$sim_{\mathcal{R}}\ \left[(\bar{x}_a, \bar{y}_a, \bar{v}_a, \bar{w}_a)_{a\in\mathcal{R}}\,(\varphi_a(\bar{x}_a,\bar{y}_a), \psi_a(\bar{v}_a,\bar{w}_a))_{a\in\mathcal{R}}\right].$$

The *tensor* or *Kronecker product* of an $I \times J$ matrix $A = (a_{ij})$ and a $K \times L$ matrix $B = (b_{kl})$ over a ring $\mathcal{R}$ is defined as the $(I \times K) \times (J \times L)$ matrix $A \otimes B$, where

$$(A \otimes B)_{(i,j),(k,l)} := a_{ij} \cdot b_{kl}.$$

Let A and B be $I \times I$ matrices over $\mathcal{F}$ and let $q(A,B) := rk_{\mathcal{F}}(A \otimes E_I - E_I \otimes B)$ where E_I is the appropriate matrix of unity. Dixon showed that A and B are similar iff $q(A,B)^2 = q(A,A)q(B,B)$. Clearly, the Kronecker product of two definable matrices is again definable. Thus, from the preceding characterization it follows that matrix similarity can be translated into a rank equality between definable matrices. Each rank equality is captured by matrix equivalence of the same matrices since we are working over fields, thus the claim follows. □

Figure 3.1 summarizes the relations between the introduced extensions by operators from linear algebra that we have obtained so far. The underlying arguments in proofs were first-order transformations of given formulas which rely on known characterizations from algebra. Hence, all inclusions apply to extensions of first-order and fixed point logic in precisely the same manner. Thus, the diagram omits to represent the relations with respect to these two logics.

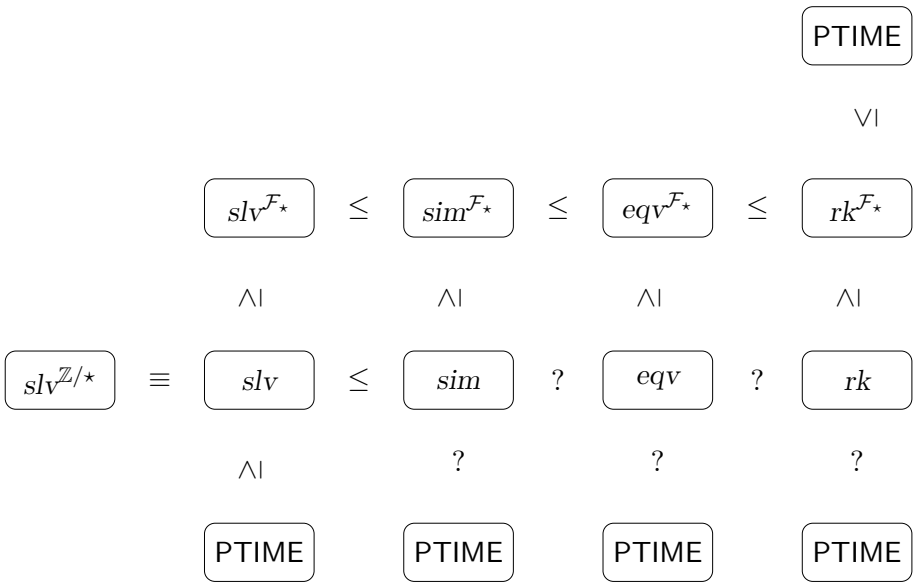

Figure 3.1.: Relations between operators from linear algebra

The rank of a matrix, or in logical means that of a relation, is a numerical parameter whose intuitive meaning is hard to understand. The field of *algebraic graph theory* studies the relationship between graph theoretical properties and algebraic parameters [9, 34]. For instance, one is typically interested in the adjacency or incidence matrix of a graph. Unfortunately, almost all investigations are carried out assuming that matrices are defined over the reals. The reason is that symmetric matrices over the reals share convenient properties, as e.g. having only real eigenvalues. Moreover, if A is an $I \times I$ matrix over $\mathbb{R}$, then there is a orthonormal basis of $\mathbb{R}^I$ consisting of eigenvectors of A. As a consequence, most of the results do not apply for matrices over finite fields.

However, an analysis of the results from this area seems reasonable. For instance, one can show that the rank of the incidence matrix of an undirected graph, regarded over $\mathbb{Q}$, characterizes the number of bipartite components in the graph (e.g. Theorem 8.2.1, [34]). Noteworthy, if we consider the incidence matrix over any finite field of odd characteristic, then the statement remains true, whereas if we consider it over $\mathbb{F}_{2^m}$ then its rank characterizes the number of connected components.

Despite that, we are not aware of any structural characterizations of matrix rank over finite domains. Recall that this fact contrasts with other notions as the determinant [57] or with linear equation systems. However, Halldórsson et al. [42] studied an interesting family of problems from graph theory for which we are able to establish a close connection to matrix rank at least over the two-element $\mathbb{F}_2$.

Let $\sigma, \rho \subseteq \omega$ be two sets of natural numbers and consider a directed graph $\mathcal{G} = (V,E)$. A subset $S \subseteq V$ is called a (σ,ρ)-*subset of* $\mathcal{G}$ iff for all vertices $v \in S$ ($v \notin S$) the number of successors in S is an element contained in σ (or ρ, respectively), i.e.

$$\begin{aligned} &\text{for all } v \in S: \quad |vE \cap S| \in \sigma \\ &\text{for all } v \notin S: \quad |vE \cap S| \in \rho. \end{aligned}$$

Accordingly, the (σ,ρ)-*subset problem for* $\mathcal{G}$, denoted by (σ,ρ)-Subset($\mathcal{G}$), is to decide whether $\mathcal{G}$ possesses a (σ,ρ)-subset. It is likely that the general problem is hard to solve. In fact, Halldórsson et al. proved that the problem $(\{0\},\rho)$-Subset($\mathcal{G}$) is complete for the complexity class NP whenever $\rho \neq \{n \in \omega : n \geq 1\}$ and if there exists an $x + 1 \in \rho$ such that $x \notin \rho$. In the remaining cases, the problem is decidable in polynomial time [43].

By the notion of adjacency matrices, an one-to-one correspondence between directed graphs and square matrices over $\mathbb{F}_2$ is given: for any graph $\mathcal{G}$, let $M_\mathcal{G}$ be the unordered $V \times V$ matrix over $\mathbb{F}_2$ such that $M_\mathcal{G}(v,w) = 1$ iff $(v,w) \in E$, and for any unordered $V \times V$ matrix M over $\mathbb{F}_2$ let $\mathcal{G}_M$ be the graph $(V, \{(v,w) : M(v,w) = 1\})$.

Now, let $\mathsf{even} = 2\omega$ and $\mathsf{odd} = \mathsf{even} + 1$. Halldórsson et al. proved that in the case where $\sigma, \rho \in \{\mathsf{even},\mathsf{odd}\}$, the problem (σ,ρ)-Subset($\mathcal{G}$) is decidable in PTIME. We will show that

Theorem 3.3.4. *$\mathcal{G}$ has an* (even,even)*-subset of size $k+1$ but no* (even,even)*-subset of size k iff $\mathrm{rk}(M_\mathcal{G}) = k$. In particular, the graph $\mathcal{G}$ has an* (even,even)*-subset iff $M_\mathcal{G}$ has not full rank.*

Proof. Let $S = \{v_1, \ldots, v_k\} \subseteq V$ be an (even,even)-subset of size k. We claim that the set of V columns $Y = \{M_\mathcal{G}(\cdot,v_1), \ldots, M_\mathcal{G}(\cdot,v_k)\}$ is linearly dependent. For each vertex $x \in V$ there is an even number of $y \in V$ such that $(x,y) \in E$, hence we have $\sum Y = 0$. Thus, the claim follows. □

Theorem 3.3.4 implies that the (even,even)-subset problem is decidable in $\mathsf{MOD}_2\mathsf{L}$ which is the class of problems decidable by a nondeterministic logspace Turing machine that accepts in input iff the number of accepting computations is odd, see Section 4.2. The idea can be adapted for the remaining cases, i.e. for the (even,even)-, (odd,even)- and (odd,odd)-subset problem.

3.4. Infinitary Logics and Pebble Games

We establish game theoretical methods to limit the expressive power of fixed point logics which are extended by operators from linear algebra. It is commonplace that many powerful tools from classical model theory fail formulated for the domain of finite structures. For instance, the compactness theorem for first-order logic no longer holds. On the other hand, many complex effects inherent to the infinite disappear. It is a fact that logics behave differently if we investigate their expressive power on the domain of finite structures. In particular, first-order logic is able to define the isomorphism class of each structure, and thus $\mathsf{L}^{\infty}_{\infty\omega}$ is able to express any possible query, even non recursive ones.

In order to establish undefinability results, one often invokes arguments which rely on combinatorics and game theory. The way of choice is to find winning strategies in suitable model comparison games that are played on sufficiently symmetric structures. For this purpose, traditional Ehrenfeucht-Fraïssé games as designed for first-order logic were extended. This leads to the notion of k-pebble (bijections) games [44]. These games capture logical equivalence of the k-variable fragment of infinitary logic (with counting). Recall their rules from Section 1.3.

We proceed similarly for the logics $\mathsf{FP}{+}\mathsf{slv}, \mathsf{FP}{+}\mathsf{sim}$ and $\mathsf{FP}{+}\mathsf{rk}$, i.e. first we introduce appropriate infinitary logics, and then develop suitable pebble games which capture logical equivalence of their finite variable fragments. Our investigations are based on the approach of Dawar and Holm [24] for rank logics.

First, we consider $\mathsf{FP}{+}\mathsf{slv}$ and $\mathsf{FP}{+}\mathsf{sim}$. These logics were introduced by extending the two-sorted fixed point logic FP^{+} by Lindström quantifiers that decide solvability and similarity, respectively. Additionally, they were closed under the formation of counting terms. Hence, we can directly translate formulas of $\mathsf{FP}{+}\mathsf{slv}$ and $\mathsf{FP}{+}\mathsf{sim}$ into equivalent formulas of $\mathsf{C}^{\omega}_{\infty\omega}(\mathit{slv})$ or $\mathsf{C}^{\omega}_{\infty\omega}(\mathit{sim})$ by standard techniques [30, 39].

Theorem 3.4.1. $\mathsf{FP}{+}\mathsf{slv} \leq \mathsf{C}^{\omega}_{\infty\omega}(\mathit{slv})$ *and* $\mathsf{FP}{+}\mathsf{sim} \leq \mathsf{C}^{\omega}_{\infty\omega}(\mathit{sim})$.

However, the rank logic $\mathsf{FP}{+}\mathsf{rk}$ was introduced by closing FP^{+} under the formation of rank terms. Hence, in order to come up with appropriate infinitary logics, we have to define a class of Lindström quantifiers first. Like for the embedding of $\mathsf{FP}{+}\mathsf{C}$ into $\mathsf{C}^{\omega}_{\infty\omega}$, we introduce, for each finite ring $\mathcal{R}$, for each matrix dimension $(v,w) \in \hat{s}$ and for each $i \in \omega$ the Lindström quantifier defined by

$$rk^{\geq i}_{\mathcal{R},(v,w)} = \{\mathfrak{A} = (A,\bar{M}) \in \mathit{fin}[\tau^{(v,w)}_{\mathcal{R}}] \,:\, rk(M_{\mathfrak{A}}) \geq i\}.$$

We define $\mathsf{R}^{\omega}_{\infty\omega}$ to be the *finite variable fragment of infinitary rank logic*, i.e. the extension of $\mathsf{L}^{\omega}_{\infty\omega}$ by the aforementioned Lindström quantifiers. Furthermore, let $\mathsf{R}^{k}_{\infty\omega}$ denote the corresponding k-variable fragment.

Theorem 3.4.2 (Dawar et al. [27]). *For each formula $\varphi \in \mathsf{FP}{+}\mathsf{rk}$ (without free variables ranging over the numerical sort) one can find an equivalent formula $\varphi' \in \mathsf{R}^k_{\infty\omega}$ for some $k \in \omega$, i.e. we have $\mathsf{FP}{+}\mathsf{rk} \leq \mathsf{R}^\omega_{\infty\omega}$.*

The *arity* of a Lindström quantifier is the maximal number of different variables it is able to bind for a single formula. The class of Lindström quantifiers $slv^{[n]} \subseteq slv$ consists of all quantifiers $slv_{\mathcal{R}}$ of arity of at most n, i.e. of quantifiers that are able to decide solvability of linear equation systems with coefficient matrices of dimension (v,w) where $v + w \leq n$.

Accordingly, let $sim^{[n]} \subseteq sim$ denote the class of similarity quantifiers of arity of at most n, i.e. the class of $sim_{\mathcal{R}}$ quantifiers which decide similarity of square matrices of dimension (v,v), where $2v \leq n$. For the introduced Lindström rank quantifiers we denote the restricted class of quantifiers of arity of at most n by $rk^{[n],\geq}$.

We also limit the quantifier arities in the corresponding logics. The logic $\mathsf{FP}{+}\mathsf{rk}^{[n]}$ is defined as $\mathsf{FP}{+}\mathsf{rk}$ with the restriction that numeric rank terms $rk_{\mathcal{R}}(\varphi(\bar{x},\bar{y}))$ can only be formed if $|\bar{x}|+|\bar{y}| \leq n$. Logics $\mathsf{FP}{+}\mathsf{slv}^{[n]}$ and $\mathsf{FP}{+}\mathsf{sim}^{[n]}$ are defined similarly. Furthermore, we follow this convention to obtain the corresponding restrictions of infinitary logics, i.e. $\mathsf{C}^\omega_{\infty\omega}(slv^{[n]})$, $\mathsf{C}^\omega_{\infty\omega}(sim^{[n]})$ and $\mathsf{R}^{\omega,[n]}_{\infty\omega}$. All inclusions stated in the theorems above are still valid if we restrict arities to n [27].

We introduce suitable pebble games for a fixed arity $n \leq k$, where k denotes the number of different variables considered in the infinitary logic. These games capture logical equivalence in $\mathcal{L}$, where $\mathcal{L}$ is one of the logics $\mathsf{C}^k_{\infty\omega}(slv^{[n]})$, $\mathsf{C}^k_{\infty\omega}(sim^{[n]})$ or $\mathsf{R}^{k,[n]}_{\infty\omega}$, respectively. For a ring $\mathcal{R}$, a set A, a matrix dimension $(v,w) \in \hat{m}$, where $m \leq n$ and a partition $\mathbf{P}$ of $A^v \times A^w$ we define for each *labeling* $\gamma\colon \mathbf{P} \to \mathcal{R}$ the $A^v \times A^w$ matrix $M^{\mathbf{P}}_\gamma$ over $\mathcal{R}$ by setting

$$M^{\mathbf{P}}_\gamma(\bar{a},\bar{b}) := x \text{ iff } \gamma(P) = x \text{ for the unique } P \in \mathbf{P} \text{ such that } (\bar{a},\bar{b}) \in P.$$

The partition $\mathbf{P}$ can be restricted to a partition $\mathbf{P}^v$ of A^v in a natural way. We define

$$\mathbf{P}^v := \{\{\bar{a} \in A^v : (a_1,\ldots,a_v,a_v,\ldots,a_v) \in P\}\colon P \in \mathbf{P}\}.$$

In the same way we define for a labeling $\delta\colon \mathbf{P}^v \to \mathcal{R}$ the A^v column vector $b^{\mathbf{P}}_\delta$ over $\mathcal{R}$. Since the definitions and arguments are very similar, we simultaneously carry out our investigations for all three different extensions.

Definition 3.4.3. For two τ-structures $\mathfrak{A}$ and $\mathfrak{B}$ let $\mathrm{Part}^k(\mathfrak{A},\mathfrak{B})$ be the set of partial isomorphisms p between $\mathfrak{A}$ and $\mathfrak{B}$ with $|dom(p)| \leq k$. For $\star \in \{\mathrm{slv},\mathrm{sim},\mathrm{rk}\}$, a partial isomorphism $p \in \mathrm{Part}^k(\mathfrak{A},\mathfrak{B})$, a set $M \subseteq \mathrm{Part}^k(\mathfrak{A},\mathfrak{B})$ and an arity n, the property $prp^\star(M)$

of the partial isomorphism p is defined as follows:

$$prp^\star(M) \begin{cases} \text{For all } (v,w) \in \hat{m},\ m \leq n, \text{ all rings } \mathcal{R} \text{ and all } C \subseteq dom(p) \text{ there are partitions} \\ \mathbf{P} \text{ of } A^v \times A^w,\ \mathbf{Q} \text{ of } B^v \times B^w \text{ and a bijection } f\colon \mathbf{P} \to \mathbf{Q} \text{ so that} \\ \quad \bullet \text{ either we have } v+w=1 \text{ and } |\mathbf{P}| = |\mathbf{Q}| = |A|, \text{ thus } f \text{ is a bijection from} \\ \quad\quad A \text{ to } B, \text{ or } (cond^\star) \text{ holds, and} \\ \quad \bullet \text{ for all } P \in \mathbf{P}, \bar{a} \in P, \bar{b} \in f(P) \text{ with } a_i = a_j \text{ iff } b_i = b_j \text{ for all } i,j \leq m \text{ and} \\ \quad\quad |C \cup \bar{a}| \leq k \text{ we have } (p \restriction C) \cup \{(a_1,b_1),\dots,(a_m,b_m)\} \in M. \end{cases}$$

The conditions $(cond^\star)$ referred to in the definition of the property $prp^\star(M)$ are given by: for all labelings $\gamma\colon \mathbf{P} \to \mathcal{R}$ and...

$$\begin{aligned} (\text{for } slv): &\begin{cases} \text{for all labelings } \delta\colon \mathbf{P}^v \to \mathcal{R} \text{ the linear system } (M^{\mathbf{P}}_\gamma, b^{\mathbf{P}}_\delta) \text{ is solv-} \\ \text{able iff } (M^{\mathbf{Q}}_{\gamma\circ f^{-1}}, b^{\mathbf{Q}}_{\delta\circ f^{-1}}) \text{ is solvable,} \end{cases} \\ (\text{for } sim): &\begin{cases} \text{for all labelings } \delta\colon \mathbf{P} \to \mathcal{R} \text{ the matrix } M^{\mathbf{P}}_\gamma \text{ is similar to } M^{\mathbf{P}}_\delta \text{ iff} \\ M^{\mathbf{Q}}_{\gamma\circ f^{-1}} \text{ is similar to } M^{\mathbf{Q}}_{\delta\circ f^{-1}}, \end{cases} \\ (\text{for } rk): &\left\{ rk(M^{\mathbf{P}}_\gamma) = rk(M^{\mathbf{Q}}_{\gamma\circ f^{-1}}). \right. \end{aligned}$$

Furthermore we define

$$\begin{aligned} [I^\star]^k_0 &:= \mathrm{Part}^k(\mathfrak{A},\mathfrak{B}), \\ [I^\star]^k_{l+1} &:= \left\{ p \in [I^\star]^k_l \colon p \text{ has the property } prp^\star([I^\star]^k_l) \right\}. \end{aligned}$$

Finally we set $[I^\star]^k(\mathfrak{A},\mathfrak{B}) := \bigcap_{l\in\omega} [I^\star]^k_l$, which is the *$n$-ary (solve, similarity, rank) back and forth system over k variables for the structures $\mathfrak{A}$ and $\mathfrak{B}$*.

As for traditional Ehrenfeucht-Fraïssé games, the defined algebraic relation between structures via back and forth systems can be described by a game. The *n-ary (solve, similarity, rank) k-pebble partition game* $\mathcal{G}^{\mathrm{slv}}_{n,k}(\mathfrak{A},\mathfrak{B})$, $\mathcal{G}^{\mathrm{sim}}_{n,k}(\mathfrak{A},\mathfrak{B})$, $\mathcal{G}^{\mathrm{rk}}_{n,k}(\mathfrak{A},\mathfrak{B})$ is played by two players, Duplicator and Spoiler, on structures $\mathfrak{A}$ and $\mathfrak{B}$ by means of the following rules. There are k pairs of pebbles $(x_1,y_1),\dots,(x_k,y_k)$ which can be placed on elements of the structures. Positions in this game are partial mappings $h : \{1,\dots,k\} \to A \times B$. The initial position is $h = \emptyset$, i.e. no pebbles are placed yet. In each round Spoiler first chooses two integers $v,w \geq 0$ such that $1 \leq v + w =: m \leq n$ and then picks up m pairs of corresponding pebbles in a specific order. If $v + w = 1$, then the play continues as in the usual k-pebble bijection game. Otherwise, Spoiler selects a finite ring $\mathcal{R}$ and the play proceeds as follows:

- Duplicator chooses partitions $\mathbf{P}$ of $A^v \times A^w$, $\mathbf{Q}$ of $B^v \times B^w$ and a bijection $f\colon \mathbf{P} \to \mathbf{Q}$.

She looses directly if there is a labeling $\gamma\colon \mathbf{P} \to \mathcal{R}$ and

$$\text{(solve)} : \begin{cases} \text{a labeling } \delta\colon \mathbf{P}^v \to \mathcal{R} \text{ such that the linear system } (M^{\mathbf{P}}_\gamma, b^{\mathbf{P}}_\delta) \text{ is} \\ \text{not solvable iff } (M^{\mathbf{Q}}_{\gamma\circ f^{-1}}, b^{\mathbf{Q}}_{\delta\circ f^{-1}}) \text{ is solvable,} \end{cases}$$

$$\text{(similarity)} : \begin{cases} \text{a labeling } \delta\colon \mathbf{P} \to \mathcal{R} \text{ such that the matrix } M^{\mathbf{P}}_\gamma \text{ is not similar} \\ \text{to } M^{\mathbf{P}}_\delta \text{ iff } M^{\mathbf{Q}}_{\gamma\circ f^{-1}} \text{ is similar to } M^{\mathbf{Q}}_{\delta\circ f^{-1}}, \end{cases}$$

$$\text{(rank)} : \begin{cases} rk(M^{\mathbf{P}}_\gamma) \neq rk(M^{\mathbf{Q}}_{\gamma\circ f^{-1}}). \end{cases}$$

- Spoiler selects a block $P \in \mathbf{P}$ and places the m chosen pebbles (in the same order he selected them first) on a tuple in P and $f(P)$.

Let the resulting position be denoted by h. If $range(h) \in \mathrm{Part}^k(\mathfrak{A},\mathfrak{B})$, then the play continues. Otherwise Duplicator looses. She wins the game if she can force each play to be of infinite duration. There is an adapted version of the game in which for designated elements $\bar{a} \in A, \bar{b} \in B$, $|\bar{a}| = |\bar{b}| = l \leq k$ the starting position is not $h = \emptyset$ but $h(1) = (a_1, b_1), \ldots, h(l) = (a_l, b_l)$. This version is denoted by $\mathcal{G}^\star_{n,k}(\mathfrak{A},\bar{a},\mathfrak{B},\bar{b})$. We specify the connection between these model comparison games (or back and forth systems) and logical equivalence in infinitary logics.

Definition 3.4.4. Let $\mathcal{L}$ be one of the logics $\mathsf{C}^k_{\infty\omega}(slv^{[n]})$, $\mathsf{C}^k_{\infty\omega}(sim^{[n]})$ or $\mathsf{R}^{k,[n]}_{\infty\omega}$. For $p \in \mathrm{Part}^k(\mathfrak{A},\mathfrak{B})$ we say that p *preserves the truth of* $\mathcal{L}$ *on* $\mathfrak{A}$ *and* $\mathfrak{B}$ if for any formula $\varphi(\bar{x}) \in \mathcal{L}$ and any tuple $\bar{c} \subseteq dom(p)$ we have

$$\mathfrak{A} \models \varphi(\bar{c}) \text{ iff } \mathfrak{B} \models \varphi(p\bar{c}).$$

By $[J^\star]^k(\mathfrak{A},\mathfrak{B})$ we denote for $\star \in \{\mathrm{slv}, \mathrm{sim}, \mathrm{rk}\}$ the set of partial isomorphisms with this property.

We want to prove that $[I^\star]^k(\mathfrak{A},\mathfrak{B}) = [J^\star]^k(\mathfrak{A},\mathfrak{B})$ for all $k \geq 1$ and all $\star \in \{\mathrm{slv}, \mathrm{sim}, \mathrm{rk}\}$. Intuitively the correctness of this claim can be explained as follows: Like in the usual k-pebble bijection game, Duplicator has to guarantee that for each realized k-type t the *total number* of realized k-types reachable from t by exchanging the value of one variable is equal in both structures. This is captured by letting Duplicator select a bijection specifying the correspondence of elements in this sense. For instance, she directly looses if her bijection does not respect already pebbled pairs. If there is a reachable k-type with a different number of realizations, then she is likewise not able to present a suitable bijection and Spoiler wins by taking advantage of her deficiency.

Moreover, in the n-ary (solve, similarity, rank) k-pebble partition game, we have to take into account n-ary quantifiers of type *solve*, *similarity* and *rank*. Duplicator has to guarantee that for each realized k-type all "reachable" matrices (definable with at most n variables) are indistinguishable in both structures in terms of solvability of linear

equation systems, similarity or rank. This means that one cannot only count different k-types, but can make statements about their *global arrangement* in both structures. In order to model this, Duplicator has to select partitions of tuples and a bijection such that all definable matrices, with respect to this partitioning are "sufficiently alike". The appropriate conditions of being sufficiently alike are expressed in the rules of the games.

Theorem 3.4.5. $[J^\star]^k(\mathfrak{A},\mathfrak{B}) = [I^\star]^k(\mathfrak{A},\mathfrak{B})$.

Proof. Again let $\mathcal{L}$ be one of the logics $\mathsf{C}^k_{\infty\omega}(slv^{[n]})$, $\mathsf{C}^k_{\infty\omega}(sim^{[n]})$ or $\mathsf{R}^{k,[n]}_{\infty\omega}$.

First we prove $[I^\star]^k(\mathfrak{A},\mathfrak{B}) \subseteq [J^\star]^k(\mathfrak{A},\mathfrak{B})$ by induction on formulas in $\mathcal{L}$. Let $p \in [I^\star]^k(\mathfrak{A},\mathfrak{B})$ be arbitrary. The induction base follows since $[I^\star]^k(\mathfrak{A},\mathfrak{B}) \subseteq \mathrm{Part}^k(\mathfrak{A},\mathfrak{B})$. Also the induction step for (infinitary) conjunctions and for negation is trivial.

For $\varphi(\bar{x}) = \exists^{\geq i} y\psi(\bar{x},y)$ and $\bar{c} \subseteq dom(p)$ with $|\bar{c}| = |\bar{x}|$, choose an appropriate bijection $f\colon A \to B$ according to the closure property $prp^\star([I^\star]^k(\mathfrak{A},\mathfrak{B}))$ of p (for $v = 1, w = 0$). Since for all $a \in A$ we have $(p \restriction \bar{c}) \cup \{(a,fa)\} \in [I^\star]^k(\mathfrak{A},\mathfrak{B})$, we can conclude from the induction hypothesis

$$\begin{aligned} \mathfrak{A} \models \varphi(\bar{c}) \quad &\text{iff} \quad \mathfrak{A} \models \psi(\bar{c},a), \quad \text{for at least } i \text{ different } a \in A \\ &\text{iff} \quad \mathfrak{B} \models \psi(p\bar{c},fa), \quad \text{for at least } i \text{ different } a \in A \\ &\text{iff} \quad \mathfrak{B} \models \varphi(p\bar{c}). \end{aligned}$$

We illustrate how to handle operators from linear algebra for the case of *slv*-quantifiers. Consider a finite ring $\mathcal{R}$, a matrix dimension $(v,w) \in \hat{m}$ with $1 < m \leq n$ and a formula

$$\varphi(\bar{x}) = slv_{\mathcal{R}}\left[(\bar{x}_a, \bar{y}_a, \bar{z}_a)_{a\in\mathcal{R}}\left(\psi_a(\bar{x}_a,\bar{y}_a,\bar{x}), \vartheta_a(\bar{z}_a,\bar{x})\right)_{a\in\mathcal{R}}\right],$$

with $(|\bar{x}_a|,|\bar{y}_a|) = (v,w)$ and $|\bar{z}_a| = v$. For $\bar{c} \subseteq dom(p)$ with $|\bar{c}| = |\bar{x}|$, select appropriate partitions $\mathbf{P}$ and $\mathbf{Q}$ of $A^v \times A^w$ and $B^v \times B^w$ and a bijection $f\colon \mathbf{P} \to \mathbf{Q}$ according to the closure property $prp^\star([I^\star]^k(\mathfrak{A},\mathfrak{B}))$ of p (with respect to v,w). Then it is guaranteed that for all $\bar{a} \in P, \bar{b} \in f(P)$ we have $(p \restriction \bar{c}) \cup \{(\bar{a},\bar{b})\} \in [I^\star]^k(\mathfrak{A},\mathfrak{B})$. It follows by induction hypothesis for all $a \in \mathcal{R}$

$$\mathfrak{A} \models \psi_a(\bar{a},\bar{c}) \quad \text{iff} \quad \mathfrak{B} \models \psi_a(\bar{b},p\bar{c}).$$

Since the same holds for ϑ, there are labelings $\gamma, \delta\colon \mathbf{P} \to \mathcal{R}$ so that

$$M^{\mathfrak{A}}_\psi = M^{\mathbf{P}}_\gamma, M^{\mathfrak{B}}_\psi = M^{\mathbf{Q}}_{\gamma\circ f^{-1}} \text{ and } M^{\mathfrak{A}}_\vartheta = M^{\mathbf{P}}_\delta, M^{\mathfrak{B}}_\vartheta = M^{\mathbf{Q}}_{\delta\circ f^{-1}}.$$

Hence, $(M^{\mathfrak{A}}_\psi,M^{\mathfrak{A}}_\vartheta)$ is solvable over $\mathcal{R}$ iff $(M^{\mathfrak{B}}_\psi,M^{\mathfrak{B}}_\vartheta)$ is solvable over $\mathcal{R}$, i.e.

$$\mathfrak{A} \models \varphi(\bar{c}) \quad \text{iff} \quad \mathfrak{B} \models \varphi(p\bar{c}).$$

We prove the remaining inclusion $[J^\star]^k(\mathfrak{A},\mathfrak{B}) \subseteq [I^\star]^k(\mathfrak{A},\mathfrak{B})$ by induction on l, i.e. we argue that $[J^\star]^k(\mathfrak{A},\mathfrak{B}) \subseteq [I^\star]^k_l(\mathfrak{A},\mathfrak{B})$ for all $l \geq 0$. The induction base follows right from the definitions. Let $l > 0$ and $p \in \mathrm{Part}^k(\mathfrak{A},\mathfrak{B})$ such that p preserves the truth of $\mathcal{L}$. From the induction hypothesis we know that $p \in [I^\star]^k_{l-1}(\mathfrak{A},\mathfrak{B})$. We define for each $v,w \geq 0$, $1 \leq v+w = m \leq n$, $\bar{a} = (\bar{a}_1,\bar{a}_2) \in A^v \times A^w$, $\bar{b} = (\bar{b}_1,\bar{b}_2) \in B^v \times B^w$, each finite ring $\mathcal{R}$ and $\bar{c} \subseteq dom(p)$ the $\mathcal{L}$-types:

$$tp^k_p(\mathfrak{A},\bar{a},\bar{c}) := \{\varphi(\bar{x},\bar{y}) \in \mathcal{L} : |x| + |y| \leq k,\ \mathfrak{A} \models \varphi(\bar{a},\bar{c})\}$$
$$tp^k_p(\mathfrak{B},\bar{b},\bar{c}) := \{\varphi(\bar{x},\bar{y}) \in \mathcal{L} : |x| + |y| \leq k,\ \mathfrak{B} \models \varphi(\bar{b},p\bar{c})\}.$$

With respect to these types we obtain equivalence relations $\sim^{p,\bar{c}}_{\mathfrak{A},k}$ on $A^v \times A^w$ and $\sim^{p,\bar{c}}_{\mathfrak{B},k}$ on $B^v \times B^w$ in the natural way:

$$\bar{a} \sim^{p,\bar{c}}_{\mathfrak{A},k} \bar{a}' :\Leftrightarrow \mathrm{tp}^p_k(\mathfrak{A},\bar{a},\bar{c}) = \mathrm{tp}^p_k(\mathfrak{A},\bar{a}',\bar{c}) \text{ and respectively}$$
$$\bar{b} \sim^{p,\bar{c}}_{\mathfrak{B},k} \bar{b}' :\Leftrightarrow \mathrm{tp}^p_k(\mathfrak{B},\bar{b},\bar{c}) = \mathrm{tp}^p_k(\mathfrak{B},\bar{b}',\bar{c}).$$

The induced partitions $\mathbf{P}_{p,\bar{c}}$ and $\mathbf{Q}_{p,\bar{c}}$ of $A^v \times A^w$ and $B^v \times B^w$ show that p has indeed the property $prp^\star([I^\star]^k_{l-1}(\mathfrak{A},\mathfrak{B}))$. To see this, we first prove that there is a (canonical) bijection between them.

Lemma 3.4.6. *Let $f_{p,\bar{c}}\colon \mathbf{P}_{p,\bar{c}} \to \mathbf{Q}_{p,\bar{c}}$ be a mapping satisfying*

$$f_{p,\bar{c}}([\bar{a}]) = [\bar{b}] \quad \textit{iff} \quad tp^p_k(\mathfrak{A},\bar{a},\bar{c}) = tp^p_k(\mathfrak{B},\bar{b},\bar{c}).$$

Then $f_{p,\bar{c}}$ exists, is uniquely determined and a well-defined bijection.

Proof. Assume that a tuple $\bar{a} \in A$ exists such that for all $\bar{b} \in B$ we have $\mathrm{tp}^p_k(\mathfrak{A},\bar{a},\bar{c}) \neq \mathrm{tp}^p_k(\mathfrak{B},\bar{b},\bar{c})$. In this case the formula $\varphi(\bar{y}) := \exists\bar{x} \bigwedge \mathrm{tp}^p_k(\mathfrak{A},\bar{a},\bar{c})$ would witness that p does not preserve the truth of $\mathcal{L}$ on $\mathfrak{A}$ and $\mathfrak{B}$. Thus, such a mapping $f_{p,\bar{c}}$ exists. In the same manner, the surjectivity is verified. Furthermore, as a direct consequence of the definitions of $\sim^{p,\bar{c}}_{\mathfrak{A},k}$ and $\sim^{p,\bar{c}}_{\mathfrak{B},k}$, one checks that $f_{p,\bar{c}}$ is well-defined and one-to-one. □

For convenience, set $\mathbf{P} := \mathbf{P}_{p,\bar{c}}$, $\mathbf{Q} := \mathbf{Q}_{p,\bar{c}}$ and $f := f_{p,\bar{c}}$. We illustrate the remaining steps for the case $\mathcal{L} = \mathsf{C}^k_{\infty\omega}(slv^{[n]})$. Assume towards a contradiction that there are labelings $\gamma, \delta : \mathbf{P} \to \mathcal{R}$ such that

$$(M^{\mathbf{P}}_\gamma, M^{\mathbf{P}}_\delta) \text{ is solvable iff } (M^{\mathbf{Q}}_{\gamma\circ f^{-1}}, M^{\mathbf{Q}}_{\delta\circ f^{-1}}) \text{ is not solvable.}$$

According to the definitions of $\mathbf{P}$ and $\mathbf{Q}$, all matrices above are definable in $\mathcal{L}$ using as parameters the elements $\bar{c}$. To be precise, set $\varphi(\bar{x},\bar{y}) = (\varphi_a(\bar{x},\bar{y}))_{a\in\mathcal{R}}$ where

$$\varphi_a(\bar{x},\bar{y}) := \bigwedge_{\bar{a}\in P\in\mathbf{P},\gamma(P)=a} \mathrm{tp}^p_k(\mathfrak{A},\bar{a},\bar{c}).$$

Since $M_{\mathfrak{A}}^{\varphi(\bar{c})} = M_{\gamma}^{\mathbf{P}}$, the existence of the labelings γ, δ contradicts the fact that p preserves the truth of $\mathcal{L}$ on $\mathfrak{A}$ and $\mathfrak{B}$.

Finally let $\bar{a} \in P \in \mathbf{P}_{p,\bar{c}}$ and $\bar{b} \in f_{p,\bar{c}}(P) \in \mathbf{Q}_{p,\bar{c}}$ be arbitrary tuples, and assume there is a formula $\varphi(\bar{x},\bar{y}) \in \mathcal{L}$ such that

$$\mathfrak{A} \models \varphi(\bar{a},\bar{c}) \;\Leftrightarrow\; \mathfrak{B} \not\models \varphi(\bar{b},p\bar{c}).$$

This would be a direct contradiction to the definition of $f_{p,\bar{c}}$, thus by induction hypothesis we conclude

$$(p \restriction \bar{c}) \cup \{(a_1,b_1),\ldots,(a_m,b_m)\} \in [J^{\star}]^k(\mathfrak{A},\mathfrak{B}) \subseteq [I^{\star}]_l^k(\mathfrak{A},\mathfrak{B}). \qquad \square$$

Theorem 3.4.5 establishes the connection between the model comparison games and logical equivalence. If for each $k \geq n \geq 1$ we can find two structures $\mathfrak{A}_{k,n}, \mathfrak{B}_{k,n}$ such that $\mathfrak{A}_{k,n} \ncong \mathfrak{B}_{k,n}$, but Duplicators wins $\mathcal{G}_{n,k}^{\mathrm{slv}}(\mathfrak{A},\mathfrak{B})$, then the class $\{\mathfrak{A}_{k,n} : k \geq n \geq 1\}$ is not definable in $\mathsf{C}_{\infty\omega}^{\omega}(slv)$, thus it is not definable in $\mathsf{FP}{+}\mathsf{slv}$.

Corollary 3.4.7. *$\mathfrak{A}$ and $\mathfrak{B}$ are $\mathcal{L}$-equivalent iff $\emptyset \in [J^{\star}]^k(\mathfrak{A},\mathfrak{B}) = [I^{\star}]^k(\mathfrak{A},\mathfrak{B})$.*

There are some important modifications to the games. For instance, by limiting the number of rounds rather than the number of pebbles, one obtains games that capture logical equivalence with respect to $\mathsf{FO}{+}\mathsf{slv}$, $\mathsf{FO}{+}\mathsf{sim}$, $\mathsf{FO}{+}\mathsf{rk}$. We can also restrict the requirements in the properties $prp^{\star}$, e.g. we can force Spoiler to choose the ring out of a restricted set of finite rings. This allows to investigate operators from linear algebra over rings of different characteristics. The next result is due to Dawar and Holm, and it is an important first step into this direction.

Theorem 3.4.8 ([24])**.** *For all primes p, q where $q \equiv 1 \mod p$, there is a class $\mathcal{C}$ of finite graphs which is definable in $\mathsf{FO}{+}\mathsf{rk}_{\mathbb{F}_q}$ if we restrict to quantifiers of arity 2, but which is not definable in $\mathsf{R}_{\infty\omega}^{\omega,[2]}$ if we restrict to rank quantifiers over the ring $\mathbb{F}_p$.*

The games are sophisticated and it is hard to analyze and prove the existence of winning strategies. The main problem is to guarantee the (linear algebraic) properties requested in the rules of the games. For instance, one has to establish conditions which guarantee that all matrices, which are definable with respect to the chosen partitions have the same rank. This becomes even more problematic if we consider quantifiers of arity > 2. Currently we are not able to present applications of these games, though there are many open questions in this regard. The main goal, of course would be to clarify whether the extensions of fixed point logic can be separated from PTIME. Besides that, a more basic question remains open as well, namely to clarify the relationship between the extensions of first-order logic and fixed point logics. Furthermore, the problem solved by Theorem 3.4.8 is open for arities > 2 and general pairs of primes.

Chapter 4.

Hierarchies and Descriptive Complexity

In Chapters 2 and 3 we investigated problems of linear algebra which are not definable in $\mathsf{FP}+\mathsf{C}$ and studied ways to enrich logics. In Chapter 4 we analyzed logics extended by operators from linear algebra which are able to decide solvability of linear equation systems, similarity of matrices, and the rank of definable matrices, respectively. This chapter continues the study in the light of logical hierarchies and descriptive complexity.

In Section 4.1 we review a result of Dawar et al. By exploiting an idea of Hella [44], they proved that rank operators form a strict hierarchy with respect to increasing arities. We notice that their method also applies to extensions by solve quantifiers. Another result of Dawar et al. is presented in Section 4.2. It states that on the domain of ordered structures, logspace modulo counting classes are captured by various extensions of first-order logic. Again, their result was formulated for rank logics but it directly applies to the case of solve and similarity quantifiers as well. In particular, we obtain that on the domain of ordered structures these extensions are equivalent.

4.1. Logical Hierarchies for Operators from Linear Algebra

The arities of operators from linear algebra form a strict hierarchy with respect to logical expressive power. This is true for all introduced kinds of quantifiers (cf. Chapter 3). To obtain this result, we review the original proof presented by Dawar et al. for the case of rank quantifiers [27]. Recall the corresponding infinitary logics, i.e. $\mathsf{C}^{\omega}_{\infty\omega}(\mathit{slv}^{[n]})$, $\mathsf{C}^{\omega}_{\infty\omega}(\mathit{sim}^{[n]})$ and $\mathsf{R}^{\omega,[n]}_{\infty\omega}$ from Section 3.4. Dawar et al. proved the strict hierarchy for the rank logic, i.e. they showed that

$$\mathsf{R}^{\omega,[2]}_{\infty\omega} \lneq \mathsf{R}^{\omega,[3]}_{\infty\omega} \lneq \cdots \lneq \mathsf{R}^{\omega,[n]}_{\infty\omega} \lneq \mathsf{R}^{\omega,[n+1]}_{\infty\omega} \lneq \ldots.$$

By reusing the same arguments we obtain

$$\mathsf{C}^{\omega}_{\infty\omega}(\mathit{slv}^{[2]}) \lneq \mathsf{C}^{\omega}_{\infty\omega}(\mathit{slv}^{[3]}) \lneq \cdots \lneq \mathsf{C}^{\omega}_{\infty\omega}(\mathit{slv}^{[n]}) \lneq \mathsf{C}^{\omega}_{\infty\omega}(\mathit{slv}^{[n+1]}) \lneq \ldots.$$

However, for the extensions by similarity quantifiers we cannot derive the same hierarchy. This is due to the fact that similarity quantifiers are only defined for even arities -

they always decide properties for square matrices. However, the following considerations will reveal that for all $k \geq 1$ it holds that

$$\mathsf{C}^{\omega}_{\infty\omega}(sim^{[k]}) \leq \mathsf{C}^{\omega}_{\infty\omega}(sim^{[2k]}).$$

As pointed out, the underlying idea is to exploit a result due to Hella [44]. Let $\mathcal{Q}_n$ be the class of all generalized Lindström quantifiers of arity $\leq n$. Hella showed that for all $n \geq 1$ there is a query on finite structures which is not definable in $\mathsf{L}^{\omega}_{\infty\omega}(\mathcal{Q}_n)$, but decidable in PTIME. However, just as in the case of CFI-graphs (cf. Section 2.5), the query of Hella can be formulated as a linear equation system over $\mathbb{F}_2$. This was proved by Dawar et al., and moreover they showed that the corresponding equation system can be defined by a first-order formula and has a coefficient matrix of dimension $(n,1)$. In this manner they obtained the desired hierarchy result, since $\mathsf{R}^{\omega,[n]}_{\infty\omega} \leq \mathsf{L}^{\omega}_{\infty\omega}(\mathcal{Q}_n)$.

Lemma 4.1.1. $\mathsf{C}^{\omega}_{\infty\omega}(slv^{[n]})$, $\mathsf{C}^{\omega}_{\infty\omega}(sim^{[n]})$, $\mathsf{R}^{\omega,[n]}_{\infty\omega} \leq \mathsf{L}^{\omega}_{\infty\omega}(\mathcal{Q}_n)$ *for all* $n \geq 2$.

We now present the construction of Hella. Let $\mathcal{G} = (V, E^{\mathcal{G}}, <^{\mathcal{G}})$ be an (undirected) connected $(n+1)$-regular ordered graph. For each $v \in V$ we introduce the set C_v of new vertices defined by

$$C_v := \{(v,w)_0, (v,w)_1 : w \in vE^{\mathcal{G}}\}.$$

Let $S \subseteq V$. The *Hella graph* $\mathcal{D}(\mathcal{G},S)$ is a structure of signature $\tau_n := \{E, R, \prec\}$, where $E, \prec$ are binary and R is an $(n+1)$-ary relation symbol. The universe of $\mathcal{D}(\mathcal{G},S)$ is given by the set $\bigcup_{v\in V} C_v$. The relations are defined as follows:

$$\begin{aligned}
E^{\mathcal{D}(\mathcal{G},S)} &:= \{((v,w)_i, (w,v)_i) : (v,w) \in E^{\mathcal{G}}, i = 0,1\} \\
R^{\mathcal{D}(\mathcal{G},S)} &:= \{((v,w_1)_{i_1} \dots (v,w_{n+1})_{i_{n+1}}) : v \in V, w_1 <^{\mathcal{G}} \cdots <^{\mathcal{G}} w_{n+1}, \\
&\qquad \text{and } \textstyle\sum_j i_j \text{ even iff } v \notin S\} \\
\prec^{\mathcal{D}(\mathcal{G},S)} &:= \{((v,w)_i, (x,y)_j) : v <^{\mathcal{G}} x \text{ or } v = x \text{ and } w <^{\mathcal{G}} y\}
\end{aligned}$$

The construction of Hella can be seen as an adaption of the one used by Cai et al. Every vertex in the original graph is replaced by a gadget and every edge by a pair of edges connecting the different gadgets. The main difference to the CFI-construction is that the sophisticated parity property is not defined by designated *inner nodes* and twists of edges, but is encoded into the $(n+1)$-ary relation $R^{\mathcal{D}(\mathcal{G},S)}$. Accordingly, the twists are also encoded in the relation $R^{\mathcal{D}(\mathcal{G},S)}$. The preorder $\prec^{\mathcal{D}(\mathcal{G},S)}$ has width two since all *incomparable pairs* are vertices of the form $(v,w)_0, (v,w)_1$ for some $(v,w) \in E^{\mathcal{G}}$.

Theorem 4.1.2 (Hella [44])**.** *For all* $S, T \subseteq V$ *the graphs* $\mathcal{D}(\mathcal{G},S)$ *and* $\mathcal{D}(\mathcal{G},T)$ *are isomorphic iff* $|S|$ *and* $|T|$ *have the same parity.*

Thus, each connected regular graph $\mathcal{G}$ gives rise to precisely two isomorphism classes of corresponding Hella graphs. We fix some vertex $u \in V$ and two representatives from these classes, i.e. we distinguish between the *even Hella graphs* $\mathcal{D}(\mathcal{G},\emptyset)$ and the *odd Hella graphs* $\mathcal{D}(\mathcal{G},\{u\})$.

Theorem 4.1.3 (Hella [44])**.** *For each $n \geq 1$ there is a family of $(n+1)$-regular connected graphs $(\mathcal{G}_k)_{k\geq 1}$ such that for every sentence $\varphi \in \mathsf{L}^{\omega}_{\infty\omega}(\mathcal{Q}_n)$ there is $k_\varphi \geq 1$ such that for all $k \geq k_\varphi$ we have*

$$\mathcal{D}(\mathcal{G}_k,\emptyset) \models \varphi \text{ iff } \mathcal{D}(\mathcal{G}_k,\{u\}) \models \varphi.$$

Actually, the graphs can be distinguished in LOGSPACE. As a result we obtain that for each arity $n \geq 1$ the logic $\mathsf{L}^{\omega}_{\infty\omega}(\mathcal{Q}_n)$ does not capture PTIME. Since $\mathsf{FP{+}C} \leq \mathsf{L}^{\omega}_{\infty\omega}(\mathcal{Q}_1)$, this result extends the one which Cai et al. had obtained. However, the constructed classes are based on vocabularies of growing complexity. Intuitively it seems reasonable that generalized quantifiers of arity n are insufficient if structures contain relations of arity $n+1$. In particular, it remains possible that the logic $\mathsf{L}^{\omega}_{\infty\omega}(\mathcal{Q}_n)$ captures PTIME on the domain of finite graphs for some $n \geq 2$.

Theorem 4.1.4 (Dawar et al. [27])**.** *For all $n \geq 2$ there is a sentence $\varphi \in \mathsf{C}^{\omega}_{\infty\omega}(slv^{[n+1]})$ of signature τ_n such that for all $(n+1)$-regular connected graphs $\mathcal{G}$ we have*

$$\mathcal{D}(\mathcal{G},\emptyset) \models \varphi \text{ and } \mathcal{D}(\mathcal{G},\{u\}) \models \neg\varphi.$$

Proof. We argue that there is a first-order interpretation of a linear equation system $\mathcal{S}$ over $\mathbb{F}_2$ in $\mathcal{D}(\mathcal{G},S)$ which is solvable iff $|S|$ is even. For each vertex $(v,w)_i$ in $\mathcal{D}(\mathcal{G},S)$, we introduce a variable $x_{(v,w)_i}$. The system includes the following equations:

$$\text{for all incomparable pairs } (v,w)_0,(v,w)_1: \quad x_{(v,w)_0} + x_{(v,w)_1} = 1 \tag{4.1.1}$$

$$\text{for each edge } ((v,w)_i,(v,w)_i): \quad x_{(v,w)_i} + x_{(v,w)_i} = 0 \tag{4.1.2}$$

$$\text{for all } ((v,w_1)_{i_1}\dots(v,w_{n+1})_{i_{n+1}}) \in R^{\mathcal{D}\mathcal{G},S}: \quad x_{(v,w_1)_{i_1}} + \dots + x_{(v,w_{n+1})_{i_{n+1}}} = 0. \tag{4.1.3}$$

If $S = \emptyset$, a solution for the system $\mathcal{S}$ is given by setting $x_{(u,v)_i} = i$. Towards a contradiction, assume that the system $\mathcal{S}$ is solvable although $S = \{u\}$. Each solution defines an isomorphism f between $\mathcal{D}(\mathcal{G},\emptyset)$ and $\mathcal{D}(\mathcal{G},\{u\})$ by setting

$$f((v,w)_i) = \begin{cases} (v,w)_0 & \text{iff } x_{(v,w)_i} = 0 \\ (v,w)_1 & \text{iff } x_{(v,w)_i} = 1. \end{cases}.$$

First of all, one can check that f is a bijection which respects the edge relation E and the preorder $\prec$. This is guaranteed by the equations (4.1.1) and (4.1.2). Furthermore, $((v,w_1)_{i_1}\dots(v,w_{n+1})_{i_{n+1}}) \in R^{\mathcal{D}(\mathcal{G},\emptyset)}$ iff $\sum_j i_j$ is even. Note that we have

$$f((v,w)_i) = (v,w)_{x_{(v,w)_i}}.$$

Furthermore, equations of type (4.1.3) guarantee that

$$((v,w_1)_{i_1} \dots (v,w_{n+1})_{i_{n+1}}) \in R^{\mathcal{D}(\mathcal{G},\{u\})} \text{ iff } \sum\nolimits_j x_{(v,w_j)_{i_j}} \text{ is even.}$$

By combining these facts and reusing the equations (4.1.1), one verifies via an easy calculation that f is an isomorphism. But since $\mathcal{D}(\mathcal{G},\emptyset)$ is not isomorphic to $\mathcal{D}(\mathcal{G},\{u\})$, we conclude that the system $\mathcal{S}$ is solvable iff $\mathcal{D}(\mathcal{G},S)$ is an even Hella graph.

It remains to show that the described linear system is definable as an $(n+1)$-ary relation in $\mathsf{C}^{\omega}_{\infty\omega}(slv^{[n+1]})$. As pointed out, one can use a coefficient matrix of dimension $(n,1)$, i.e. the system is definable by first-order formulas $\psi(\bar{x},y), \vartheta(\bar{x})$ where $|\bar{x}| = n$. To be more precise, equations of type (4.1.1) can be defined at tuples whose individual components are $(v,w)_i$, equations of type (4.1.2) at tuples whose first two components are connected by an edge and equations of type (4.1.3) at tuples of the form $((v,w_1)_{i_1} \dots (v,w_n)_{i_n})$ which form a continuous segment with respect to the preorder $\prec$. □

Together with our foregoing explanations and Theorem 3.2.3, this result implies the hierarchies for the logics $\mathsf{C}^{\omega}_{\infty\omega}(slv)$ and $\mathsf{C}^{\omega}_{\infty\omega}(sim)$ that we have depicted in the beginning of the current section. For the case of rank logics, we still have to argue that deciding solvability of linear equation systems can be reduced to rank queries without increasing the arity. This is true for equation systems over fields [27].

Lemma 4.1.5. *For each $\varphi \in \mathsf{C}^{\omega}_{\infty\omega}(slv^{\mathcal{F},[n]})$ there is an equivalent formula $\psi \in \mathsf{R}^{\omega,[n]}_{\infty\omega}$.*

Proof. A linear equation system (A,b) over a field is solvable iff for all columns in A the addition of b does not change its column rank. Thus, we can easily find an equivalent formula without increasing the arity. □

The hierarchy results can be considered from another point of view. They attest that the investigated properties from linear algebra are structurally more complex compared to ordinary n-ary counting. The latter is known to be reducible to unary counting (for fixed point logics). We stress that it is a relevant open question whether or not quantifiers of bounded arity yield the same expressive power on the domain of finite graphs.

4.2. Capturing Logspace Modulo Counting Classes

Dawar et al. [27] characterized the descriptive complexity of first-order logic extended by rank operators for a fixed ring $\mathcal{R}$ on the domain of ordered structures. It turns out that their arguments apply to the extension of FO by operators deciding solvability of linear equation systems. Thus, on ordered structures (and for special fixed rings) the specific kind of operator from linear algebra (cf. Chapter 3) has no influence on the resulting expressive power with respect to first-order extensions. This result is a first step towards

relating the various operators to each other. However, since FP already captures PTIME on the domain of ordered structures, the results are useless for the corresponding extensions of fixed point logic.

Theorem 3.1.2 states that the introduced extensions of FO (even those resulting while fixing the underlying ring) can express all queries definable in FO+STC. This already shows that on ordered structures, $\mathsf{SLOGSPACE} \leq \mathsf{FO}{+}\mathsf{slv}_{\mathcal{R}}$ for all finite rings $\mathcal{R}$. However, it seems unlikely that the data complexity of $\mathsf{FO}{+}\mathsf{slv}_{\mathcal{R}}$ is contained in SLOGSPACE. In particular, we believe that its datacomplexity crucially depends on the characteristics of the underlying ring $\mathcal{R}$. Hence we have to consider more appropriate complexity classes.

In [15], Buntrock et al. introduced *logarithmic space modulo counting classes* in analogy to prior studied modulo counting classes for PTIME. They share many common properties, e.g. closure under Boolean operations or reductions. The class $\mathsf{MOD}_k\mathsf{L}$ consists of problems decidable by nondeterministic logspace Turing machines which accept inputs iff k does not divide the number of accepting computations. For all primes k, Buntrock et al. proved that many problems of linear algebra over $\mathbb{Z}_k$ are complete for $\mathsf{MOD}_k\mathsf{L}$ with respect to NC^1 many-one reductions. Further work of Hertrampf et al. [45] revealed that $\mathsf{MOD}_k\mathsf{L}$ is even closed under oracle queries to $\mathsf{MOD}_k\mathsf{L}$ machines in this case.

Definition 4.2.1. Let $\#\mathsf{L}$ be the class of functions $f\colon \Sigma^\star \to \omega$ for which there is a nondeterministic logspace bounded Turing machine so that $f(x)$ equals the number of accepting computations when started on input x.

For $k \geq 2$, the complexity class $\mathsf{MOD}_k\mathsf{L}$ is defined as containing precisely all problems $A \subseteq \Sigma^\star$ for which an $f \in \#\mathsf{L}$ exists such that for all $x \in \Sigma^\star$ we have

$$x \in A \text{ iff } f(x) \not\equiv 0 \mod k.$$

We summarize some important results used throughout the following argumentation. From now on let p be a prime.

Theorem 4.2.2 ([15, 45])**.** *For the complexity class* $\mathsf{MOD}_p\mathsf{L}$*, the following holds:*

(i) $\mathsf{MOD}_p\mathsf{L}$ *is closed under intersection, union, complement, many-one* NC^1 *and even Turing* $\mathsf{MOD}_p\mathsf{L}$ *reductions.*

(ii) Deciding the rank of a matrix over $\mathbb{F}_p$ *is complete for* $\mathsf{MOD}_p\mathsf{L}$ *with respect to* NC^1 *many-one reductions.*

(iii) Deciding solvability of a linear equation system over $\mathbb{F}_p$ *is complete for* $\mathsf{MOD}_p\mathsf{L}$ *with respect to many-one* NC^1 *reductions.*

Dawar et al. [27] proved that $\mathsf{FO}{+}\mathsf{rk}_{\mathbb{F}_p}$ captures $\mathsf{MOD}_p\mathsf{L}$ on finite structures. Moreover, their arguments show that also $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p}$ captures $\mathsf{MOD}_p\mathsf{L}$ on this domain. For this reason

we obtain on ordered structures:

$$\mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p} \equiv \mathsf{FO}{+}\mathsf{sim}_{\mathbb{F}_p} \equiv \mathsf{FO}{+}\mathsf{eqv}_{\mathbb{F}_p} \equiv \mathsf{FO}{+}\mathsf{rk}_{\mathbb{F}_p} \equiv \mathsf{MOD}_p\mathsf{L}.$$

In fact, each formula in $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p}$ contains a fixed number of nesting of $slv_{\mathbb{F}_p}$ operators. The preceding theorem states that each single operator can be decided by a $\mathsf{MOD}_p\mathsf{L}$ machine and furthermore that each $\mathsf{MOD}_p\mathsf{L}$ machine can be simulated by a $\mathsf{MOD}_p\mathsf{L}$ machine. Thus we obtain $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p} \leq \mathsf{MOD}_p\mathsf{L}$.

For the remaining direction consider a vocabulary τ and a class $\mathcal{C} \subseteq ord[\tau]$ of finite ordered structures with $\mathcal{C} \in \mathsf{MOD}_p\mathsf{L}$. We choose a nondeterministic Turing machine M that decides the class $\mathcal{C}$ and has a space bound of $c \log n$ for a fixed constant $c > 0$. We assume that M has precisely one accepting configuration and that its configuration graph G_M is acyclic. This can be realized by equipping M with a step counter. An input $x \in \Sigma^*$ is accepted by M iff the number of paths from the initial to the accepting configuration in G_M is not a multiple of p.

Lemma 4.2.3 ([55]). *There are* FO *formulas* $\varphi_{init}(\bar{x}), \varphi_{final}(\bar{x}), \varphi_{next}(\bar{x},\bar{y})$ *such that for all structures* $\mathfrak{A} \in ord[\tau]$ *the transition relation in the configuration graph of* M *started with input* $\langle A \rangle$ *is encoded by* $\varphi^{\mathfrak{A}}_{next}$*. The accepting configuration of* M *is encoded by* $\varphi^{\mathfrak{A}}_{final}$ *and the initial configuration by* $\varphi^{\mathfrak{A}}_{init}$*.*

The central idea for the following result is due to Cook [20]. He presented a way to reduce the NLOGSPACE complete problem of (directed) graph accessibility, denoted by Reach, to the problem of deciding singularity of integer matrices. For the complexity classes $\mathsf{MOD}_p\mathsf{L}$, it is complete to decide whether in an acyclic directed graph the number of paths between to designated vertices is not divisible by p. In the following, this query is denoted by Reach_p. By our knowledge, a relation between the two complexity classes $\mathsf{MOD}_p\mathsf{L}$ and NLOGSPACE has yet not been established. Stated otherwise, it remains unanswered whether the problems Reach and Reach_p are equivalent, e.g. with respect to NC^1 many-one reductions. However, Dawar et al. showed that the idea of Cook can also be adapted for Reach_p.

For an acyclic directed graph $\mathcal{G}$ on n vertices consider the corresponding adjacency matrix $M_\mathcal{G}$ over $\mathbb{Z}$. It is a simple observation that the entry (s,t) in the matrix $M^i_\mathcal{G}$ equals the total number of different paths of length i from s to t in $\mathcal{G}$. Since $\mathcal{G}$ is acyclic this implies $M^n_\mathcal{G} = 0$. Let E be the identity matrix appropriate for $M_\mathcal{G}$. Then $(E - M_\mathcal{G})$ is invertible because

$$(E - M_\mathcal{G}) \cdot (E + M^1_\mathcal{G} + M^2_\mathcal{G} + \cdots + M^{n-1}_\mathcal{G}) = E.$$

Thus, the entry at position (s,t) in $(E - M_\mathcal{G})^{-1}$ equals the total number of different paths from s to t in $\mathcal{G}$. Note that $det(E - M_\mathcal{G}) = 1$, thus by the adjugate rule this number

equals, up to sign, the determinant of $(E - M_{\mathcal{G}})_{ts}$. The matrix $(E - M_{\mathcal{G}})_{ts}$ results from $(E - M_{\mathcal{G}})$ by deleting row t and column s. We conclude that there is a path from s to t in $\mathcal{G}$ iff $(E - M_{\mathcal{G}})_{ts}$ is nonsingular over $\mathbb{Z}$. In particular, the number of paths from s to t is not congruent 0 modulo p iff $(E - M_{\mathcal{G}})_{ts}$ is nonsingular over $\mathbb{F}_p$. By the preceding lemma, there are FO formulas that define the adjacency matrix of the configuration graph of the Turing machine M besides its initial and accepting configurations. It remains to show that $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p}$ is able to express nonsingularity of definable (square) matrices.

Lemma 4.2.4. *Let $(\varphi_a(\bar{x}_a,\bar{y}_a))_{a\in\mathbb{F}_p}$ be a sequence of formulas in $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p}$ that encode a square matrix over $\mathbb{F}_p$. Then there is $\psi \in \mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p}$ such that for all structures $\mathfrak{A}$*

$$\mathfrak{A} \models \psi \text{ iff } M_{\mathfrak{A}}^{\varphi} \text{ is nonsingular.}$$

Proof. Let $\vartheta_1 := (\bar{v}_1 = \bar{z})$ and $\vartheta_a := 0$ for all $a \in \mathbb{F}_p \setminus \{1\}$. It suffices to define

$$\psi := \forall \bar{z} \left[\mathit{slv}_{\mathcal{R}} \left[(\bar{x}_a, \bar{y}_a, \bar{v}_a)_{a\in\mathcal{R}} \left(\varphi_a(\bar{x}_a,\bar{y}_a), \vartheta_a(\bar{v}_a)\right)_{a\in\mathcal{R}}\right]\right]. \qquad \square$$

Theorem 4.2.5. *Let p be a prime. On ordered structures we have*

$$\mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p} = \mathsf{FO}{+}\mathsf{sim}_{\mathbb{F}_p} = \mathsf{FO}{+}\mathsf{rk}_{\mathbb{F}_p} = \mathsf{MOD}_p\mathsf{L}.$$

Proof. Recall that the rank of a matrix over $\mathbb{F}_p$ can be decided in $\mathsf{MOD}_p\mathsf{L}$. $\square$

Like in the case of $\mathsf{FO}{+}\mathsf{TC}$, we conclude that on ordered structures the logics $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{F}_p}$, $\mathsf{FO}{+}\mathsf{sim}_{\mathbb{F}_p}$, $\mathsf{FO}{+}\mathsf{rk}_{\mathbb{F}_p}$ possess a normal form, i.e. every sentence is equivalent to a sentence with only one occurrence of the corresponding operator.

Recall that every formula in $\mathsf{FO}{+}\mathsf{STC}$ can be transformed into an equivalent formula in $\mathsf{FO}{+}\mathsf{slv}_{\mathcal{R}}$ for each finite ring $\mathcal{R}$. If this was also true for $\mathsf{FO}{+}\mathsf{TC}$, the foregoing theorem would yield that $\mathsf{NLOGSPACE} \subseteq \mathsf{MOD}_p\mathsf{L}$. Thus it seems hard to obtain such a relation. However, it may be possible to show that undirected graph accessibility is not definable in $\mathsf{FO}{+}\mathsf{rk}$ on the domain of all finite structures. A result in this direction would not have similar impacts on algorithmic complexity theory.

Restricting our considerations again to the ordered setting, a recent result of Bourke et al. [14] shows that $\mathsf{FO}{+}\mathsf{rk}$ is able to define directed reachability also on the class of all ordered planar graphs. Remarkably, the authors expect that $\mathsf{ULOGSPACE} = \mathsf{NLOGSPACE}$. In this case the query Reach would be definable in $\mathsf{FO}{+}\mathsf{rk}$ on the class of all finite ordered graphs.

Dawar et al. [27] suggest to investigate alternating graph reachability as well, which is known to be a PTIME complete problem. It is unlikely that $\mathsf{FO}{+}\mathsf{rk}$ is able to express this query since this would imply $\mathsf{PTIME} = \mathsf{NC}^2$. Thus, alternating reachability is a promising candidate for showing the expected separation of $\mathsf{FO}{+}\mathsf{rk}$ and $\mathsf{FP}{+}\mathsf{rk}$.

Conclusion and Future Work

Motivated by the seminal work of Atserias et al. [7], in this thesis the descriptive complexity of problems from linear algebra was studied. We analyzed corresponding extensions of logics that have been proven successful in the area of finite model theory. Investigations are orientated on the pioneering papers of Blass et al. [12], Dawar et al. [27] as well as Dawar and Holm [24]. This thesis makes some contributions to this current topic of research and points out new aspects for the following investigations. Moreover, it reviews many of the known results in order to present a comprehensive overview.

The results of Atserias et al. showed that over each finite Abelian group FP+C cannot express solvability of linear equation systems. Although Abelian groups cannot be embedded into fields in general, all related studies have focused on problems of linear algebra defined over finite fields (or infinite domains $\mathbb{Z}$ and $\mathbb{Q}$). From the well known structure theorem for finite Abelian groups, we know that for each Abelian group there is an operation extending the group to a finite commutative ring. With this in mind, we have extended the perspective and have considered linear algebra over finite commutative rings. It is a known fact that a remarkable amount of problems of linear algebra is definable in FP+C. In Chapter 2 we have demonstrated that this remains true for many queries over finite rings: we proved that matrix multiplication and matrix singularity can be defined in FP+C over arbitrary finite commutative rings. Definability for the matrix determinant and the characteristic polynomial in FP+C has been clarified only partially.

The minimal polynomial is a very important algebraic parameter for matrices over fields. Its coefficients can be characterized as the solution of a linear equation system which has a very specific form. An exploitation of this fact provided an FP+C-definition of the minimal polynomial for matrices over finite fields and over $\mathbb{Q}$. Apart from that, we established new classes of problems, primarily from the area of linear algebra which are not definable in FP+C, however decidable in polynomial time. This fact underlines the important role of linear algebra with respect to classes of structures separating FP+C from PTIME.

These findings have led us to study various extensions of FP+C by operators from linear algebra in Chapter 3. These extensions are oriented on the rank logics studied by Dawar et al. [27]. In particular, we have introduced extensions by operators that decide solvability of linear equation systems, similarity of matrices, equivalence of matrices, and rank of matrices. Restricted to finite fields, we have obtained a clear hierarchy in which the rank

logics subsume all other extensions. As many of the well-known characterizations from linear algebra fail over rings, some relations between the newly introduced logics remain open in the general case. The operators from linear algebra are very powerful, thus it is not surprising that it is difficult to obtain an intuition for their semantics. Actually, we lack convenient structural characterizations which makes the meaning of formulas hard to capture. Hence we have started to search for some natural graph properties which are strongly connected to the queries from linear algebra. Especially circuit value problems over modulo gates and the (σ,ρ)-subset problem for graphs turned out to be relevant in this concern, cf. Section 3.1 and 3.3. Furthermore, we have adapted the newly introduced partition games to our extensions, which Dawar and Holm studied for rank logics in [24].

In Chapter 4 we have taken up further results of Dawar et al. [27]. They proved the strictness of the arity hierarchy for rank operators. Their proof immediately applies to our extensions, thus we have derived a strict hierarchy of arities for solvability, similarity and equivalence operators. Moreover, Dawar et al. obtained a capturing result for first-order logic extended by rank operators for $\mathbb{Z}_p$ on the class of ordered structures. Their result extends to first-order logic with operators for solvability, for similarity and for equivalence. Hence, on the class of ordered structures the different kinds of extensions are equivalent. In the following part, we present many ideas which can trigger off further research.

First-order extensions. Currently we are not aware of any non-trivial limits in the expressive power for the proposed logics. An analysis of the extensions $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{Z}_m}$ for integers $m \geq 2$ seems to be most promising. Whenever m is a prime, we have seen in Section 4.2 that $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{Z}_m}$ captures $\mathsf{MOD}_m\mathsf{L}$ on the domain of ordered structures. Here $\mathsf{MOD}_m\mathsf{L}$ is the class of problems decidable by a nondeterministic logspace Turing machine that accepts an input iff the number of accepting paths is no multiple of m. However, the relation does remain unclarified for composite integers m. It is not known whether in this general case $\mathsf{MOD}_m\mathsf{L}$ is closed under intersection or complement. This is of course a necessary condition for extending the capturing result. It also remains unknown whether there is a relevant algorithmic complexity class captured by $\mathsf{FO}{+}\mathsf{slv}$ on the class of ordered structures. Can we define transitive closure in $\mathsf{FO}{+}\mathsf{slv}$, i.e. is $\mathsf{NLOGSPACE} \leq \mathsf{FO}{+}\mathsf{slv}$? It appears unlikely that alternating reachability is definable in $\mathsf{FO}{+}\mathsf{slv}$, since this would imply $\mathsf{NC}^2 = \mathsf{PTIME}$. As a result, alternating reachability is a promising candidate for limiting the expressive power of $\mathsf{FO}{+}\mathsf{slv}$. Allender et al. [3] showed that over the rationals, unsolvability can be reduced to solvability of linear equation systems. So far, a similar result is not known for systems over finite rings. Clearly, we can translate each formula into an equivalent one, only using operators for a single finite ring. We hope that in general, one application of an operator is sufficient. The same investigations are reasonable for quantifiers deciding similarity and matrix rank. Over finite fields, matrix rank characterizes many other notions. It has not been discussed

whether we can simulate rank operators over finite rings by those defined over finite fields, i.e. whether we have $\mathsf{FO}{+}\mathsf{rk}^{\mathcal{F}_\star} \equiv \mathsf{FO}{+}\mathsf{rk}$. Imaginably, there is a more sensible notion of matrix rank over commutative rings which has stronger connections to solvability of linear equation systems. A significant open issue concerns the algorithmic complexity of matrix rank over rings: can we show that $\mathsf{FO}{+}\mathsf{rk} \leq \mathsf{PTIME}$? In order to obtain a deeper understanding of the descriptive complexity, one should continue to search for structural graph properties that are intimately related to these queries from linear algebra. For instance, the problem of counting the number of paths between two designated vertices modulo m ($\textsc{Reach}_m$) seems to be promising, cf. Section 3.1. It is possible that the extension which results by adding operators for deciding solvability of linear equation systems to first-order logics is equivalent to first-order logic extended by operators deciding $\textsc{Reach}_m$. This is true on the domain of ordered structures, cf. Section 4.1.

The mathematical field of *algebraic graph theory* reveals the connections of algebraic parameters of matrices and properties from graph theory [9, 34]. Unfortunately, matrices in this area are typically studied over the reals, rendering most of the results are non-applicable for our purpose. Still, it seems worthwhile to explore the manifold ideas of algebraic graph theory. There also are interesting combinatorial approaches to various concepts from linear algebra. For instance, the determinant of a matrix can be characterized in terms of a cycle decomposition of a special associated graph, cf. [58, 63]. Since singularity of matrices is definable in all introduced first-order extensions, these characterizations might help to gain deeper insight into the structure of definable classes.

Different Characteristic We maintain the conjecture that operators from linear algebra are incomparable if considered for rings of different characteristic. For extensions of first-order logic, the circuit value problem over modulo gates may be an appropriate candidate for obtaining separation results in this concern, i.e. for separating $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{Z}_p}$ and $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{Z}_q}$ for different primes p,q. It is a simple observation that this problem is complete for $\mathsf{MOD}_m\mathsf{L}$ for all integers m, and we have seen that it can be expressed in $\mathsf{FO}{+}\mathsf{slv}_{\mathbb{Z}_m}$. Solving this issue would probably help to make progress in understanding the open relation between $\mathsf{FO}{+}\mathsf{slv}$ and $\mathsf{FP}{+}\mathsf{slv}$. To clarify the expressive power between $\mathsf{FP}{+}\mathsf{slv}_{\mathbb{Z}_p}$ and $\mathsf{FP}{+}\mathsf{slv}_{\mathbb{Z}_q}$ for different primes p and q, we may engage the queries itself, i.e. show that solvability of linear systems over $\mathbb{Z}_p$ cannot be defined in $\mathsf{FP}{+}\mathsf{slv}_{\mathbb{Z}_q}$.

Linear algebra and counting In Chapter 3 we have analyzed and related logical extensions by various operators from linear algebra. Whether the obtained inclusions are strict, is a question which naturally arises. In particular, this concern relates to the expressive power of $\mathsf{FP}(\mathit{slv})$ and $\mathsf{FP}(\mathit{eqv})$. Rank terms directly simulate ordinary counting terms, thus we can abandon counting terms in $\mathsf{FP}{+}\mathsf{rk}$. On the contrary, whether we can abandon them in $\mathsf{FP}{+}\mathsf{slv}$, is a question which is left unanswered. We claim that this is

not possible. We have shown that modulo counting is definable in $\mathsf{FP}(slv)$. However, the Härtig and Rescher quantifier seem to be undefinable in $\mathsf{FP}(slv)$. Noteworthy, the Härtig quantifier is definable in $\mathsf{FP}(eqv)$, however the question if the Rescher quantifier is definable remains open as well. Having a better algorithmic understanding for matrix rank and similarity over finite rings would be profitable with respect its descriptive complexity as well. Refining the ideas of [6] seems to be a promising possibility to tackle this question. Finally, we have to face the problem of clarifying definability for the characteristic polynomial over arbitrary finite rings in $\mathsf{FP}{+}\mathsf{C}$, see Chapter 2.

Fixed point extensions and pebble games Certainly, the main task is to find classes that can be used to separate $\mathsf{FP}{+}\mathsf{rk}^{\mathcal{F}_\star}$ from PTIME, or to prove that $\mathsf{FP}{+}\mathsf{rk}^{\mathcal{F}_\star}$ captures PTIME. The introduced pebble games may provide the appropriate technical method for results in this direction. If we limit the number of moves instead of the number of pebbles, these games capture the expressive power of first-order extensions. In this case the correspondence to logic is the quantifier rank of formulas, as in the case of traditional Ehrenfeucht-Fraïssé games. In contrast to other model comparison games, these games are rather complex and only few results have been established so far [24]. To make progress towards settling this topic, we have to work out sufficient structural criteria which guarantee equal rank for two different matrices. This is a challenging task since we have to consider matrices defined over tuples of elements. Additionally, the rank may depend on the chosen dimension of the encoded matrix. In general, we lack natural examples showing how to take advantage of combining operators from linear algebra and fixed point recursion. This is also true for the nesting of operators.

Rank equality vs. rank terms The relationship between $\mathsf{FP}{+}\mathsf{eqv}$ and $\mathsf{FP}{+}\mathsf{rk}$ is of special interest. We know that matrix equivalence over fields is precisely the *Härtig rank quantifier*, i.e. the generalized quantifier which decides whether two matrices have the same rank. Otto [61] clarified the relation for the case of FP and its extension $\mathsf{FP}{+}\mathsf{C}$. He proved that extending FP by the Härtig and Rescher quantifier leads to a logic which is strictly less expressive than $\mathsf{FP}{+}\mathsf{C}$. His result even holds for the extension of FP by the set of all Lindström counting quantifiers. We guess that one can adapt his proof to the case of rank operators. The intrinsic difficulty lies in the following fact: the affected queries from linear algebra cannot be decided by knowledge about the membership of the parts with respect to an arbitrary decomposition. In order to illustrate this, assume that we decompose a matrix into k blocks, and assume that we have knowledge about the matrix rank for each of the single blocks. Then there is no way to conclude to the rank of the whole matrix. For the mechanism of ordinary counting the opposite is true. Removing the obstacles in this way means to extend our knowledge about the behavior of matrices which are defined by equality types. Matrices of this type were used to simulate modulo

counting by solve quantifiers. In fact, the linear algebraic properties of matrices defined by equality types are the inherent part of the expressive power of the studied extensions. They even can be defined in highly symmetric structures like e.g. complete graphs. In particular, it seems necessary to gain knowledge about the linear algebraic properties of matrices defined by combining different equality types. We derived some first results for matrices of dimension two but the general case remains unsolved. Furthermore, answering these questions will help to apply the presented pebble partition games.

Ordering k-types It is a significant result that for each fixed $k \in \omega$ a linear order on $\mathsf{L}^k_{\infty\omega}$ types can be defined in FP. Abiteboul and Vianu [2] used this ordering to show that $\mathsf{FP} = \mathsf{PFP}$ iff $\mathsf{PTIME} = \mathsf{PSPACE}$. One obtains a similar result for $\mathsf{C}^k_{\infty\omega}$ types and definability in $\mathsf{FP}{+}\mathsf{C}$, cf. [61]. Dawar et al. [26] studied the same problem for extensions of infinitary logic by generalized Lindström quantifiers. They proved that for any finite class $\mathcal{Q}$ of Lindström quantifiers an ordering of $\mathsf{L}^k_{\infty\omega}(\mathcal{Q})$ types can be defined in $\mathsf{PFP}(\mathcal{Q})$. The same question arises for the extension of fixed point logics by Lindström quantifiers from linear algebra. Can we define an ordering of $\mathsf{L}^k_{\infty\omega}(\mathit{slv})$ types in $\mathsf{FP}{+}\mathsf{slv}$? We worked on this issue, but encountered similar problems regarding the decompositions of matrices as described in the previous paragraph.

Positive results Dawar et al. proposed to explore more positive ways: Is it possible to define the isomorphism query on the class of bounded degree graphs in $\mathsf{FP}{+}\mathsf{rk}$? This query is known to be decidable in polynomial time [56]. Furthermore, the result of Blass et al. [12] shows that perfect matching on bipartite graphs is definable in $\mathsf{FP}{+}\mathsf{C}$. Perhaps perfect matching is definable in $\mathsf{FP}{+}\mathsf{rk}$, even for general graphs.

Altogether we have just begun to explore the exciting qualities of linear algebra in the light of its descriptive complexity. Unquestionably, if we want to make progress in settling the task of finding a logic for PTIME, the structural reasons for the indicated descriptive power of linear algebra have to be revealed.

Bibliography

[1] S. Abiteboul, M.Y. Vardi, and V. Vianu. Fixpoint logics, relational machines, and computational complexity. In *Structure in Complexity Theory Conference*, pages 156–168, 1992.

[2] Serge Abiteboul and Victor Vianu. Computing with first-order logic. *J. Comput. Syst. Sci.*, 50:309–335, April 1995.

[3] E. Allender, R. Beals, and M. Ogihara. The Complexity of Matrix Rank and Feasible Systems of Linear Equations. *Computational Complexity*, 8:99–126, 1999.

[4] Carme Àlvarez and Raymond Greenlaw. A Compendium of Problems Complete for Symmetric Logarithmic Space. *Computational Complexity*, 9(2):123–145, 2000.

[5] Vikraman Arvind and T.C. Vijayaraghavan. The Complexity of Solving Linear Equations over a Finite Ring. In *STACS 2005*, volume 3404 of *Lecture Notes in Computer Science*, pages 472–484. Springer, 2005.

[6] Vikraman Arvind and T.C. Vijayaraghavan. Classifying Problems on Linear Congruences and Abelian Permutation Groups Using Logspace Counting Classes. *Computational Complexity*, 19:57–98, 2010.

[7] Albert Atserias, Andrei A. Bulatov, and Anuj Dawar. Affine Systems of Equations and Counting Infinitary Logic. *Theoretical Computer Science*, 410(18):1666–1683, 2009.

[8] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18(3):147–150, 1984.

[9] Norman Biggs. *Algebraic Graph Theory*. Cambridge University Press, 1993.

[10] Gilberto Bini and Flaminio Flamini. *Finite Commutative Rings and Their Applications*. Kluwer Academic Publishers, Norwell, MA, USA, 2002.

[11] Andreas Blass and Yuri Gurevich. A Quick Update on the Open Problems in Blass-Gurevich-Shelah's Article On Polynomial Time Computation Over Unordered Structures, 2005.

[12] Andreas Blass, Yuri Gurevich, and Saharon Shelah. On Polynomial Time Computation over Unordered Structures. *Journal of Symbolic Logic*, 67(3):1093–1125, 2002.

[13] Hans Bodlaender. Treewidth: Algorithmic techniques and results. In *Mathematical Foundations of Computer Science 1997*, volume 1295 of *Lecture Notes in Computer Science*, pages 19–36. Springer, 1997.

[14] Chris Bourke, Raghunath Tewari, and N. V. Vinodchandran. Directed Planar Reachability Is in Unambiguous Log-Space. *ACM Transactions on Computation Theory*, 1(1):1–17, 2009.

[15] Gerhard Buntrock, Carsten Damm, Ulrich Hertrampf, and Christoph Meinel. Structure and Importance of Logspace-MOD Class. *Mathematical Systems Theory*, 25(3): 223–237, 1992.

[16] JinYi Cai, Martin Fürer, and Neil Immerman. An optimal lower bound on the number of variables for graph identifications. *Combinatorica*, 12(4):389–410, 1992.

[17] C.C. Chang and H.J. Keisler. *Model Theory*. North Holland, 1990.

[18] Arkadev Chattopadhyay, Navin Goyal, Pavel Pudlák, and Denis Thérien. Lower bounds for circuits with MODm gates. In *FOCS*, pages 709–718. IEEE Computer Society, 2006.

[19] Wai-Sin Ching. Linear equations over commutative rings. *Linear Algebra and its Applications*, 18(3):257 – 266, 1977.

[20] Stephen A. Cook. A taxonomy of problems with fast parallel algorithms. *Information and Control*, 64(1-3):2 – 22, 1985.

[21] L. Csanky. Fast Parallel Matrix Inversion Algorithms. *SIAM Journal on Computing*, 5(4):618–623, 1976.

[22] Anuj Dawar. Generalized Quantifiers and Logical Reducibilities. *Journal of Logic and Computation*, 5(2):213–226, 1995.

[23] Anuj Dawar. A Restricted Second Order Logic for Finite Structures. *Information and Computation*, 143(2):154–174, 1998.

[24] Anuj Dawar and Bjarki Holm. Pebble Games for Rank Logics. In *Logical Approaches to Barriers in Computing and Complexity*, Greifswald, Germany, 2010.

[25] Anuj Dawar and David Richerby. The Power of Counting Logics on Restricted Classes of Finite Structures. In *CSL*, pages 84–98, 2007.

[26] Anuj Dawar, Lauri Hella, and A. Seth. Ordering finite variable types with generalized quantifiers. In *Logic in Computer Science, 1998. Proceedings. Thirteenth Annual IEEE Symposium on*, pages 28 –43, 1998.

[27] Anuj Dawar, Martin Grohe, Bjarki Holm, and Bastian Laubner. Logics with Rank Operators. In *LICS '09: Proceedings of the 2009 24th Annual IEEE Symposium on Logic In Computer Science*, pages 113–122, 2009.

[28] Reinhard Diestel. *Graph Theory*. Springer, 2005.

[29] John D. Dixon. An isomorphism criterion for modules over a principal ideal domain. *Linear and Multilinear Algebra*, 8:69–72, 1979.

[30] H.D. Ebbinghaus and J. Flum. *Finite Model Theory*. Springer Verlag, 2005.

[31] V. P. Elizarov. Necessary conditions for solvability of a system of linear equations over a ring. *Discrete Mathematics and Applications*, 14(2):153–162, 2004.

[32] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. *American Mathematical Society*, pages 43–74, 1974.

[33] G. Ganske and B.R. McDonald. Finite local rings. *Rocky Mountain Journal of Mathematic*, 3:521–540, 1973.

[34] Chirs Godsil and Gordon Royle. *Algebraic Graph Theory*. Springer, 2001.

[35] Mikael Goldmann and Alexander Russell. The Complexity of Solving Equations over Finite Groups. *Information and Computation*, 178(1):253–262, 2002.

[36] Erich Grädel and Gregory L. McColm. Deterministic vs. Nondeterministic Transitive Closure Logic. In *LICS*, pages 58–63, 1992.

[37] Erich Grädel, P. G. Kolaitis, L. Libkin, M. Marx, J. Spencer, Moshe Y. Vardi, Y. Venema, and Scott Weinstein. *Finite Model Theory and Its Applications*. Springer, 2005.

[38] Martin Grohe. Fixed-Point Definability and Polynomial Time on Chordal Graphs and Line Graphs. In *Fields of Logic and Computation*, pages 328–353, 2010.

[39] Erich Grädel and Martin Otto. Inductive Definability with Counting on Finite Structures. In *In Proceedings of Computer Science Logic 92*, pages 231–247. Springer, 1993.

[40] Yuri Gurevich. Logic and the Challenge of Computer Science. *Trends in Theoretical Computer Science*, 1001:1–57, 1988.

[41] Yuri Gurevich and Saharon Shelah. On Finite Rigid Structures. *Journal of Symbolic Logic*, 61(2):549–562, 1996.

[42] Magnús Halldórsson, Jan Kratochvíl, and Jan Telle. Mod-2 Independence and Domination in Graphs. In *Graph-Theoretic Concepts in Computer Science*, volume 1665 of *Lecture Notes in Computer Science*, pages 101–109. Springer, 1999.

[43] Magnús M. Halldórsson, Jan Kratochvíl, and Jan Arne Telle. Independent sets with domination constraints. *Discrete Applied Mathematics*, 99(1-3):39 – 54, 2000.

[44] Lauri Hella. Logical Hierarchies in PTIME . *Information and Computation*, 129(1): 1–19, 1996.

[45] Ulrich Hertrampf, Steffen Reith, and Heribert Vollmer. A Note on Closure Properties of Logspace-MOD Classes. *Information Processing Letters*, 75(3):91–93, 2000.

[46] Thanh Minh Hoang and Thomas Thierauf. The Complexity of the Characteristic and the Minimal Polynomial. *Theoretical Computer Science*, 295(1-3):205–222, 2003.

[47] Thanh Minh Hoang and Thomas Thierauf. On the Minimal Polynomial of a Matrix. *International Journal of Foundations of Computer Science*, 15(1):89–105, 2004.

[48] Henrik Imhof. Fixed-Point Logics, Generalized Quantifiers, and Oracles. *Journal of Logic and Computation*, 7(3):405–425, 1997.

[49] Neil Immerman. Relational Queries Computable in Polynomial Time. *Information and Control*, 68(1-3):86–104, 1986.

[50] Neil Immerman. Languages that Capture Complexity Classes. *SIAM J. Comput.*, 16(4):760–778, 1987.

[51] Erich Kaltofen and Gilles Villard. On the Complexity of Computing Determinants. *Comput. Complex.*, 13:91–130, February 2005.

[52] Anthony W. Knapp. *Basic Algebra*. Birkhäuser Boston, 2006.

[53] Stephan Kreutzer. Expressive Equivalence of Least and Inflationary Fixed-Point Logic. In *LICS*, 2002.

[54] Felix Lazebnik. On Systems of Linear Diophantine Equations. *Mathematics Magazine*, 69(4):261–266, 1996.

[55] Leonid Libkin. *Elements Of Finite Model Theory*. Springer Verlag, 2004.

[56] Eugene M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. In *Proceedings of the 21st Annual Symposium on Foundations of Computer Science*, pages 42–49, Washington, DC, USA, 1980. IEEE Computer Society.

[57] M. Mahajan and V. Vinay. Determinant: Combinatorics, algorithms, and complexity. *Chicago Journal of Theoretical Computer Science*, 5(1997):730–738, 1997.

[58] Meena Mahajan and V. Vinay. Determinant: Old Algorithms, New Insights. In *Algorithm Theory — SWAT'98*, volume 1432 of *Lecture Notes in Computer Science*. Springer, 1998.

[59] Bernard R. McDonald. *Linear Algebra over Commutative Rings*. Dekker, 1984.

[60] Ketan Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. *Combinatorica*, 7:101–104, 1987.

[61] Martin Otto. The Expressive Power of Fixed-Point Logic with Counting. *The Journal of Symbolic Logic*, 61(1):pp. 147–176, 1996.

[62] Martin Otto. *Bounded variable logics and counting - A study in finite models*, volume 9. Springer, 1997.

[63] Günter Rote. Division-Free Algorithms for the Determinant and the Pfaffian: Algebraic and Combinatorial Approaches. In *Computational Discrete Mathematics*, volume 2122 of *Lecture Notes in Computer Science*, pages 119–135. Springer, 2001.

[64] Paul D. Seymour and Robin Thomas. Graph Searching and a Min-Max Theorem for Tree-Width. *Journal of Combinatorial Theory*, 58(1):22–33, May 1993.

[65] Kenjiro Shoda. Über die Automorphismen einer endlichen Abelschen Gruppe. *Mathematische Annalen*, 100:674–686, 1928.

[66] Arne Storjohann. An O(n3) algorithm for the Frobenius normal form. In *ISSAC '98: Proceedings of the 1998 international symposium on Symbolic and algebraic computation*, pages 101–105. ACM, 1998.

[67] Arne Storjohann. *Algorithms for matrix canonical forms*. Dissertation, Technische Wissenschaften ETH Zürich, Zürich, 2000.

[68] Moshe Y. Vardi. The Complexity of Relational Query Languages. In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, STOC '82, pages 137–146, New York, NY, USA, 1982.

[69] Joachim von zur Gathen. Parallel linear algebra. In J. Reif, editor, *Synthesis of parallel algorithms*, pages 573–617. MKP, 1993.

Appendices

Appendix A.

Overview: Considered Problems

Problem / Query	Algorithmic Complexity	Descriptive Complexity
Undirected Reachability (REACH)	complete for SLOGSPACE	FO+STC $\leq$ FO+slv$_{\mathcal{R}}$ ([27], Sec. 3.1)
Reachability modulo $n \in \omega$ (REACH$_n$)	complete for MOD$_n$L ([15])	FO+slv$_{\mathbb{Z}_n}$, and for primes n on ordered structures FO+slv$_{\mathbb{Z}_n}$ $\equiv$ MOD$_n$L ([27], Sec. 4.2)
Circuit value problem over modulo gates ($CVP(\mathbb{Z}_n)$)	corresponds to complexity class CC[n] ([18])	FO+slv$_{\mathbb{Z}_n}$ (Sec. 3.1)
(σ,ρ)-subset problem ((σ,ρ)-SUBSET($\mathcal{G}$))	depends on ρ,$\sigma \subseteq \omega$ ([42, 43])	depends on ρ,$\sigma \subseteq \omega$, (Sec. 3.3), e.g. (even,even)-SUBSET($\mathcal{G}$) $\in$ FO+slv$_{\mathbb{F}_2}$

Table A.1.: Structural queries from graph theory

Problem / Query	Domain	Descriptive Complexity
matrix addition	finite field	FO ([12], Sec. 2.2)
	finite ring	FO (Sec. 2.2)
	$\mathbb{Z}$	FP$^+$ ([12], Sec. 2.2)
	$\mathbb{Q}$	FP$^+$ ([27], Sec. 2.2)
matrix multiplication	finite field	FO+C ([12], Sec. 2.2)
	finite ring	FO+C (Sec. 2.2)
	$\mathbb{Z}$	FP+C ([12], Sec. 2.2)
	$\mathbb{Q}$	FP+C ([27], Sec. 2.2)
iterated, matrix multiplication	finite field	FP+C ([12], Sec. 2.2)
	finite ring	FP+C (Sec. 2.2)
	$\mathbb{Z}$	FP+C ([12], Sec. 2.2)
	$\mathbb{Q}$	FP+C ([27], Sec. 2.2)
matrix singularity	finite field	FO+slv, FP+C ([12], Sec. 2.2)
	finite ring	FO+slv, FO+rk, FP+C (Sec. 2.2)
	$\mathbb{Z}$	FP+C ([12], Sec. 2.2)
	$\mathbb{Q}$	FP$^+$ ([27], Sec. 2.2)

...

matrix determinant	finite field	FP+C ([11], Sec. 2.3)
	finite ring	open, (partial results in Sec. 2.3)
	$\mathbb{Z}$	FP+C ([27], Sec. 2.3)
	$\mathbb{Q}$	FP+C ([27], Sec. 2.3)
characteristic polynomial (+ determinant, inverse)	finite field	FP+C (Sec. 2.3)
	finite ring	open, (partial results in Sec. 2.3)
	$\mathbb{Z}$	FP+C (Sec. 2.3)
	$\mathbb{Q}$	FP+C (Sec. 2.3)
minimal polynomial (+ diagonalizable)	finite field	FP+C (Sec. 2.4)
	finite ring	-
	$\mathbb{Z}$	-
	$\mathbb{Q}$	FP+C (Sec. 2.4)
linear equation systems	finite field	$\mathsf{FO{+}slv}^{\mathcal{F}\star} \setminus \mathsf{C}^{\omega}_{\infty\omega}$ ([7, 27], Sec. 2.5, 3.1)
	finite ring	$\mathsf{FO{+}slv} \setminus \mathsf{C}^{\omega}_{\infty\omega}$ ([7, 27], Sec. 2.5, 3.1)
	$\mathbb{Z}$	open, $\notin \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6)
	$\mathbb{Q}$	FP+C ([27], Sec. 2.5)
matrix similarity	finite field	$\mathsf{FO{+}sim}^{\mathcal{F}\star} \setminus \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6, 3.2)
	finite ring	$\mathsf{FO{+}sim} \setminus \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6, 3.2)
	$\mathbb{Z}$	open, $\notin \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6)
	$\mathbb{Q}$	FP+C (Lemma 2.5.7 + Thm. 2.3.3, 3.3.3)
matrix equivalence	finite field	$\mathsf{FO{+}eqv}^{\mathcal{F}\star} \setminus \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6, 3.2)
	finite ring	$\mathsf{FO{+}eqv} \setminus \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6, 3.2)
	$\mathbb{Z}$	open, $\notin \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6)
	$\mathbb{Q}$	FP+C (Lemma 2.5.7 + Thm. 2.3.3, 3.3.3)
matrix rank	finite field	$\mathsf{FO{+}rk}^{\mathcal{F}\star} \setminus \mathsf{C}^{\omega}_{\infty\omega}$ ([7, 27], Sec. 2.6, 3.3)
	finite ring	$\mathsf{FO{+}rk} \setminus \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6, 3.3)
	$\mathbb{Z}$	open, $\notin \mathsf{C}^{\omega}_{\infty\omega}$ (Sec. 2.6)
	$\mathbb{Q}$	FP+C ([27], Sec. 2.5)

Table A.2.: Problems from the field of linear algebra