Logical and algorithmical aspects of rank notions over rings

Nikolas P. Breuckmann - December 3, 2013

Bachelor thesis under supervision of
Prof. Dr. E. Grädel

Fakultät für Mathematik, Informatik und Naturwissenschaften - Fakultät 1
Mathematische Grundlagen der Informatik

RWTH AACHEN UNIVERSITY

Acknowledgments

This thesis would not have been possible without the guidance and encouragement of my supervisor Wied Pakusa. I would also like to thank Prof. Erich Grädel for assigning me this interesting topic.

Contents

Notations

$\mathrm{Fin}(\tau)$	class of all finite structures with signature τ
$\mathrm{Ord}(\tau)$	class of all ordered finite structures with signature τ
Σ^*	set of all finite words over the alphabet Σ
FO	first-order logic
$\exists$SO	existential fragment of second-order logic
$\mathrm{code}(\mathfrak{A})$, $\mathrm{code}(\mathcal{C})$	encoding of the structure $\mathfrak{A}$, respectively the class of structures $\mathcal{C}$
$\mathcal{P}(S)$	power set of S
F_ψ	operator induced by the formula ψ
$R^\times$	set of units of the ring R
$M^{\oplus k}$	direct sum of k copies of the module M
$I_t(A)$	ideal generated by the determinants of all $t \times t$-submatrices of A
$\underline{n}$	set of natural numbers $\{1, \ldots, n\}$
$A_{i,*}$	i-th row of the matrix A
$A_{*,j}$	j-th column of the matrix A
E_n	$n \times n$ identity matrix
$GL(n, R)$	set of invertible $n \times n$-matrices over R
$(a_1, \ldots, a_n)$	ideal generated by $a_1, \ldots, a_n$

1 Introduction

Model theory is a branch of mathematical logic which studies the relation between the the syntax of a logic and interpretations which are given by classes of mathematical structures (such as graphs, groups or fields) called models. Classical results in the area of model theory are the compactness theorem for first-order logic (FO) which states that a set of first-order sentences has a model if and only if all finite subsets have a model or the Löwenheim–Skolem theorem which roughly states that first-order logic is incapable of controlling infinite cardinalities of structures.

Since problems in computer science can be formulated by means of finite structures *finite model theory* became a successful framework to investigate in computational complexity. However, many tools such as the compactness theorem do not hold when only finite structures are considered. Therefore new techniques had to be developed for finite model theory.

Most important for our investigations is that finite model theory makes it possible to link logics to complexity classes. This is done in the following way: A logic L corresponds to a complexity class $Comp$ if each class of finite structures which is definable in L is decidable in $Comp$ and each class of finite structures decidable in $Comp$ is a model class of some sentence in L. We will often say that L *captures* $Comp$.

The branch of finite model theory which deals with finding such capturing results is called *descriptive complexity*. It allows us to analyze the the difficulty of solving computational problems by means of finite model theory and mathematical logic. The study of descriptive complexity was initiated by Fagin who showed that the complexity class NP can be captured by the existential fragment of second-order logic ($\exists$SO) [9].

The main open question in descriptive complexity is whether there is a logic which corresponds to the complexity class PTIME. A promising strategy to construct a suitable logic is extending first-order logic because it can only define properties which are decidable in polynomial time. A shortcoming of first-order logic is that it is not capable of defining properties which depend on recursion such as the transitive closure of a graph. One extension of first order logic which introduces recursion is called *inductive fixed-point logic* (IFP). Immerman [15] and Vardi [22] could show that this logic can capture PTIME if we only consider structures which include a total linear order. If there is no order given then some quite elementary propteries such as the property of a structure to contain an even number of elements can not be defined in IFP. But obviously this property can be easily checked in polynomial time by simple counting.

Therefore Immerman suggested to introduce a counting mechanism into IFP [16]. This lead to the so called *inductive fixed-point logic with counting* (IFP+C). But despite many promising results, such as IFP+C capturing PTIME on *almost all* structures proven by Hella, Kolaitis and Luosto [12], a construction by Cai, Fürer and Immerman showed that there were still properties decidable in polynomial time which IFP+C could not express [2]. However their construction involving graphs was considered artificial and it was hoped that IFP+C could at least define all *natural* PTIME-properties.

This was refuted in 2009 by Atserias, Bulatov and Dawar who showed that the solvability of systems of linear equations over a fixed finite abelian group could not be expressed by any sentence of IFP+C [1]. Therefore the solvability of systems of linear equations over finite fields is not definable in IFP+C although it is decidable in polynomial time by Gaussian elimination. Since a linear equation system $(A \mid b)$ over a field is solvable if and only if $rk(A \mid b) = rk(A)$ we can see that IFP+C is also incapable of expressing the rank of a matrix over arbitrary fields.[1]

Similarly to the case before were counting was introduced into IFP it is hoped that by extending IFP with the ability to express the rank of a matrix the resulting logic will be able to capture polynomial time on a broader class of structures. What makes this second expansion more difficult is that there are several ways of defining the rank of a matrix. These definitions coincide on matrices over fields, but they fall apart when we consider matrices over rings.

[1] However it was shown by Blass et. al that the class of square singular matrices as well the characteristic polynomial and therefore the determinant of any matrix defined over finite fields, the field of rationals $\mathbb{Q}$ or the ring of integers $\mathbb{Z}$. Furthermore IFP+C can define the rank of matrices over $\mathbb{Q}$ (see [13]).

Outline

In Section 2 we give some basic definitions of complexity theory and descriptive complexity. We explain how mathematical structures are encoded into strings over a finite alphabet to make them accessible to Turing machines and give the precise definition of what it means when we say that a logic captures a complexity class. Afterwards we discuss some notions from ring and module theory.

In Section 3 we introduce inductive fixed-point logic and how it is extended by counting. We discuss how matrices are encoded into (unordered) finite structures and how the notion of a matrix rank is incorporated into the logical framework which leads to the definition of the inductive fixed-point logic with rank.

In Section 4 we introduce five different notions of matrix rank. We also analyze on which classes of rings these rank notions are well-defined.

In Section 5 we explore some of the properties of the rank notions. First we check whether they are invariant under transposition. For those rank notions which are defined via columns and rows of a matrix this shows if column rank equals row rank. Since we consider unordered matrices we have to make sure that the ranks notions are invariant under permutation of columns and rows. We also check the more restrictive condition of being invariant under equivalence. Finally we study the relationship between the ranks. We define classes of rings where two rank notions are equal and examine if there are any other relations between two rank notions such as one being an upper bound of the other.

In Section 6 we analyze if the rank can be used to as a criterion for the solvability of linear equation systems over rings. This is done by applying the Kronecker-Capelli Theorem which states that a system of linear equations $Ax = b$ is solvable if and only if $rk(A \mid b) = rk(A)$.

In Section 7 we analyze the computational complexity of the rank notions.

2 Preliminaries

This section is meant as a summary providing the necessary background for this thesis. We give the precise definitions of notions introduced in Section 1 and we define some basic concepts of algorithmic complexity theory as well as linear algebra. We also show how both are incorporated into a logical formalism.

2.1 Descriptive complexity

The aim of computational complexity theory is to classify computational problems based on how difficult they are to solve. A problem is regarded as difficult if its solution requires a significant amount of resources regardless of the algorithm which is used. Those resources are running time, memory (space) and other measurable quantities which can be formalized in a mathematical model of computation. The exact amount of resources depends on the model of computation but we can define classes of problems which are robust in this respect. The classes which appear in this thesis are given in the following definition.

Definition 2.1. Let $\mathrm{TIME}(f(n))$ be the class of problems which can be solved by a Turing machine in at most $\mathcal{O}(f(n))$ steps where n quantifies the size of the input. We define the class of problems PTIME[2] as

$$\mathrm{PTIME} \coloneqq \bigcup_{k\in\mathbb{N}} \mathrm{TIME}\left(n^k\right) \tag{2.1}$$

and the class of problems EXPTIME as

$$\mathrm{EXPTIME} \coloneqq \bigcup_{k\in\mathbb{N}} \mathrm{TIME}\left(2^{n^k}\right). \tag{2.2}$$

Similarly let $\mathrm{NTIME}(f(n))$ be the class of problems which can be solved by a non-deterministic Turing machine in at most $\mathcal{O}(f(n))$ steps. Then we obtain the class

$$\mathrm{NP} \coloneqq \bigcup_{k\in\mathbb{N}} \mathrm{NTIME}\left(n^k\right). \tag{2.3}$$

In order to formalize the notion of a logic that captures a complexity class we need to introduce an encoding of finite relational structures.

Definition 2.2. Let τ be a signature, $\tau_<$ its extension by a binary relation symbol $<\notin \tau$ and $\mathrm{Fin}(\tau_<)$ the class of finite $\tau_<$-structures. Then the *class of ordered finite τ-structures* $\mathrm{Ord}(\tau)$ is defined as

$$\mathrm{Ord}(\tau) \coloneqq \{(\mathfrak{A},<) \in \mathrm{Fin}(\tau_<) \mid \mathfrak{A} \in \mathrm{Fin}(\tau), < \text{ is a linear order on } A\}. \tag{2.4}$$

Ordered finite structures $(\mathfrak{A},<) \in \mathit{Ord}(\tau)$ can be encoded into a finite word over a finite alphabet Σ, i.e. $\mathrm{code}(\mathfrak{A},<) \in \Sigma^*$. Note that we need an encoding which identifies isomorphic structures, is polynomially bounded, first-order definable and allows the computation of atomic statements in polynomial time. A more formal description of these conditions as well as an example for such an encoding scheme can be found in [10].
By fixing a finite alphabet Σ and an encoding scheme we can associate finite structures with finite words and therefore classes of finite structures with subsets of Σ^*

Definition 2.3. A *machine representation* of a class of finite structures $\mathcal{C} \subseteq \mathrm{Fin}(\tau)$ with $<\notin \tau$ is given by

$$\mathrm{code}(\mathcal{C}) \coloneqq \{\mathrm{code}(\mathfrak{A},<) \mid \mathfrak{A} \in \mathcal{C} \text{ and } < \text{ is a linear order on } A\} \subseteq \Sigma^* \tag{2.5}$$

[2]We say that problems are *efficiently computable* when they are in PTIME.

By considering the machine representation of a class of finite structures it makes sense to ask if it is contained in a certain complexity class: When we say that an algorithm decides a class of finite τ-structures $\mathcal{C}$ then we actually mean that it decides code($\mathcal{C}$).

Definition 2.4. Let τ be a signature then a *model class* $\mathcal{C}$ is a class of τ-structures that is closed under isomorphism, i.e. if $\mathfrak{A} \in \mathcal{C}$ and $\mathfrak{A} \cong \mathfrak{B}$, then $\mathfrak{B} \in \mathcal{C}$.
A *domain* is a subclass $\mathcal{D} \subseteq \bigcup_\tau \mathrm{Fin}(\tau)$ such that $\mathcal{D}(\tau) := \mathcal{D} \cap \mathrm{Fin}(\tau)$ is a model class for all τ.

Definition 2.5. Let L be a logic, *Comp* a complexity class and $\mathcal{D}$ a domain of finite structures. Then *Comp* is captured by L on $\mathcal{D}$ if

1. For every signature τ and every sentence $\psi \in L(\tau)$, the model checking problem for ψ on $\mathcal{D}(\tau)$ is in *Comp*, i.e. there exists an algorithm which decides for any $\mathfrak{A} \in \mathcal{D}(\tau)$ if $\mathfrak{A} \models \psi$ in *Comp*.
2. Let $\mathcal{C} \subseteq \mathcal{D}(\tau)$ be a model class whose membership problem is in *Comp*, i.e. there is an algorithm which decides in *Comp* if some $\mathfrak{A} \in \mathcal{D}(\tau)$ is in $\mathcal{C}$. Then there exists a $\psi \in L(\tau)$ such that $\mathcal{C} = \{\mathfrak{A} \in \mathcal{D}(\tau) \mid \mathfrak{A} \models \psi\}$.

In case that either 1. or 2. hold we write $L \leq_\mathcal{D} Comp$ respectively $Comp \leq_\mathcal{D} L$ and $L =_\mathcal{D} Comp$ if both statements are true. If $\mathcal{D} = \mathrm{Fin}(\tau)$ we omit the subscript.

As already mentioned in the Introduction the following results regarding the complexity classes PTIME and NP are known:

Theorem 2.6 (Fagins Theorem)**.** *The complexity class NP is captured by the existential fragment of first order logic ∃SO on the domain of all finite structures.*[3]

Theorem 2.7 (Immerman-Vardi Theorem)**.** *Inductive fixed-point logic IFP captures PTIME on the class of all ordered structures.*

Note that the domain in the above theorems is different. In fact capturing results on the class of finite structures are known for all complexity classes in the polynomial hierarchy above NP but none for classes below NP (see [13]). Especially the question whether there is a logic capturing PTIME on all finite structures is very important: If there is such a logic it reduces the problem of separating the complexity classes P and NP to separating the logics which capture them. Some people such as Gurevich [11] believe that there is no logic which captures PTIME. This would solve the P vs. NP problem directly because it is known that a logic for NP exists.

2.2 Rings and modules

Definition 2.8. A *ring* is a nonempty set R with two binary operations $+$ and $\cdot$ such that

1. $(R, +)$ is an abelian group;
2. $(R, \cdot)$ is a semigroup;
3. for all $a, b, c \in R$ we have

$$(a + b) \cdot c = a \cdot c + b \cdot c \tag{2.6}$$

and

$$a \cdot (b + c) = a \cdot b + a \cdot c \tag{2.7}$$

(left and right distributive laws).

We often omit the $\cdot$ and simply write ab instead of $a \cdot b$.
If the multiplication is commutative then R is called a *commutative ring*.

[3]The existential fragment of second-order logic ∃SO consists of all formulae of the form $\exists R_1 \ldots \exists R_n \phi$ where $R_1, \ldots, R_n$ are relation symbols and $\phi \in FO$.

If not otherwise mentioned we assume that a ring R has a multiplicative identity element 1_R and that $1_R \neq 0_R$ holds in R where 0_R is the neutral element of the addition. An element $a \in R$ which has an inverse in R, i.e. there exists $b \in R$ such that $ab = ba = 1_R$, is called a *unit* of R. The set of all units of R is denoted by $R^\times$. A nonzero element in a ring R is said to be a *left* (resp. right) *zero divisor* if there exists a nonzero $b \in R$ such that $ab = 0_R$ (resp. $ba = 0_R$). A *zero divisor* is an element which is both a left and right zero divisor. If an element is not a left or right zero divisor we call it *regular*.

Definition 2.9. If R is a ring without left and right zero divisors then R is called a *domain*. If R is also commutative it is called an *integral domain*.

Definition 2.10. Let R be a ring. A subset $I \subseteq R$ is called a *left* (resp. right) *ideal* if $(I, +)$ is a subgroup of $(R, +)$ and $RI \subseteq I$ (resp. $IR \subseteq I$), i.e. for all $a \in I$ and $r \in R$ we have $ra \in I$ (resp. $ar \in I$).

Definition 2.11. Let R be a ring, $X \subseteq R$ a subset and $\mathcal{F} = \{I \subseteq R \mid I \text{ is an ideal of } R \text{ and } X \subseteq I\}$. Then the *ideal generated by* X is defined as

$$(X) \coloneqq \bigcap_{I \in \mathcal{F}} I. \tag{2.8}$$

If $X = \{x_1, \ldots, x_k\}$ for some $k \in \mathbb{N}$ then we call the ideal $(x_1, \ldots, x_k)$ finitely generated and we have

$$(x_1, \ldots, x_k) = \{r_1 x_1 s_1 + \cdots + r_k x_k s_k \mid r_i, s_i \in R\}. \tag{2.9}$$

If all ideals of R are finitely generated we call R a *Noetherian ring*.

An ideal $I \neq R$ is called *maximal left* (resp. right) *ideal* if for all left (resp. right) ideals J with $I \subseteq J$ follows that either $I = J$ or $J = R$. A *maximal ideal* is an ideal thats both a left and right maximal ideal. If R is commutative and from $ab \in I$ follows that either $a \in I$ or $b \in I$ then I is called a *prime ideal*. Note that every maximal ideal is a prime ideal.[4]

We can define a class of rings by demanding that the ideals of the rings must have certain properties (We have seen this already for Noetherian rings). The classes of rings which will be important in this thesis are the following.

Definition 2.12. A ring R is called

- *local* if it has a unique maximal ideal,
- *(left) principal ideal ring* (PIR) if every (left) ideal is of the form Ra for some $a \in R$,
- *principal ideal domain* (PID) if it is a PIR and an integral domain,
- *chain ring* if it is a PIR and local,
- *Galois–Eisenstein ring* (GE-ring) if it is a finite commutative chain ring,
- *Bézout domain* if it is a domain and the sum of two principal ideals is again a principal ideal.

In this thesis we will make use of the following two ideals.

Definition 2.13. If R is a commutative ring then the *nilradical* $\mathcal{N}(R)$ is the ideal consisting of all nilpotent elements of the ring, i.e.

$$\mathcal{N}(R) = \{r \in R \mid r^k = 0 \text{ for some } k \in \mathbb{N}\}. \tag{2.10}$$

The *nilpotency index* of an element $r \in \mathcal{N}(R)$ is the smallest $k \in \mathbb{N}$ such that $r^k = 0$.

Definition 2.14. Let R be a ring and I an ideal in R then the *(left) annihilator* of I is defined as

$$\operatorname{ann}_R(I) = \{r \in R \mid ra = 0 \text{ for all } a \in I\} \tag{2.11}$$

[4]This is not necessarily true for rings without a unit.

The rank of a matrix over a field can be defined as the dimension of the column (resp. row) space of the matrix. In Section 4 this notion will be generalized to matrices over rings. To do this we have to define the concept of a module which is a generalization of the notion of vector space.

Definition 2.15. Let R be a ring. A *left R-module* is an abelian group $(M,+)$ with a scalar product $\cdot : R \times M \to M$ such that

$$\begin{aligned} r \cdot (x+y) &= r \cdot x + r \cdot y \\ (r+s) \cdot x &= r \cdot x + r \cdot y \\ (rs) \cdot x &= r \cdot (s \cdot x) \\ 1_R \cdot x &= x \end{aligned} \tag{2.12}$$

for all $r, s \in R$ and $x, y \in M$. Similarly we can define *right R-modules*.

Let M and N be modules and $N \subseteq M$ then we call N a *submodule* of M and write $N \leq M$. If a module M has no submodules except for $\{0\}$ and M then M is called *simple*.

Definition 2.16. Let R be a ring, M a left R-module and $X = \{x_1, \ldots, x_k\}$ a subset of M. X is called *(left) linearly independent* if from

$$r_1 x_1 + \cdots + r_k x_k = 0 \tag{2.13}$$

with $r_1, \ldots r_k \in R$ follows that $r_1 = \ldots = r_k = 0$.
X is called a *generating set* if for each $m \in M$ there exist $r_1, \ldots, r_k \in R$ such that

$$m = r_1 x_1 + \cdots + r_k x_k. \tag{2.14}$$

X is called a *basis* if it is linearly independent and a generating set.[5]

The notion of the dimension of a vector space as the cardinality of one of its bases is well-defined since every vector space has a basis and if X and X' are bases of the same vector space then $|X| = |X'|$. Both of these conditions are not fulfilled by all modules. Those modules which have a nonempty basis are called *free modules*. If the number of basis elements of a R-module does not vary we say that R has the *invariant basis number property* (IBN). For example do all commutative rings have IBN. More information can be found in [21]. Now we can define the dimension of a module which, for historical reasons, is called the rank of a module.

Definition 2.17. Let R have the IBN property and let M be a free R-module with basis X. Then the *rank* of M is defined as

$$\operatorname{rank}(M) = |X|. \tag{2.15}$$

Additionally we have to make sure that submodules of free modules are again free modules themselves. the rings for which this is the case are given in the following definition.

Definition 2.18. A *free ideal ring* (FIR) is a ring in which all right ideals are free modules with unique rank.
A ring such that all right ideals with at most n generators are free and have unique rank is called *n-FIR*.

Note that the class of commutative free ideal rings is precisely the class of principal ideal domains (see [5]).

[5]The empty set $\emptyset$ is by definition the basis of the zero module $\{0\}$.

3 Rank logics

In this section we will give the definitions of the logics IFP and IFP+C which extend FO by inductive fixed-points respectively fixed-points and counting operators. Furthermore we show how matrices can be encoded into a logical formalism and how IFP can be extended by rank operators.

3.1 Inflationary fixed-point logic

A limitation of first-order logic is the lacking of a recursion mechanism. This limitation can be overcome by introducing relations which are defined by inductive fixed points. We first observe that if we fix a τ-structure $\mathfrak{A}$ and a formula $\psi(R, \overline{x}) \in \mathrm{FO}(\tau \cup \{R\})$, with k being the arity of $\overline{x}$ and R, we can define the operator $F_\psi : \mathcal{P}(A) \to \mathcal{P}(A)$ by setting $F_\psi(R) \coloneqq \{\overline{a} \in A^k \mid \mathfrak{A} \models \psi(R, \overline{a})\}$. By putting restrictions on the formulas we obtain operators with certain properties. The property which is important to us is given in the following definition.

Definition 3.1. An operator $F : \mathcal{P}(S) \to \mathcal{P}(S)$ is called *inflationary* if it holds that $X \subseteq G(X)$ for all $X \subseteq S$.

One can associate with any operator $G : \mathcal{P}(S) \to \mathcal{P}(S)$ an inflationary operator F by setting $F(X) \coloneqq G(X) \cup X$ for all $X \subseteq S$.

Via these operators we can associate with any formula $\psi(R, \overline{x})$ a relation which is given by the fixed point of the induced operator.

Definition 3.2. The *inflationary fixed point* of any $F : \mathcal{P}(S) \to \mathcal{P}(S)$ is defined as the limit of the increasing sequence of sets which is defined as $R^0 \coloneqq \emptyset$, $R^{\alpha+1} \coloneqq F(R^\alpha) \cup R^\alpha$ and $R^\lambda \coloneqq \bigcup_{\alpha<\lambda} R^\alpha$ for limit ordinals λ.

Definition 3.3. The logic IFP is the extension of first-order logic FO by the following rules. Let τ be a signature then $\mathrm{FO}(\tau) \subseteq \mathrm{IFP}(\tau)$. Furthermore, if $\psi(R, \overline{x}) \in \mathrm{IFP}(\tau)$ and $\overline{t}$ is a tuple such that the arity of $\overline{x}$ and $\overline{t}$ match the arity of R then $[\mathrm{ifp}\ R\overline{x}.\psi](\overline{t}) \in \mathrm{IFP}(\tau)$.

For a given structure $\mathfrak{A}$ we have $\mathfrak{A} \models [\mathrm{ifp}\ R\overline{x}.\psi](\overline{t})$ if $\overline{t}^{\mathfrak{A}}$ is contained in the inflationary fixed-point of F_ψ.

Example 1. We mentioned in the introduction that IFP allows us to define transitive closures which is not possible for FO. Let $\phi(x, y) \coloneqq Exy \vee \exists z(Exz \wedge Rzy)$ where E is the edge relation and R a free relation symbol. Then

$$TC(x, y) \coloneqq [\mathrm{ifp}\ Rxy.\phi](u, v) \tag{3.1}$$

holds in a graph $G = (V, E)$ if and only if there exists a path between u and v.

We define the extension IFP+C by introducing *two-sorted structures* first.

Definition 3.4. Suppose $\mathfrak{A} \in \mathrm{Fin}(\tau)$. We define $\mathfrak{A}^+$ as the disjoint union of $\mathfrak{A}$ with the standard arithmetic:

$$\mathfrak{A}^+ \coloneqq \mathfrak{A} \uplus \{\mathbb{N}_0, +, \cdot, \leq, 0, 1\} \tag{3.2}$$

Let L be either FO or IFP. Then L^+ is the associated logic evaluated in the two-sorted structures $\mathfrak{A}^+$ where each occurrence of a numeric variable in formulas is bounded by a numeric term.

Definition 3.5. The *inflationary fixed-point logic with counting* is the extension IFP^+ under counting terms. The counting terms are defined as follows: for each $\phi(x) \in$ IFP+C where x is a free variable of the first sort we can define a counting term $\#x\phi(x)$. The set of free variables of the term is given by $\mathrm{free}(\phi) \setminus \{x\}$. For a model $\mathfrak{A}$ the value is interpreted as the number of different $a \in A$ such that $\mathfrak{A} \models \phi(a)$.

For more information on many-sorted structures and the syntax and semantic of IFP+C see [10].

3.2 Rank operators

Since capturing results on ordered structures are already known (see Theorem 2.7) we would like to encode matrices into arbitrary unordered structures. This means in particular that we can not demand the existence of an order on the index sets of matrices. However, many properties of matrices do not depend on the order of rows and columns. As we see in Section 5 almost all of the defined ranks are invariant under permutation of rows and columns.

Definition 3.6. Let I and J be two arbitrary sets (not necessarily ordered) then a $I \times J$*-matrix* A over a ring R is a mapping from the cartesian product $I \times J$ into R, i.e. $A : I \times J \to R$.

We interpret this as rows and columns which are indexed by elements of the sets I and J. Note that if we choose the ordered sets $I = \underline{m}$ and $J = \underline{n}$ for some $m, n \in \mathbb{N}$ then we obtain the familiar $R^{m\times n}$-matrices. Addition and multiplication are defined in the obvious way.

Definition 3.7. Let A and B be two $I \times J$-matrices over the same ring R. Their sum is a $I \times J$-matrix over R with the following entries:

$$(A + B)(x, y) \coloneqq A(x, y) + B(x, y) \tag{3.3}$$

Let A be a $I \times J$-matrix and B a $J \times K$-matrix both over the same ring R. Then their product is a $I \times K$-matrix over R with entries

$$(A \cdot B)(x, y) \coloneqq \sum_{j\in J} A(x, j) \cdot B(j, y). \tag{3.4}$$

Note that since the addition is commutative in all rings this sum is well-defined without an order on J.

Definition 3.8. A *linear equation system* (A, b) over a ring R consists of a matrix $A : I \times J \to R$ and an I-column vector $b : I \to R$.

The system (A,b) is said to be *solvable* if there exists a solution vector $\tilde{x} : J \to R$ such that $A \cdot \tilde{x} = b$.

We need to incorporate matrices over rings into the framework of mathematical logic. We will define the encoding as in [20]. We first observe that given a formula $\psi(x, y) \in \mathrm{FO}(\tau)$ and a τ-structure $\mathfrak{A}$ we can interpret $\mathfrak{A} \models \psi(a, b)$ as 1 respectively $\mathfrak{A} \not\models \psi(a, b)$ as 0. That means we identify the extended structure $(\mathfrak{A}, \psi^{\mathfrak{A}})$ with its adjacency matrix.

Let $R = \{r_1, \dots r_k, \}$ be a finite ring and τ a signature containing $v + w$-ary relations M_{r_i} for each element in R for some fixed $v, w \in \mathbb{N}$. Suppose $\mathfrak{A}$ is a τ-structure and we have tuples $\overline{a} \in A^v$ and $\overline{b} \in A^w$. We define the index set $I \subseteq \{1, \dots, k\}$ as the smallest set satisfying that whenever $i \notin I$ then $\mathfrak{A} \not\models M_{r_i}(\overline{a}, \overline{b})$. Then we define the entry of the matrix element at position $(\overline{a}, \overline{b})$ as the sum $\sum_{i\in I} r_i$.

Instead of demanding a signature to include the relations M_{r_i} we can also describe these relations by formulae i.e. we expand a given structure $\mathfrak{A}$ by k formulae $\phi_{r_i}(x_1, \dots, x_v, y_1, \dots, y_w)$. Then the matrix is encoded in the expanded structure $(A, (\phi_{r_i}^{\mathfrak{A}})_{i\in\underline{k}})$.

Let R be a finite ring, $\phi = (\phi_r(\overline{x}_r, \overline{y}_r))_{r\in R}$, $\mathfrak{A}$ a finite structure and $M_\phi^{\mathfrak{A}}$ the encoded matrix. Then we define the *numeric rank term* $rk(\phi)$ for which all free variables are precisely those which occur in the ϕ_r but are not $\overline{x}_r$ or $\overline{y}_r$. Its numerical value is given by the rank of $M_\phi^{\mathfrak{A}}$.

Let rk be a notion of a matrix rank for a fixed ring R. Then we define the *inductive fixed-point logic with rank* FP+rk similarly to IFP+C.

Definition 3.9. The logic FP+rk is the extension IFP^+ obtained by the closure under the formation of numeric rank terms $rk_R(\cdot)$ for all finite rings R.
Alternatively we can fix a ring R and define $\mathrm{FP{+}rk}_R$ for this particular ring.

4 Rank notions

There exists several natural ways to extend the definition of matrix rank over fields to a notion of matrix rank over rings. But for the more general case of matrices over rings there are some obstacles. For example the well-known fact that the row rank equals the column rank of a matrix fails for matrices over rings (Example 2). We have to be more careful when we consider matrices over rings. The examination of different notions of a rank will be guided by the following four questions:

1. On which classes of rings is the rank notion well-defined? **(domain)**
2. What is the relationship between the ranks? **(interrelationship)**
3. Does the rank notion provide a criterion for the solvability of a LES? **(solvability)**
4. Can it be computed efficiently? **(complexity)**

4.1 Linear independence rank

Definition 4.1. Let R be a commutative ring and $A \in R^{m\times n}$ then we define the *linear indepence row rank* $rk^{LI}_{row}(A)$ as the maximal number of rows of A that are linearly independent.
The *linear indepence column rank* rk^{LI}_{col} is defined similarly for columns.

Example 2. Consider the finite commutative ring $R = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and the matrix $A \in R^{3\times 2}$ given as

$$A = \begin{bmatrix} (1,0,0) & (0,0,1) \\ (0,1,0) & (1,0,0) \\ (0,0,1) & (0,1,0) \end{bmatrix}. \tag{4.1}$$

Here we have $rk^{LI}_{col}(A) = 2$ since both columns are linear independent. The rows on the other hand are all annihilated by a single element of R and therefore $rk^{LI}_{row}(A) = 0$.

Since the elements of A are not from a field the columns and rows span a module and not a vector space. Hence we have to be more careful because modules are not as well behaved.

4.2 McCoy rank

Definition 4.2. Suppose R is a commutative ring, $A \in R^{m\times n}$ and $t \in \mathbb{N}_0$. Then let $I_t(A)$ be the ideal generated by the determinants of all $t \times t$ submatrices of A if $1 \leq t \leq r \coloneqq \min(m,n)$. If $t > r$ then $I_t(A)$ is chosen to be the zero ideal (0) and if $t = 0$ then $I_t(A)$ is the complete ring R.

From the Laplace expansion theorem follows that every $(t+1) \times (t+1)$ minor of A lies in $I_t(A)$ and therefore we have an ascending chain of ideals in R:

$$(0) \subseteq I_r(A) \subseteq \ldots \subseteq I_1(A) \subseteq R \tag{4.2}$$

By using this chain of ideals we can define a notion of matrix rank.

Definition 4.3. Let R be a commutative ring[6] and $A \in R^{m\times n}$. The *McCoy-rank* rk_{MC} is the largest natural number t such that the annihilator of the ideal $I_t(A)$ is the zero ideal (0), i.e.

$$rk_{MC}(A) \coloneqq \max\{t \in \mathbb{N}_0 \mid \operatorname{ann}_R(I_t(A)) = (0)\}. \tag{4.3}$$

Note that rk_{MC} is always between 0 and $\min(m,n)$ since $I_0(A) = R$ and $\operatorname{ann}_R(R) = (0)$ respectively $I_t(A) = (0)$ for all $t \geq min\{m,n\}$ and $\operatorname{ann}_R(0) = R$.

[6]The restriction to commutative rings is necessary because we need to evaluate determinants.

We can also define an alternative version of the McCoy rank as the maximal number $t \in \mathbb{N}_0$ for which $I_t(A) \neq (0)$. The definition is less restrictive since the ideals do not need to be free of zero divisors and therefore this rank is at least as big as the McCoy rank. Naturally both definitions coincide for matrices with entries from an integral domain.

Example 3. For some $n \in \mathbb{N}$ we define $A = \operatorname{diag}(p, \dots, p) \in \mathbb{Z}_{p^{n+1}}$ with p prime. Then $I_t(A) = (p^t) \neq (0)$ for all $t \in \underline{n}$ and therefore the alternative McCoy rank equals n. But $\operatorname{ann}_R(I_t(A)) = (p^{n+1-t})$ for all $t \in \underline{n}$ which means that the McCoy rank is 0.
We conclude that the difference between the McCoy rank and its less restrictive alternative definition can be arbitrary large.

4.3 Column and row rank

Probably the most commonly known definition for a matrix rank are the column/row rank. In case of fields the column rank is defined as the dimension of the vector space spanned by the columns of the matrix. But if we only require the entries of the matrix to be elements of a ring then the column space is a module and not a vector space. Therefore we have to be careful with our definition. Let us consider the following example.

Example 4. To show that the image of a module homomorphism induced by a matrix is not necessarily free, we consider a finite ring R and the 1×1-matrix (a) with $a \in R \setminus R^\times$.

The image $im(A) = aR$ is a submodule of R. Suppose aR is a free R-module then there would exist a $k \in \mathbb{N}_0$ such that $aR \cong R^{\oplus k}$. But this would imply $|aR| = |R^{\oplus k}|$ which does not hold for any $k \in \mathbb{N}$ since $|aR| < |R|$. Therefore aR is not a free R-module.

To overcome this problem we have to restrict ourselves to so-called *free ideal rings* (see 2.18).

Definition 4.4. Let R be a n-FIR and $A \in R^{m \times n}$ then the *column rank* rk_{col} is defined as the rank of the submodule of $R^{m \times 1}$ spanned by the n columns of A, i.e.

$$rk_{col} \coloneqq \text{rank } im(A) \tag{4.4}$$

if we think of A as a right R-module homomorphism of columns $R^{n \times 1} \to R^{m \times 1}$.

Similarly we can define the row rank.

Definition 4.5. Let R be a m-FIR and $A \in R^{m \times n}$ then the *row rank* rk_{row} is defined as the rank of the submodule of $R^{1 \times n}$ spanned by the m rows of A, i.e.

$$rk_{row} \coloneqq \text{rank } im(A) \tag{4.5}$$

if we think of A as a left R-module homomorphism of rows $R^{1 \times m} \to R^{1 \times n}$.

If we are dealing with a $m \times n$ matrix A over a $\max(m,n)$-FIR we both rank notions are well-defined. We will discuss later how column and row rank are related.

4.4 Inner rank

The rank which can be defined for the most general class of rings is the inner rank rk_{inn}, since it is defined over arbitrary rings.

Definition 4.6. Let R be a ring and $A \in R^{m \times n}$ then the *inner rank* rk_{inn} is defined as

$$rk_{inn} \coloneqq \begin{cases} 0, & \text{if } A = 0 \\ \min\{k \in \mathbb{N} \mid \text{ex. } B \in R^{m \times k}, C \in R^{k \times n} \text{ s.t. } A = B \cdot C\}, & \text{if } A \neq 0 \end{cases} \tag{4.6}$$

which is an integer between 0 and $\min(m,n)$[7].

[7] Because the decompostion $A = E_m A$ or $A = A E_n$ always exists.

There are a number of equivalent definitions respectively interpretations for the inner rank, e.g.

- if we interpret A as a left R-module homomorphism of rows $R^{1\times m} \to R^{1\times n}$ it is equal to the least $k \in \mathbb{N}_0$ such that the image of A in $R^{1\times n}$ is contained in a submodule generated by k elements
- if we interpret A as a right R-module homomorphism of columns $R^{n\times 1} \to R^{m\times 1}$ it is equal to the least $k \in \mathbb{N}_0$ such that the image of A in $R^{m\times 1}$ is contained in a submodule generated by k elements
- the least $k \in \mathbb{N}_0$ of pairs of columns $b_i \in R^{m\times 1}$ and rows $c_i \in R^{1\times n}$ such that

$$A = \sum_{i=1}^{k} b_i \cdot c_i \tag{4.7}$$

  i.e. the least $k \in \mathbb{N}_0$ such that A can be written as the sum of rank 1 matrices.

The last definition is simply the matrix multiplication of 4.6 rewritten in terms of rows of B and columns of C.

4.5 Sign rank

The sign rank gives us the desired necessary and sufficient condition for the solvability of a linear equation system.

Definition 4.7. Let R be a Galois-Eisenstein ring with nilradical $\mathcal{N}(R) = (\pi)$ and nilpotency index n. Furthermore we suppose $A \in R^{m\times n}$. By Lemma **??** there exist matrices $S \in GL(m, R)$ and $T \in GL(n, R)$ such that

$$SAT = \operatorname{diag}(\pi^{s_1}, \ldots, \pi^{s_r}) \tag{4.8}$$

with $r = min\{m, n\}$ and $0 \leq s_1 \leq \ldots \leq s_r \leq n$. The *sign-rank* rk_{sign} is the tuple

$$rk_{sign}(A) \coloneqq (s_1, \ldots, s_r). \tag{4.9}$$

Hence, in order to determine $rk_{sign}(A)$ it suffices to find suitable matrices S and T. Note that the sign rank is closely related to the *elementary divisors* of the Smith normal form.

5 Elementary Properties

5.1 Invariance under transposition

One of the first theorems a student of linear algebra comes across states that the row rank of a matrix equals its column rank. In other words, the rank of a matrix should be equal to its transposed matrix. We want to analyze if this property is true in general, i.e. if for a rank rk

$$rk(A^{tr}) = rk(A) \tag{5.1}$$

holds for all matrices A for which the rank is defined.

The McCoy rank inherits the invariance from the properties of the determinant of a matrix. Since $\det(A^{tr}) = \det(A)$ holds for arbitrary matrices[8] we conclude that the determinal ideals are invariant under transposition, i.e. $I_t(A^{tr}) = I_t(A)$ and thus 5.1 holds.

The sign rank is invariant under transposition because

$$rk(A^{tr}) = rk((SDT^{-1})^{tr}) = rk((T^{-1})^{tr}D^{tr}S^{tr}) = rk(D) = rk(A). \tag{5.2}$$

Here we used the fact that the transposed of an invertible matrix is again an invertible matrix[8].

It is also easy to see that the inner rank is invariant under transposition. Let us assume that the inner rank of some matrix A is $k \in \mathbb{N}$, Then there are rows r_i and columns c_i such that $A = \sum_{i=1}^{k} c_i \cdot r_i$. By transposing the equation we obtain a decomposition of A^{tr}:

$$A^{tr} = \sum_{i=1}^{k} r_i^{tr} \cdot c_i^{tr} \tag{5.3}$$

The decomposition is minimal since if we had a decomposition with $k' < k$ summations we could transpose again and get a decomposition of A with k' summations which is a contradiction to the minimality of k.

We have seen in example 2 that column and row rank defined by linear independence are not equal in general and therefore they are not invariant under transposition. But also with our more careful definition over the module rank, column and row rank are in general unrelated, as we can see in the following example taken from [5].

Example 5. Let R be a free ideal ring and $x_1, \ldots, x_m \in R$ left linearly independent elements, i.e. from $\sum_{i=1}^{m} \lambda_i x_i = 0$ follows $\lambda_i = 0$ for all $i \in \underline{m}$. For the matrix

$$A = \begin{bmatrix} x_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x_m & 0 & \cdots & 0 \end{bmatrix} \tag{5.4}$$

we have that $rk_{row}(A) = m$ whereas $rk_{col}(A) = 1$.

5.2 Invariance under equivalence

The McCoy rank is invariant under equivalence. To show this we need the following Lemma taken from [18].

Lemma 5.1. *Let R be a commutative ring, $A \in R^{m\times k}$ and $B \in R^{k\times n}$. Then we have*

$$I_t(AB) \subseteq I_t(A) \cap I_t(B) \tag{5.5}$$

for all $t \in \mathbb{N}_0$.

[8] For elementary results from linear algebra see [14].

Theorem 5.2. *Let R be a commutative ring, $S \in GL(m,R)$, $T \in GL(n,R)$ and $A \in R^{m\times n}$. Then*

$$I_t(SAT) = I_t(A) \tag{5.6}$$

for all $t \in \mathbb{N}_0$.

Proof. With Lemma 5.1 follows:

$$I_t(SA) \subseteq I_t(S) \cap I_t(A) \subseteq I_t(A) \tag{5.7}$$

and

$$I_t(A) = I_t(S^{-1}SA) \subseteq I_t(S^{-1}) \cap I_t(SA) \subseteq I_t(SA). \tag{5.8}$$

Therefore we have $I_t(A) = I_t(SA)$ for all $t \in \mathbb{N}_0$. A similar proof for $I_t(A) = I_t(AT)$ yields the claim. ∎

Since the McCoy rank was defined by means of the determinal ideals $I_t(A)$ we get the following corollary.

Corollary 5.3. *Let R be a commutative ring, $S \in GL(m,R)$, $T \in GL(n,R)$ and $A \in R^{m\times n}$ then $rk_{MC}(SAT) = rk_{MC}(A)$.*

Theorem 5.4. *Let R be a commutative chain ring, $S \in GL(m,R)$, $T \in GL(n,R)$ and $A \in R^{m\times n}$ then $rk_{sign}(SAT) = rk_{sign}(A)$.*

Proof. This follows directly from the definition. ∎

Theorem 5.5. *Let R be a ring, $S \in GL(m,R)$, $T \in GL(n,R)$ and $A \in R^{m\times n}$ then $rk_{inn}(SAT) = rk_{inn}(A)$.*

Proof. If $A = 0$ there is nothing to show. For $A \neq 0$ we assume that $k \coloneqq rk_{inn}(SAT) < rk_{inn}(A)$. Then we can find matrices $B \in R^{m\times k}$ and $C \in R^{k\times n}$ such that $SAT = BC$. But this is a contradiction since $A = S^{-1}BCT^{-1}$.
The case $rk_{inn}(SAT) > rk_{inn}(A)$ is follows similarly. ∎

Theorem 5.6. *Let R be a FIR, $S \in GL(m,R)$, $T \in GL(n,R)$ and $A \in R^{m\times n}$ then $rk_{row}(SAT) = rk_{row}(A)$ and $rk_{col}(SAT) = rk_{col}(A)$.*

Proof. Since T is invertible we have

$$im(A) = AR^n = ATR^n = im(AT) \tag{5.9}$$

and therefore $rk_{col}(AT) = rk_{col}(A)$. On the other hand we have that since S is invertible $\operatorname{rank}(im(SA)) = \operatorname{rank}(im(A))$ and therefore $rk_{col}(SA) = rk_{col}(A)$.
The claim for the row rank is proven similarly. ∎

The linear independence rank is not invariant under equivalence for matrices over general rings, as the following example shows.

Example 6. Suppose $R = \mathbb{Z}_6^{2\times 2}$. Consider the matrices

$$A = \begin{bmatrix} 4 & 3 \\ 0 & 0 \end{bmatrix} \in R^{2\times 2} \tag{5.10}$$

and

$$S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in GL(2,R). \tag{5.11}$$

Then $rk_{col}^{LI}(A) = 0$ since the first column of A is annihilated by 3 and the second column by 4. On the other hand we have

$$SAT = \begin{bmatrix} 1 & 3 \\ 0 & 0 \end{bmatrix} \tag{5.12}$$

and therefore $rk_{col}^{LI}(SAT) = 1$.

5.3 Comparability

The fact that the McCoy rank, the inner rank, the column rank and the row rank are equal over fields is an immediate consequence of their invariance under equivalence and the fact that every matrix over a field is equivalent to a matrix of the form $\mathrm{diag}(1,\dots,1,0,\dots,0)$. Furthermore since the number of linear independent columns (resp. rows) of a matrix is exactly the dimension of the image of A, if interpreted as a mapping of columns via left-multiplication (resp. mapping of rows via right-multiplication), both linear independence ranks are also equal to the ones above if the .

Theorem 5.7. *Let F be a field and $A \in F^{m\times n}$ then then the McCoy rank, inner rank, linear independence rank (of columns and rows) and the column/row rank of A are equal, i.e.*

$$rk_{MC}(A) = rk_{inn}(A) = rk^{LI}_{col/row}(A) = rk_{col/row}(A). \tag{5.13}$$

We want to investigate further in which relation the ranks notions stand over rings which are not fields. We will do this by defining the class of rings on which two rank notions are well-defined and comparing them.

5.3.1 McCoy and column/row rank

The McCoy rank was defined over commutative rings whereas row and column rank were defined over free ideal rings. Therefore it only makes sense to compare both over the class of commutative free ideal rings which is exactly the class of principal ideal domains (see [5]). Let R be a PID and $A \in R^{m\times n}$ then we can assume w.l.o.g. that A is in Smith normal form since we know that equivalent matrices have equal ranks. Thus let $A = \mathrm{diag}(d_1,\dots,d_r,0,\dots,0)$. Since R is a domain we have $\mathrm{ann}_R(I) = (0)$ for any ideal $I \neq (0)$. Therefore the maximal $k \in \mathbb{N}_0$ such that $\mathrm{ann}_R(I_k(A)) = (0)$ is r. On the other hand the row/column rank is obviously also r. This means on the class of rings on which both McCoy and row/column rank are defined they are equal.

5.3.2 Inner and column/row rank

Theorem 5.8. *For any matrix $A \in R^{m\times n}$ with R a free ideal ring we have*

$$rk_{inn}(A) \leq rk_{col}(A) \tag{5.14}$$

and

$$rk_{inn}(A) \leq rk_{row}(A). \tag{5.15}$$

Proof. Let R be a free ideal ring and $A \in R^{m\times n}$. Set $k \coloneqq rk_{inn}(A)$ and $d \coloneqq rk_{col}(A)$. Since $im(A)$ is a free module there exist $b_1,\dots,b_d \in R^m$ such that $\langle b_1,\dots,b_d\rangle_R = im(A)$. The columns of A are elements of the image of A, i.e. $A_{*,j} \in im(A)$. Therefore we can find $c_{r,j} \in R$ such that

$$A_{*,j} = \sum_{r=1}^{d} b_r c_{r,j} \tag{5.16}$$

for each $j \in \underline{m}$. By defining the matrices $B \coloneqq (b_1,\dots,b_d) \in R^{m\times d}$ and $C \coloneqq (c_{r,j})_{r\in\underline{d},j\in\underline{n}} \in R^{d\times n}$ we have a decomposition $A = BC$. But since the inner rank k is defined as the the smallest integer such that a decomposition into a $m\times k$- and a $k\times n$-matrix exists we have $k \leq d$.
The inequality for the row rank is proven similarly. ∎

The following Lemma is taken from [5] without a proof.

Lemma 5.9. *Let R be a right Bézout domain and M a right R-module. If N is a submodule or a homomorphic image of M then*

$$rank(N) \leq rank(M). \tag{5.17}$$

The same statement holds for left Bézout domains R and left R-modules.

Theorem 5.10. *If R is a right Bézout domain and $A \in R^{m\times n}$ then the inner rank equals the column rank, i.e. $rk_{inn}(A) = rk_{col}(A)$.*
Similarly, if R is a left Bézout domain and $A \in R^{m\times n}$ then the inner rank equals the row rank, i.e. $rk_{inn}(A) = rk_{row}(A)$.

Proof. We can interpret A as a right R-module homomorphism of columns $R^n \to R^m$. Under this interpretation the inner rank is the smallest $k \in \mathbb{N}_0$ such that A factors through R^k via mappings B and C with $A = BC$. Since $im(A) \leq im(B)$ and $im(B)$ is a homomorphic image of R^k we have by Lemma 5.9:

$$rk_{col}(A) = rank(im(A)) \leq rank(im(B)) \leq rank(R^k) = rk_{inn}(A) \tag{5.18}$$

With Theorem 5.8 follows the equality of both ranks.
If we interpret a matrix over a left Bézout domain R as a left R-module homomorphism of rows we can similarly proof the equality of the inner rank and the row rank. ∎

Corollary 5.11. *If R is a left and right Bézout domain then column, row and inner rank are equal for all matrices with entries in R.*

5.3.3 Inner and LI-rank

Theorem 5.12. *Let R be a commutative ring. For all $A \in R^{m\times n}$ we have*

$$rk^{LI}_{col}(A) \leq rk_{inn}(A) \tag{5.19}$$

and

$$rk^{LI}_{row}(A) \leq rk_{inn}(A) \tag{5.20}$$

Proof. Let A be some matrix as defined above. We set $k \coloneqq rk^{LI}_{col}(A)$. By definition of the LI-rank we can find k linearly independent columns $\{c_1, \ldots, c_k\}$ of A. The mapping $\phi : R^k \to im(A), (r_1, \ldots, r_k) \mapsto \sum_{i=1}^{k} r_i c_i$ is injective.
On the other hand we can find matrices $B \in R^{m\times l}$ and $C \in R^{l\times n}$ with $l \coloneqq rk_{inn}(A)$ and $A = BC$. From this we see that

$$im(A) \leq im(B) \leq R^l. \tag{5.21}$$

Combining both estimates we obtain $k \leq l$.
The claim for rk^{LI}_{row} is proven similarly. ∎

The following example shows that the inequality can be strict.

Example 7. We consider the matrix

$$A = \begin{bmatrix} 2 & \\ & 2 \end{bmatrix} \in \mathbb{Z}_4^{2\times 2}. \tag{5.22}$$

We have $rk^{LI}_{col}(A) = rk^{LI}_{row}(A) = 0$ but $rk_{inn}(A) = 2$.[9]

[9] Note that $rk_{inn}(A) = 2$ can be proven by writing down an arbitrary 2×1- resp. 1×2-matrix and derive contradicting properties for their entries. The full inner rank does not follow from the diagonal form of A.

5.3.4 Inner and McCoy rank

Lemma 5.13. *Let R be a commutative ring, $m, k \in \mathbb{N}$ with $k < m$ and $A \in R^{m\times m}$, $B \in R^{m\times k}$, $C \in R^{k\times m}$ such that $A = B \cdot C$. Then* $\det(A) = 0$.

Proof. The determinant of a matrix is multilinear in the columns of the matrix, i.e.

$$\begin{aligned}&\det\left[A_{*1}, \ldots, rA_{*i} + sA'_{*i}, \ldots, A_{*m}\right]\\ =&r\det\left[A_{*1}, \ldots, A_{*i}, \ldots, A_{*m}\right] + s\det\left[A_{*1}, \ldots, A'_{*i}, \ldots, A_{*m}\right].\end{aligned} \tag{5.23}$$

Since $A = B \cdot C$ we can think of the columns of A as a linear combination of the k columns $B_{*i} \in R^m$:

$$A = \left[\sum_{i=1}^{k} C_{i1}B_{*i}, \ldots, \sum_{i=1}^{k} C_{im}B_{*i}\right] \tag{5.24}$$

By applying 5.23 repeatedly we get the following equation:

$$\begin{aligned}\det(A) &= \det\left[\sum_{i=1}^{k} C_{i1}B_{*i}, \sum_{j=1}^{k} C_{j2}B_{*j}, \ldots, \sum_{q=1}^{k} C_{qm}B_{*q}\right]\\ &= \sum_{i=1}^{k} C_{i1}\det\left[B_{*i}, \sum_{j=1}^{k} C_{j2}B_{*j}, \ldots, \sum_{q=1}^{k} C_{qm}B_{*q}\right]\\ &= \sum_{i=1}^{k} C_{i1}\left(\sum_{j=1}^{k} C_{j2}\det\left[B_{*i}, B_{*j}, \sum_{l=1}^{k} C_{l3}B_{*l}, \ldots, \sum_{q=1}^{k} C_{qm}B_{*q}\right]\right)\\ \ldots &= \sum_{i=1}^{k} C_{i1}\left(\ldots\left(\sum_{p=1}^{k} C_{p,k+1}\det\left[\underbrace{B_{*i}, \ldots, B_{*p}}_{k+1}, \ldots, \sum_{q=1}^{k} C_{qm}B_{*q}\right]\right)\ldots\right)\end{aligned} \tag{5.25}$$

We can iterate this at least $k+1$ times since $k < m$. Thus in the last line each matrix has $k+1$ columns from B from which at least two must be equal. Therefore the determinant of each matrix must be zero from which directly follows that $\det(A) = 0$. ∎

Theorem 5.14. *Let R be a commutative ring. For all $A \in R^{m\times n}$ we have*

$$rk_{MC}(A) \leq rk_{inn}(A). \tag{5.26}$$

Proof. If $k \coloneqq rk_{inn}(A)$ then there exist matrices $B \in R^{m\times k}$ and $C \in k \times n$ such that $A = B \cdot C$. Let $\overline{A}$ be a $(k+1) \times (k+1)$-submatrix of A. Since the entries of A are given by $A_{ij} = \sum_{l=1}^{k} B_{il}C_{lj}$ we can find matrices $\overline{B} \in R^{(k+1)\times k}$ and $\overline{C} \in R^{k\times(k+1)}$ such that $\overline{A} = \overline{B} \cdot \overline{C}$. With Lemma 5.13 follows that $\det(\overline{A}) = 0$. Since $\overline{A}$ was arbitrary the determinal ideal of $(k+1)$-submatrices is the zero ideal, i.e. $I_{k+1}(A) = (0)$. Therefore we have $rk_{MC}(A) \leq k$. ∎

The matrix A from Example 7 shows again that the inequality can be strict: $rk_{MC}(A) = 0$ but $rk_{inn}(A) = 2$.

5.3.5 Column/row and LI-rank

Lemma 5.15. *Let R be an integral domain, M a free R-module. Then any two maximal linearly independent subsets of M have the same cardinality.*

Proof. By embedding R into its field of fractions the claim follows directly from the fact that it is known to be true for vector spaces. ∎

Theorem 5.16. *Let R be a PID and $A \in R^{m\times n}$. Then we have*

$$rk_{col}^{LI}(A) = rk_{col}(A) \tag{5.27}$$

and

$$rk_{row}^{LI}(A) = rk_{row}(A). \tag{5.28}$$

Proof. This follows directly from Lemma 5.15 and the fact that any basis of a module is a maximal linearly independent set. ∎

6 Solvability of LES

An application of matrix ranks that is already taught in schools is its use as a mean to check if a system of linear equations

$$Ax = b \tag{6.1}$$

has a solution. This is done via the Kronecker–Capelli Theorem.

Theorem 6.1 (Kronecker–Capelli Theorem)**.** *Let F be a field and $A \in F^{m\times n}$ and $b \in F^{m\times 1}$. Then the linear equation system 6.1 is solvable iff*

$$rk(A) = rk(A \mid b). \tag{6.2}$$

The theorem is usually proven using the row-echelon form of A respectively $(A \mid b)$.

In this chapter we investigate if the ranks we defined in chapter 4 can be used similarly to determine weither a LES over a ring has a solution or not.

6.1 McCoy rank

For the McCoy rank the Kronecker–Capelli Theorem still gives us a necessary condition for the solvability of 6.1.

Theorem 6.2. *Let R be a commutative ring, $A \in R^{m\times n}$ and $b \in R^n$. If the LES $Ax = b$ has a solution, then the rank of A is the same as the rank of the augmented matrix $(A \mid b)$, i.e. $rk_{MC}(A) = rk_{MC}(A \mid b)$.*

Proof. Since the submatrices of A are also submatrices of the augmented matrix $(A \mid b)$ we always have

$$I_t(A) \subseteq I_t(A \mid b). \tag{6.3}$$

To show that $I_t(A \mid b) \subseteq I_t(A)$ we examine the generators of $I_t(A \mid b)$. The minors of $(A \mid b)$ which do not involve elements of b are also minors of A. Thus let us consider the other case.
Since 6.1 has a solution $\tilde{x}$ we have

$$\sum_{j=1}^{m} A_{i,j}\tilde{x}_j = b_i \tag{6.4}$$

$$\Leftrightarrow \sum_{j=1}^{t} A_{i,j}\tilde{x}_j = b_i - \sum_{j=t+1}^{n} A_{i,j}\tilde{x}_j \tag{6.5}$$

for all $i \in \underline{n}$. Let us now consider the $t \times t$-submatrix $\overline{A} \coloneqq (A_{i,j})_{i,j\in\underline{t}}$ which is the submatrix in the top left corner. Together with 6.5 and by multiplication on both sides with the adjugate matrix[10] we get

$$adj(\overline{A})\overline{A} \begin{bmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_t \end{bmatrix} = adj(\overline{A}) \begin{bmatrix} b_1 \\ \vdots \\ b_t \end{bmatrix} - adj(\overline{A}) \sum_{j=t+1}^{n} \begin{bmatrix} \overline{A}_{1,j} \\ \vdots \\ \overline{A}_{1,j} \end{bmatrix} \tilde{x}_j. \tag{6.6}$$

The first term on the right hand side of 6.6 yields

$$\mathrm{adj}(\overline{A}) \begin{bmatrix} b_1 \\ \vdots \\ b_t \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{t} (\mathrm{adj}(\overline{A}))_{1j} b_j \\ \vdots \\ \sum_{j=1}^{t} (\mathrm{adj}(\overline{A}))_{tj} b_j \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{t} (-1)^{j+1} \det(\overline{A}^{j1}) b_j \\ \vdots \\ \sum_{j=1}^{t} (-1)^{j+t} \det(\overline{A}^{jt}) b_j \end{bmatrix}. \tag{6.7}$$

[10] The entries of the adjungate matrix $\mathrm{adj}(A)$ of a square matrix A are defined as $\mathrm{adj}(A)_{ij} \coloneqq (-1)^{i+j}\det(A^{ji})$. Here A^{ji} denotes the matrix which is obtained from A by deleting the jth row and ith column.

If we define $\overline{B}$ as the matrix which has $[b_1, \dots, b_t]^{tr}$ as its first column and all other columns equal to those in $\overline{A}$ we can apply the Laplace expansion formula and get

$$\text{adj}(\overline{A}) \begin{bmatrix} b_1 \\ \vdots \\ b_t \end{bmatrix} = \begin{bmatrix} \det(\overline{B}) \\ \vdots \\ \det(\overline{B}) \end{bmatrix}. \tag{6.8}$$

The second term on the right hand side of 6.6 can be rewritten similarly by defining matrices C_j where we replace the first column of $\overline{A}$ by $\left[A_{1,j}, \dots, A_{t,j}\right]^{tr}$. Note that all C_j are submatrices of A.
The left hand side of 6.6 can be rewritten by using Cramers rule

$$\text{adj}(\overline{A})\overline{A} = det(\overline{A})E_t. \tag{6.9}$$

Thus the first row of 6.6 is given by

$$det(\overline{A})\tilde{x}_1 = det(\overline{B}) - \sum_{j=t+1}^{n} det(C_j)\tilde{x}_j. \tag{6.10}$$

We see that $det(\overline{B})$, which is a generator of $I_t(A \mid b)$, is a linear combination of generators of $I_t(A)$. The claim follows for all generators of $I_t(A \mid b)$ by permuting rows and columns. ∎

Unfortunately the converse of Theorem 6.2 is not true in general as the following example shows.

Example 8. Let F be a field and $R = F[X, Y]/(X^2 - Y^3)$. Furthermore we define an equation system $Ax = b$ with

$$A = \begin{bmatrix} X & Y & 0 \\ 0 & 0 & Y \end{bmatrix} \in R^{2\times 3} \text{ and } b = \begin{bmatrix} 0 \\ X \end{bmatrix} \in R^{2\times 1}. \tag{6.11}$$

Then we have $I_1(A) = I_1(A \mid b) = (X, Y)$ and $I_2(A) = (XY, Y^2)$. Furthermore we have $I_2(A \mid b) = (XY, X^2, Y^2) = (XY, Y^2)$ since $X^2 = Y^3 \in (XY, Y^2)$.
Therefore we have $I_t(A) = I_t(A \mid b)$ for all $t \in \mathbb{N}_0$ from which directly follows that $rk_{MC}(A) = rk_{MC}(A \mid b)$.
The equation system $Ax = b$ can only have a solution if $X \in (Y)$. Then $X - \alpha Y = \beta(X^2 - Y^3)$ for some $\alpha, \beta \in F[X, Y]$. But this is impossible and therefore $Ax = b$ has no solution in $R^{3\times 1}$.

However, the McCoy rank still provides a necessary and sufficient criterion for the (non-trivial) solvability of homogeneous equation systems.

Theorem 6.3. *Let R be a commutative ring and $A \in R^{m\times n}$. The homogeneous system of equations $Ax = 0$ has a non-trivial solution if and only if $rk_{MC} < n$.*

The proof of Theorem 6.3 is directly taken from [18] p.85.

Proof. Suppose $t := rk_{MC}(A) < n$. Then $\text{ann}_R(I_{t+1})(A)) \neq (0)$. Select $0 \neq y \in R$ with $I_{t+1}(A)y = 0$. W.l.o.g. we can assume that $t < m$ since we can replace the system $Ax = 0$ with an equivalent system where we add additional equations having coefficients which are all zero. If $t = 0$, then $x_i := y$ for all $i \in \underline{n}$ is a non-trivial solution.

Suppose that $t > 0$. Then the product of y and some generator of $I_t(A)$ is nonzero. This generator is by definition a determinant of a $t \times t$-submatrix of A. By permuting columns and rows we can assume that the submatrix is given by

$$T = \begin{bmatrix} a_{11} & \cdots & a_{1t} \\ \vdots & & \vdots \\ a_{t1} & \cdots & a_{tt} \end{bmatrix} \in R^{t\times t} \tag{6.12}$$

where $A = (a_{ij})$. Consider the submatrix

$$\overline{T} = \begin{bmatrix} a_{11} & \cdots & a_{1,t+1} \\ \vdots & & \vdots \\ a_{t+1,1} & \cdots & a_{t+1,t+1} \end{bmatrix} \in R^{(t+1)\times(t+1)}. \tag{6.13}$$

Let D_i denote the determinant of the submatrix of $\overline{T}$ formed by deleting column i and row $t+1$. Let $e_i = (-1)^{t+1+i} D_i$. Set $\overline{x}_i := ye_i$ for $1 \leq i \leq t+1$ and $\overline{x}_i := 0$ for $t+2 \leq i \leq n$. Then we have

$$A\overline{x} = \begin{bmatrix} \left(\sum_{j=1}^{t+1} a_{1j}e_j\right) y \\ \vdots \\ \left(\sum_{j=1}^{t+1} a_{mj}e_j\right) y \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \tag{6.14}$$

since $\sum_{j=1}^{t+1} a_{ij}e_j = 0$ for all $1 \leq i \leq t$ by Laplace expansion and $\left(\sum_{j=1}^{t+1} a_{ij}e_j\right) y = 0$ for all $t+1 \leq i \leq m$ since $y \in \operatorname{ann}_R(I_{t+1}(A))$ and $\sum_{j=1}^{t+1} a_{ij}e_j$ is a generator of $I_{t+1}(A)$. Note that $\overline{x} \neq 0$ since $\overline{x}_{t+1} = y \det(T) \neq 0$.

Now let us assume that $\overline{x}$ is a solution with $\overline{x}_1 \neq 0$. We claim that $\operatorname{ann}_R(I_n(A)) \neq (0)$. If $n > m$, then $I_n(A) = (0)$ and thus $\operatorname{ann}_R(I_n(A)) = R$. Thus we may assume that $n \leq m$. Let D be be the determinant of the submatrix

$$T = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}. \tag{6.15}$$

Then $D\overline{x}_1 = 0$, since $T\overline{x} = 0$ implies that $D\overline{x} = \operatorname{adj}(T)T\overline{x} = 0$. Similarly, if $\overline{D}$ is the determinant of any $n \times n$ submatrix of A, then $\overline{D}\overline{x}_1 = 0$. Therefore $\overline{x}_1 \in \operatorname{ann}_R(I_n(A))$. ∎

Note that this shows the uniqueness of the solution of 6.1, provided that a solution exists and that $Ax = b$ has a nontrivial solution if and only if $\det(A)$ is a zero divisor in R.

6.2 LI-rank

The following example shows that the Kronecker–Capelli Theorem fails for the LI rank.

Example 9. We consider

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathbb{Z}_4^{4\times 3} \text{ and } b = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \in \mathbb{Z}_4^{4\times 1}. \tag{6.16}$$

Then $rk_{row}^{LI}(A) = rk_{row}^{LI}(A \mid b) = 3$ but the LES $Ax = b$ is clearly not solvable.

6.3 Sign rank

The only rank that can be used in the Kronecker-Capelli Theorem is the sign rank. The following theorem is taken from [19] without a proof.

Theorem 6.4. *Let R be a Galois-Eisenstein ring, $A \in R^{m\times n}$ and $b \in R^{m\times 1}$. The linear equation system $Ax = b$ has a solution if and only if*

$$rk_{sign}(A \mid 0) = rk_{sign}(A \mid b). \tag{6.17}$$

7 Complexity

The algorithmic complexity of the model checking problem for a logic extended by rank operators depends on the complexity of computing the rank. Therefore the computational complexity of each rank is important to understand which complexity class a rank logic with a specific rank can capture. For fields there exists the well-known Gaussian algorithm which can be used to compute the rank efficiently. However in rings divisibility of non-zero elements is not given and thus we have to analyze for each rank notion which complexity its evaluation has.

Theorem 7.1. *Let R be a commutative ring, $A \in R^{m\times n}$ and $t \in \mathbb{N}_0$. Then the problem whether*

$$rk_{MC}(A) < t \tag{7.1}$$

is in coNP.

Proof. We show that $rk_{MC}(A) \geq t$ is in NP by guessing a $t \times t$-submatrix B of A as a witness. The determinant $d =: \det(B)$ can be computed in polynomial time[11]. All we need to do is check if $r \cdot d \neq 0$ for all $r \in R \setminus \{0\}$. Then we have that $\operatorname{ann}_R(I_t(A)) = (0)$ and therefore $rk_{MC}(A) \geq t$. ∎

Lemma 7.2. *Let R be a commutative ring and $A \in R_{m\times n}$ then the problem of finding a maximal linearly independent set of rows/columns is in EXPTIME.*

Proof. In the worst case we have to check for any subset of columns if they are linear dependent. This requires $\sum_{k=0}^{n} \binom{n}{k}(k-1) = 2^{n-1}n - 2^n$ additions and $\sum_{k=0}^{n} \binom{n}{k}|R|^k \in \mathcal{O}(2^n)$ multiplications. ∎

Since the McCoy and the LI rank are defined over very general classes of rings we could not make use of the structure of the rings. However there are some rings which are not fields but which have nice properties that make the efficient computation of some ranks feasible.

Lemma 7.3. *If R is a Galois-Eisenstein ring then for any $r, s \in R$ we have $r|s$ or $s|r$.*

Proof. Since R is local the set $m = R \setminus R^\times$ is the unique maximal ideal in R. Because every ideal in R is principal we can find a $\pi \in m$ such that $m = (\pi)$. This allows us to write any $r, s \in R$ as $r = \pi^i u$ respectively $s = \pi^j V$ with $u, v \in R^\times$ and $i, j \in \mathbb{N}_0$. Thus if $j \leq i$ we have $s|r$ and if $i \leq j$ we have $r|s$. ∎

In other words, divisibility is a preorder on chain rings.

Lemma 7.4. *Given a Galois-Eisenstein ring R and a matrix $A \in R^{m\times n}$, then we can obtain the Smith normal form of A in PTIME, i.e. we can compute matrices $S \in GL(m, R)$ and $T \in GL(n, R)$ such that*

$$SAT = \begin{bmatrix} r_1 & & & & & \\ & \ddots & & & & \\ & & r_k & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix} \tag{7.2}$$

where $r_1, \ldots, r_k \in R$ and $r_i | r_{i+1}$ for all $i = 1, \ldots, k-1$.

Proof. By Lemma 7.3 we can find an entry r of A which divides all other entries. By column and row permutations we can bring r into the upper left corner. Then, we use the first row to eliminate all other entries of the first column and vice versa to obtain an equivalent matrix of the form

$$\begin{bmatrix} r & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \overline{A} & \\ 0 & & & \end{bmatrix}. \tag{7.3}$$

[11] To be exact in $\mathcal{O}(t^{2.6973})$, see [17].

Note that r still divides all entries of the submatrix $\overline{A}$ since all of its entries are linear combinations of entries of A and continue this procedure with the lower right $(m-1)\times(n-1)$-submatrix $\overline{A}$.
The elimination in the ith step takes $(m-i)+(n-i)$ additions and multiplications and there are at most $\min(m,n)$ steps in the worst case scenario. ∎

The diagonal elements are unique up to multiplication by a unit. However, in a Galois-Eisenstein ring we can improve this further to make the diagonal form unique.

Corollary 7.5. *Let R be a Galois-Eisenstein ring with nilradical $\mathcal{N}(R)=(\pi)$, q the nilpotency index of π and $A\in R^{m\times n}$. Then there exist matrices $S\in GL(m,R)$ and $T\in GL(n,R)$ such that*

$$SAT = diag(\pi^{s_1},\dots,\pi^{s_r}) \tag{7.4}$$

with $r=\min(m,n)$ and $0\leq s_1\leq\ldots\leq s_r$.

Proof. By Lemma 7.4 we can find $S\in GL(m,R)$ and $T\in GL(n,R)$ such that $SAT=\operatorname{diag}(r_1,\dots,r_k,0,\dots,0)=\operatorname{diag}(r_1,\dots,r_k,\pi^p,\dots,\pi^p)$. Since the k non-zero diagonal elements of the SNF of A have the form $r_i=u_i\pi^{q_i}$ with $u_i\in R^\times$ and $p_i\in\mathbb{N}_0$. We define

$$S' \coloneqq \operatorname{diag}(u_1^{-1},\dots,u_k^{-1},1,\dots,1)\in GL(m,R) \tag{7.5}$$

and obtain the result

$$(S'S)AT = \operatorname{diag}(\pi^{s_1},\dots,\pi^{s_r}) \tag{7.6}$$

with $r=\min(m,n)$ and $0\leq s_1\leq\ldots\leq s_r\leq p$. ∎

Theorem 7.6. *Given a Galois-Eisenstein ring R, the generating element of the nilradical of R and a matrix $A\in R^{m\times n}$ then the sign rank $rk_{sign}(A)$ can be computed in PTIME.*

Proof. The claim is an immediate consequence of Corollary 7.5. ∎

The following Lemma is taken from [6].

Lemma 7.7. *Let R be a finite commutative ring, then there exists a subset $\{e_1,\dots,e_k\}\subseteq R$ such that*

1. *the elements of this set are orthogonal idempotents*

$$e_i\cdot e_j=\begin{cases}e_i, & \text{if } i=j\\ 0, & \text{else}\end{cases}, \tag{7.7}$$

2. *they are a decomposition of 1_R*

$$\sum_{i=1}^{k} e_i = 1_R, \tag{7.8}$$

3. *and their ideals e_iR are local.*

Therefore all finite commutative rings can be decomposed into local rings

$$R = e_1R\oplus\cdots\oplus e_kR. \tag{7.9}$$

Given a finite commutatve ring these orthogonal idempotents and therefore the decomposition of R can be computed in PTIME.

Lemma 7.8. *Let R be finite commutative PIR and $A\in R^{m\times n}$. Then there exists a matrix equivalent to A which is diagonal and which can be computed in PTIME.*

Proof. By Lemma 7.7 we can decompose R into local rings. Since R is already finite, commutative and principal R is decomposed into Galois-Eisenstein rings e_iR. Therefore we have

$$A = A_1 + \cdots + A_k \tag{7.10}$$

where $A_i \in (e_iR)^{m\times n}$ for all $i \in \underline{k}$. By Lemma 7.4 for all $i \in \underline{k}$ there exist $S_i \in GL(m, e_iR)$ and $T_i \in GL(n, e_iR)$ such that $S_iA_iT_i =: D_i$ is diagonal. Therefore we have

$$\begin{aligned} A &= A_1 + \cdots + A_k \\ &= S_1D_1T_1 + \cdots + S_kD_kT_k \\ &= \left(\sum_{i=1}^{k} S_i\right)\left(\sum_{i=1}^{k} D_i\right)\left(\sum_{i=1}^{k} T_i\right) =: SDT. \end{aligned} \tag{7.11}$$

In 7.11 we used that if $i = j = l$ does not hold then we have

$$S_iD_jT_l = 0 \tag{7.12}$$

since $e_i \cdot e_j \cdot e_l = 0$. Therefore all mixed terms are 0.
The matrix D is obviously diagonal and S and T are invertible since

$$I = \sum_{i=1}^{k} e_iI = \sum_{i=1}^{k} S_i^{-1}S_i = \left(\sum_{i=1}^{k} S_i^{-1}\right)\left(\sum_{i=1}^{k} S_i\right) =: S^{-1}S. \tag{7.13}$$

■

Example 10. The ring $\mathbb{Z}_6$ is a PIR and according to Lemma 7.7 can be written as a direct sum via the orthogonal idempotents 4 and 3, i.e.

$$\mathbb{Z}_6 = 4\mathbb{Z}_6 \oplus 3\mathbb{Z}_6 = \{0, 2, 4\} \oplus \{0, 3\} \tag{7.14}$$

where $4\mathbb{Z}_6$ and $3\mathbb{Z}_6$ are finte chain rings. We consider the matrix $A \in \mathbb{Z}_6^{2\times 2}$ and its decomposition into the sum of $A_1 \in 4\mathbb{Z}_6^{2\times 2}$ and $A_2 \in 3\mathbb{Z}_6^{2\times 2}$:

$$A \coloneqq \begin{bmatrix} 5 & 1 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 2 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 3 \\ 0 & 3 \end{bmatrix} =: A_1 + A_2 \tag{7.15}$$

Diagonalization of A_1:

$$S_1^{-1}A_1T_1^{-1} = \begin{bmatrix} 4 & 0 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 & 4 \\ 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 4 & 4 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \tag{7.16}$$

Diagonalization of A_2:

$$S_1^{-1}A_2T_1^{-1} = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & 3 \\ 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & 3 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} \tag{7.17}$$

Finally we obtain the equivalence

$$(S_1^{-1} + S_2^{-1})A(T_1^{-1} + T_2^{-1}) = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 5 & 1 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}. \tag{7.18}$$

Lemma 7.8 allows us to proof that we can compute the McCoy rank and the inner rank of a matrix efficiently if the ring is a PIR.

Lemma 7.9. *Let R be a Galois-Eisenstein ring with nilradical $\mathcal{N}(R) = (\pi)$, q the nilpotency index of π and $D = diag(\pi^{s_1}, \ldots, \pi^{s_r}) \in R^{m\times n}$ with $r = \min(m, n)$ and $0 \leq s_1 \leq \ldots \leq s_r$. Then the McCoy rank of D is given by the number of s_i which are zero, i.e.*

$$rk_{MC}(D) = \max\{t \in \mathbb{N}_0 \mid s_t = 0\}. \tag{7.19}$$

In particular, given R and D we can compute $rk_{MC}(D)$ in PTIME.

Proof. We have $rk_{MC}(D) = t$ if and only if t is the largest number such that the anihilator of the determinal ideal of $t \times t$-submatrices of D is the zero ideal, i.e. $\text{ann}_R(I_t(D)) = (0)$. Since any ideal in R is of the form (π^i) for some $0 \leq i \leq q$ and because π is a zero divisor this is equivalent to t being the largest number such that a $t \times t$-submatrix exists which has a determinant which is not equal to π^i for some $0 < i \leq q$. Finally this is only the case if there are t units on the diagonal which is exactly our claim. ∎

Theorem 7.10. *Given a finite commutative PIR R and $A \in R^{m \times n}$ the McCoy rank of A can be computed in PTIME.*

Proof. By Lemma 7.7 we can decompose R into a direct sum of k Galois-Eisenstein rings R_i with nilradicals $\mathcal{N}(R_i) = (\pi_i)$ and nilpotency indices q_i for each π_i. We can compute diagonal matrices of the form $D_i = \text{diag}(\pi_i^{s_1}, \ldots, \pi_i^{s_r})$ with $r = \min(m, n)$ and $0 \leq s_1 \leq \ldots \leq s_r$ such that their sum is equivalent to A (see Lemma 7.8).
We claim that the McCoy rank of A is given by

$$rk_{MC}(A) = \min\{rk_{MC}(D_i) \mid i \in \underline{k}\}. \tag{7.20}$$

On the one hand $\min_{i \in \underline{k}} rk_{MC}(D_i)$ surely is a lower bound for $rk_{MC}(A)$.
Let us fix some $i \in \underline{k}$ and set $s \coloneqq rk_{MC}(D_i)$. Then there exists a non zero $a \in \text{ann}_{R_i}(I_s(D_i))$ i.e. $a \cdot \det(M) = 0$ for all $s \times s$-submatrices M of D_i. But since $a \in R_i$ we have that $aR_j = (0)$ for all $j \neq i$. Therefore all determinants of $s \times s$-submatrices of A are annihilated by a which means that $rk_{MC}(A) \leq rk_{MC}(D_i)$ for all $i \in \underline{k}$. This shows that 7.20 is correct.
The claim follows since the decomposition of R into Galois-Eisenstein rings and the computation of the McCoy rank over Galois-Eisenstein rings can both be done in PTIME (see 7.9). ∎

Theorem 7.11. *Given a finite commutative PIR R and $A \in R^{m \times n}$ the inner rank of can be computed in PTIME.*

Proof. By Lemma 7.7 we can decompose R into a direct sum of k Galois-Eisenstein rings R_i. Therefore we can write the matrix A as a sum of matrices $A_i \in R_i^{m \times n}$.

We claim that the inner rank of A is given by

$$rk_{inn}(A) = \max\{rk_{inn}(A_i) \mid i \in \underline{k}\} \tag{7.21}$$

To proof this we define s as the maximal inner rank of the A_i, i.e. $s \coloneqq \max_{i \in \underline{k}} rk_{inn}(A_i)$. We have that $rk_{inn}(A) \geq s$ due to the maximality of s. On the other hand we know that for every matrix A_i there exist matrices $B_i \in R^{m \times s}$ and $C_i \in R^{s \times n}$ such that $A_i = B_i \cdot C_i$. Therefore we have

$$A = \left(\sum_{i=1}^{k} B_i\right) \cdot \left(\sum_{i=1}^{k} C_i\right) \tag{7.22}$$

and thus $rk_{inn}(A) \leq s$.
The claim follows since the decomposition of R into Galois-Eisenstein rings and the computation of the McCoy rank over Galois-Eisenstein rings can both be done in PTIME (see 7.9). ∎

8 Conclusion

In this thesis we analyzed the properties of different notions of matrix rank over rings. We were particularly interested in their suitability for defining a rank logic. This Section summarizes the results and discusses some open questions for future research.

8.1 Summary of results

We introduced five different notions of matrix rank and defined the classes of rings on which they are well-defined. The inner rank had the largest domain (general rings) and the sign rank the most restricted domain (Galois-Eisenstein rings). In between we had the McCoy and LI-rank which were defined on commutative rings and the column/row rank which was defined over free ideal rings.

Since we were interested in unordered structures it was important that the rank notions should be invariant under permutation of rows and columns. All but the linear independence rank fulfilled this requirement. They even met the more restrictive condition to be an invariant under the equivalence relation. We also analyzed whether the rank notions were invariant under transposition. It turned out that the column and row rank as well as the linear independence rank of columns and rows can be different and are in general not related to each other.

But not all rank notions turned out to be unrelated. We could relate different rank notions by either showing that they were equal on certain classes of rings or by showing that one rank notion is an upper bound for another rank notion (see Table 2).

It was shown in [13] that the solvability of over linear equation systems over any finite field could be defined in FP+rk[12]. Hence we analyzed if the rank notions provide a criterion for the solvability of linear equation systems over rings. We saw that the Kronecker-Capelli Theorem only works for the sign rank. We could also find another necessary and sufficient condition for the solvability by using the McCoy rank but only if the linear equation system was homogeneous.

Regarding the computational complexity we found that the computation of the LI-rank is at least in EXPTIME by simply going through all combinations of columns or rows to find a maximal linear independent set. We could do better for the problem of deciding whether the McCoy rank is below some given number. We found that this problem can be decided in coNP. It seems as if these results can not be significantly improved upon as long as we do not have normal forms for the matrices which we could take advantage of. However we showed that if we restrict the class of rings to principal ideal rings we have efficient algorithms for the McCoy rank and the inner rank. The sign rank can always be efficiently computed.

Overall we can not say that we have found a canonical candidate for a rank notion for matrices over rings. The sign rank has the optimal properties regarding computational complexity and the solvability. However it is only defined on a restricted class of rings. The other rank notions do not give a criterion for the solvability of linear equation systems which was our motivation to introduce rank operators in the first place.

8.2 Future work

We know that all the ranks we defined are equal if the ring is also a field. It would be interesting to see over which classes of rings the different rank notions fall together.

Regarding the solvability of linear equation systems one could ask if there are stronger results for the Kronecker-Capelli Theorem for example by restricting the class of rings. A good review of the neccessary and sufficient conditions of linear eqution systems over rings can be found in [8].

Lastly it would be interesting if extending IFP by one particular rank notion would lead to a fundamentally more expressive logic. For example we could ask whether one rank can be defined by means of another.

[12]Here rk is any notion of matrix rank.

Rank	**Column/Row**	**Liner Indep.**	**McCoy**	**Inner**	**sign**
Inv. under equivalence	yes	no	yes	yes	yes
Inv. under transposition	no	no	yes	yes	yes
Criterion to solve LES	no	no	no	?	yes
Complexity	?	EXPTIME (see 7.2)	PTIME over PIRs (see 7.10)	PTIME over PIRs (see 7.11)	PTIME (see 7.6)

Table 1: Overview of the properties. The question mark indicates: *not known*

Rank 1	**Rank 2**	**Shared domain**	**Relation**	**Equal over**
Column rank	Row rank	free ideal rings	unrelated	two-sided Bézout domains
Column/Row rank	Inner rank	free ideal rings	$rk_{inn} \leq rk_{col/row}$ (see 5.8)	right/left Bézout domains
Inner rank	McCoy rank	commutative rings	$rk_{MC} \leq rk_{inn}$ (see 5.14)	?
Inner rank	LI rank	rings	$rk_{LI} \leq rk_{inn}$ (see 5.12)	?
Column/Row rank	McCoy rank	PID	equal	PID
Column/Row rank	LI rank	free ideal rings	?	PID (see 5.16)

Table 2: Direct comparison of rank notions. The question mark indicates: *not known*

References

[1] A. Atserias, A. Bulatov, A. Dawar *"Affine systems of equations and counting infinitary logic"*, *Theoretical Computer Science, 410:1666–1683, 2009*

[2] J. Y. Cai, M. Fürer, N. Immerman *"An optimal lower bound on the number of variables for graph identification"*, *Combinatorica, 12(4):389–410, 1992*

[3] P. Camion, L. Levy, H. Mann *"Linear Equations over a Commutative Ring"*, *Journal of Algebra 18, 1971*

[4] W. S. Ching *"Linear Equations over Commutative Rings"*, *Linear Algebra and its Applications Volume 18, Elsevier, 1977*

[5] P. M. Cohn *"Free Ideal Rings and Localization in General Rings"*, *Cambridge University Press, 2006*

[6] A. Dawar, E. Grädel, B. Holm, E. Kopczynski, W. Pakusa *"Definability of linear equation systems over groups and rings"*, *2012*

[7] A. Dawar, M. Grohe, B. Holm, B. Laubner *"Logics with rank operators"*, *Proceedings of the 23rd IEEE Symposium on Logic in Computer Science (LICS), IEEE Computer Society Press, 2009*

[8] V. P. Elizarov *"Necessary conditions for solvability of a system of linear equations over a ring"*, *Discrete Math. Appl., Vol. 14, No. 2, pp. 153–162, 2004*

[9] R. Fagin *"Languages which capture complexity classes"*, *Complexity of Computation , SIAM-AMS Proceedings, Volume 7, p. 43-73, 1974*

[10] E. Grädel, P. G. Kolaitis, L. Libkin, M. Marx, J.Spencer, M. Y. Vardi, Y. Venma, S. Weinstein *"Finite Model Theory and Its Applications"*. *Springer 2007*

[11] M. Grohe *"Fixed-point definability and polynomial time"*, *CSL'09/EACSL'09 Proceedings of the 23rd CSL international conference and 18th EACSL Annual conference on Computer science logic p. 20-23, Springer, 2009*

[12] L. Hella, P. G. Kolaitis, K. Luosto *"Almost everywhere equivalence of logics in finite model theory"*, *Bulletin of Symbolic Logic, 2:422–443, 1996*

[13] B. Holm *"Descriptive Complexity of Linear Algebra"*. *PhD thesis, 2010*

[14] T. W. Hungerford *"Algebra"*, *Springer, 1984*

[15] N. Immerman *"Generalized first-order spectra and polynomial-time recorgnizable sets"*, *Proceedings of the fifteenth annual ACM symposium on Theory of computing, p. 347–354, ACM Press, 1983*

[16] N. Immerman *"Expressibility as a complexity measure: Results and directions"*, *Second Structure in Complexity Theory Conference, p. 194–202, 1987*

[17] E. Kaltofen , G. Villard *"On The Complexity Of Computing Determinants"*, *Computational Complexity, Birkhäuser Verlag, 2004*

[18] B. R. McDonald *"Linear algebra over commutative rings"*, *Marcel Dekker, 1984*

[19] A. A. Nechaev *"Finite Rings with Applications"*, *Handbook of Algebra Vol. 5, p. 217-308, Elsevier, 2008*

[20] W. Pakusa *"Finite Model Theory with Operators from Linear Algebra"*, *Staatsarbeit, RWTH-Aachen University, 2010*

[21] S. Roman *"Advanced Linear Algebra"*, *Springer, 2005*

[22] M. Y. Vardi *"The complexity of relational query languages"*, *TOC '82: Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing, pages 137–146, ACM Press, 1982*

Eidesstattliche Erklärung

Ich versichere, dass ich die vorliegende Arbeit ohne Hilfe Dritter und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Aachen, den 9. Juli 2012