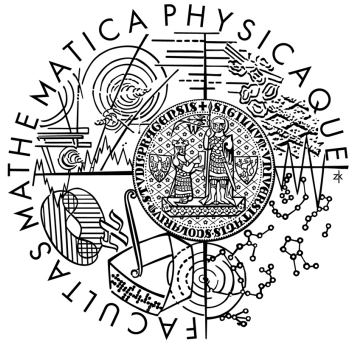
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Tomáš Kobrle

Lineární kódy nad okruhy

Katedra Algebry

Vedoucí diplomové práce: Mgr. Jan Šťovíček, PhD

Studijní program: Matemarika

Studujní obor: Matematické metody informační bezpečnosti

Praha 2012

Děkuji svému vedoucímu práce za jeho čas, trpělivost, užitečné rady při psaní a neutuchající ochotu mi pomoci zdárně práci dokončit.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Tomáš Kobrle

Název práce: Lineární Kódy nad Okruhy

Autor: Tomáš Kobrle

Katedra: Katedra Algebry

Vedoucí diplomové práce: Mgr. Jan Šťovíček, PhD, katedra algebry

Abstrakt: Tato diplomová práce se zaměřuje na speciální typ okruhů nazývaný algebry cest s cílem definovat a popsat lineární kódy nad těmito okruhy. Algebra cest je definována pomocí grafické struktury tak zvaných quiverů, jejich struktura se pak dále přenáší i na moduly algeber cest. Samotné kódy jsou definovány nad nerozložitelnými injektivními moduly algeber cest s ohledem na nedávné výsledky z teorie kódů nad okruhy. Takto definované kódy nám umožňují studovat parametry a verze základních tvrzení z teorie lineárních kódů na tělesy pro kódy nad okruhy. Zmíněná tvrzení se týkají duálních kódů a s nimi spjatou MacWilliams identitou následovaný tvrzením o ekvivalenci kódů. Nakonec se vracíme k algebrám cest s popisem způsobu, jak je lze udělat použitelné v teorii kódů nad okruhy. Klíčová slova: lineární kód, algebra cest, quiver.

Title: Linear Codes over Rings

Author: Tomáš Kobrle Department: Algebra

Supervisor: Mgr. Jan Šťovíček, PhD, Department of Algebra

Abstract: This master thesis focus on special type of rings called path algebras with a goal to define and describe codes over these rings. The path algebras are defined by graphic structures called quivers which is transferred also on the modules of the path algebra. Codes themselves are defined over indecomposible injective modules of path algebra considering the latest result in ring-coding theory. So defined codes allow us to study the parameters and the versions of elementary theorems from theory of linear codes over fields for codes over rings. These are about duals codes especially, the MacWilliams identity theorem and about code equivalency. Finally we get back to path algebras and describe a way to make them applicable in theory of codes over rings. Keywords: linear codes, path algebra, quiver.

Contents

Introduction

A first task of cryptology was to encrypt important messages and hide their contents from enemies or rivals. In the past encrypted messages were sent in a paper-form. In the last century with an arrival of radio-waves and internet we started to send messages in electronic-form. But there was a problem in unexpected errors because cryptographic protocols and techniques are often designed under the assumption that the communication channels are error-free. This makes an encryption very difficult sometimes even useless because even a single mistake in a cipher text causes that the decoded message can be completely different from the original message. So we found the theory of error-correcting codes which gives us instruments for correcting the unexpected errors in communication channels with the cost of enlarging the messages. Naturally we want to keep messages as short as possible but on the other hand more redundant bits added to message will allow us to correct more errors. Finding a compromise between these aspects of sending messages is the main goal of theory of error-correcting codes.

The classical theory of error-correcting codes studies codes over finite fields. The oldest class of these codes are linear codes which have a structure of vector space over a field that gives them many useful properties which we will discuss in Chapter 1. Apart from linear binary codes there exist non-linear binary codes, for example Kerdock and Preparata codes. Later it has been proven that there exists no linear code which has more codewords with fixed code length than Kerdock or Preparata codes. However it has been shown that these codes can be seen as linear codes over $\mathbb{Z}_4$. Even later, application of coding theory to quantum computer requires to use of other codes over $\mathbb{Z}_4$ and $\mathbb{Z}_8$.

It became clear that the coding theory should consider studying codes over rings as well as over fields. In second section of Chapter 1 we will show some findings in the theory of linear codes over rings, mainly we will describe advantages of Frobenius rings in coding theory. In Chapter 2 we will define graphic structures called quivers and show how we can construct path algebras over these quivers. The reason of studying these algebras is discussed as well. Since linear codes over rings are modules we study modules over path algebras in Chapter 3 and then we focus on the aspects of the codes, like what alphabet we will use, the bilinear form and the weight function we employ and so on. All these tools are described in Chapter 4. Then we focus on parameters of these codes, especially on the number of codewords, in Chapter 5 and then we will prove variations of important theorems from theory of linear codes over fields in Chapters 6 and 7, applied to codes defined in this thesis. In the end we will mention when a path algebra has structure of Frobenius ring and what this fact gives us in Chapter 8.

1. Error-correcting codes

A trivial way to ensure that a receiver will get a correct message is to send the message more than once. For example we can send a message by bits, so we keep sending one bit several times until we are sure that the receiver will choose the right one. By phrase choose the right one we mean taking a logical majority of received bits. Simply we take the bit which is obtained the most times. Then if we sent a bit k^{th} times then receiver will obtain a correct bit when there were less than $\lfloor k/2 \rfloor$ mistakes in the transmission. This method is called a repetition code but it is very naive solution to the problem because extension of messages is enormous.

The theory of error-correcting codes tries to find a compromise between enlarging message and ensuring the reception of a correct message. The repetition code is one of so called trivial codes, another trivial code is sending a message with no change so that the length of message stays the same but a receiver cannot detect or correct any errors.

The first non-trivial error-correcting code was invented in 1950 by Richard Hamming. Now we call this code $\mathcal{H}_3$ according to a definition of Hamming codes. This code is a linear code over binary field and we will discuss about his parameters and meaning of the number 3 later. This is only example.

In the application of the $\mathcal{H}_3$ code we divide a message into blocks of length 4 and each block we map to a set of codewords of length 7. After obtaining a codeword the receiver can correctly decode it to the correct massage if there was less than two errors in the transmission. The enlargement rate of message is $\frac{7}{4}$ instead of 3 if we had used the repetition code to correct one error.

There are many parameters of codes which determine their properties. We mentioned the length of a code. There are codes with the variable length but since we will focus on the linear codes we simply define the length as a length of a codeword which is the same for all codewords. The length of code is denoted by $\mathbf{n}$.

A related parameter of the length is the code rate which determines how many sent bits are useful, it is a reciprocal of parameter which we called the enlargement rate of message. The parameter code rate depends also on a number of codewords, for example let $\mathcal{C}$ be a code over alphabet A of length $\mathbf{n}$ and let us denote $\mathbf{k} = \log_{|A|} |C|$ then rate of code is $\frac{\mathbf{k}}{\mathbf{n}}$.

Another important parameter we mentioned is how many errors the code can correct. This value is hidden in a parameter called the minimum Hamming distance of a code which determines a minimum of number of differences between two codewords over all pairs of codewords. The minimum Hamming distance of code is denoted by $\mathbf{d}$. The code with the minimum distance $\mathbf{d}$ can correct up to $\left\lfloor \frac{\mathbf{d}-1}{2} \right\rfloor$ errors. This is because of we use the decoding to the nearest codeword.

Remark 1.1. *If* $\mathbf{n} = \mathbf{d}$ *then the code is repetition code and if* $\mathbf{d} = 1$ *the code is trivial.*

1.1 Linear codes over fields

We want to study linear codes over finite rings but we would like to ensure that such codes will have some useful properties and that the important theorems from the theory of linear codes over fields will hold. Since we will now focus on linear codes over fields, note the definition and importance of the dual code, MacWilliams identity and extension theorem.

For now $\mathbb{F}_q$ will denote finite field $GF(q)$, where $q = p^e$ of some prime p and $e \in \mathbb{N}$.

Linear codes over field $\mathbb{F}_q$ have a structure of vector space over $\mathbb{F}_q$. It means that the sum of two codewords is a codeword as well. Generally every $\mathbb{F}_q-$linear combination of codewords over field is a codeword as well. Hence we can find a basis of the code and construct a generating matrix with elements of basis in rows. We can now use a term dimension of the code instead of the number of codewords of a code. The dimension of a code is defined intuitively as the dimension of the vector space which is equal to the number of elements of a basis and a rank of the generating matrix.

For linear codes we use the notation of parameters of code $[\mathbf{n}, \mathbf{k}, \mathbf{d}]_q$, where $\mathbf{k}$ is the dimension of a code, $\mathbf{n}$ is the length of a code and $\mathbf{d}$ is the minimum distance of code.

Remark 1.2. *Let $\mathcal{C}$ be an $[\mathbf{n}, \mathbf{k}, \mathbf{d}]_q$-code and A be a generating $\mathbf{n} \times \mathbf{k}$ matrix of code $\mathcal{C}$ then*

$$\mathcal{C} = \left\{ Ax \mid x \in \mathbb{F}_q^{\mathbf{k}} \right\}.$$

Since a linear code $\mathcal{C}$ is a vector subspace of $\mathbb{F}_q^n$ we can take an orthogonal complement of $\mathcal{C}$ and we denote it $\mathcal{C}^\perp$.

Definition 1.3 (Dual Code)**.** *For a linear code $\mathcal{C}$ over $\mathbb{F}_q$ we define the code $\mathcal{C}^\perp$ by*

$$\mathcal{C}^\perp = \left\{ x \in \mathbb{F}_q^{\mathbf{n}} \mid \langle c, x \rangle = 0 \ \forall \ c \in \mathcal{C} \right\},$$

where $\langle ., . \rangle$ is the inner product over $\mathbb{F}_q^{\mathbf{n}}$. The code $\mathcal{C}^\perp$ is called dual code to the code $\mathcal{C}$.

Since the orthogonal complement $\mathcal{C}^\perp$ is also a $\mathbb{F}_q-$vector space as well, it can be seen as a code over $\mathbb{F}_q$. The dimension of a code, dual to the code $\mathcal{C}$ with parameters $[\mathbf{n}, \mathbf{k}, \mathbf{d}]$, is $\mathbf{n} - \mathbf{k}$ and its length is $\mathbf{n}$ as well. A generating matrix of a dual code $\mathcal{C}^\perp$ is called a parity-check matrix of code $\mathcal{C}$. Important property of duality of the codes over finite fields is $\mathcal{C} = \left(\mathcal{C}^\perp\right)^\perp$ for any code $\mathcal{C}$.

Definition 1.4 (Closed Code)**.** *We call a code $\mathcal{C}$ closed if $\mathcal{C} = \mathcal{C}^{\perp\perp} = \left(\mathcal{C}^\perp\right)^\perp$.*

Now we can return to the first error-correcting code - the Hamming code $\mathcal{H}_3$. The parameters of Hamming code $\mathcal{H}_r$ for $r \geq 3$ are $[2^r - 1, 2^r - r - 1, r]$, hence the code $\mathcal{H}_3$ has parameters $[7, 4, 3]$. The generating matrix of $\mathcal{H}_3$ is

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

and parity-check matrix is

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

These matrices are determined uniquely up to the permutation and linear combinations of rows. The permutation of columns of matrix M gives us only a code which is equivalent to $\mathcal{H}_3$ which will be seen as a consequence of the MacWilliams Equivalence.

For a better look on a structure of a code, especially some relations between the codewords, we define a weight function for codes. An elementary example of weight function, named again after Richard Hamming, is called the Hamming weight.

Definition 1.5. *A function* $\mathbf{w}_{\mathcal{H}} : \mathbb{F}_q \to \mathbb{Z}$ *defined by the following prescription*

$$\mathbf{w}_{\mathcal{H}}(r) = \begin{cases} 0, & \textit{for } r = 0 \\ 1, & \textit{else.} \end{cases}$$

is called the Hamming weight.

Then the Hamming weight of a codeword is the sum of weights of its coordinates

$$\omega_{\mathcal{H}}(c) = \sum_{i=1}^{\mathbf{n}} \mathbf{w}_h(c_i).$$

Hence the Hamming weight of the codeword is number of nonzero symbols in the codeword. In the theory of codes over fields the Hamming weight is the most used weight function.

The linearity of a code give us easier way to compute a minimal distance of the code because subtraction of two codewords is codeword as well and from definition of Hamming weight of codeword it holds $d(x, y) = d(x - y, 0) = \omega_{\mathcal{H}}(x - y)$, where function d is the Hamming distance which gives us the number of coordinates at which the arguments are different. Hence $\mathbf{d}$ is equal to the Hamming weight of the nonzero codeword with the smallest weight. There is also classical result about minimal distance of the code $\mathcal{C}$.

Theorem 1.6. *Let* $\mathcal{C}$ *be a linear code over* $\mathbb{F}_q$ *and* M *be its parity-check matrix. Let* $m \in \mathbb{N}$ *be a maximal number such that every* m *columns of* M *are linearly independent over* $\mathbb{F}_q$*. Then minimal distance of the code* $\mathcal{C}$ *is* $m + 1$*.*

Based on Hamming weight we can define Hamming weight enumerator polynomial of a code $\mathcal{C}$

$$\mathrm{hwe}_{\mathcal{C}}(x) = \sum_{c \in \mathcal{C}} x^{\mathbf{n}-\omega_{\mathcal{H}}(c)} = \sum_{i=0}^{\mathbf{n}} A_i x^{\mathbf{n}-i},$$

where $\mathbf{n}$ is the length of a code $\mathcal{C}$ and A_i is the number of codewords with Hamming weight equal to i.

More general polynomial for codes is called complete weight enumerator of a code $\mathcal{C}$. It is a polynomial in q indeterminates, where q is a number of elements of a field $\mathbb{F}_q$ and it is defined by

$$\mathrm{cwe}_{\mathcal{C}}(\underline{x}) = \sum_{c \in \mathcal{C}} \prod_{a \in \mathbb{F}_q} x_v^{wt_a(c)},$$

where $wt_a(c) = |\{i \in \{1, \ldots, \mathbf{n}\} \mid c_i = a\}|$.

The Hamming weight enumerator can be easily obtained from complete weight enumerator.

Remark 1.7.

$$\mathrm{hwe}_{\mathcal{C}}(x) = \mathrm{cwe}_{\mathcal{C}}(x, 1, \ldots, 1)$$

if the first indeterminate of cwe *corresponds to* $0 \in \mathbb{F}_q$.

If we return to our example of the linear code $\mathcal{H}_3$ then

$$\mathrm{hwe}_{\mathcal{H}_3}(x) = x^7 + 7x^4 + 7x^3 + 1.$$

and

$$\mathrm{cwe}_{\mathcal{H}_3}(x, y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7.$$

Interesting result on weight enumerators of code $\mathcal{C}$ and his dual code $\mathcal{C}^\perp$ is known as MacWilliams identity taken from [7], which gets name after Jessie MacWilliams.

Theorem 1.8. *Let $\mathbb{F}_q$ be the finite field of q elements, and let $\mathcal{C} \leq \mathbb{F}_q^{\mathbf{n}}$ be a linear code with Hamming weight enumerator* $\mathrm{hwe}_{\mathcal{C}}(x, y)$. *Then the Hamming weight enumerator of $\mathcal{C}^\perp$ is given by*

$$\mathrm{hwe}_{\mathcal{C}^\perp}(x) = \frac{1}{|\mathcal{C}|} \left[1 + (q-1)x\right]^{\mathbf{n}} \mathrm{hwe}_{\mathcal{C}} \left(\frac{1-x}{1+(q-1)x} \right).$$

Since any linear code over $\mathbb{F}_q$ is closed, it should hold

$$\mathrm{hwe}_{\mathcal{C}}(x) = \mathrm{hwe}_{\mathcal{C}^{\perp\perp}}(x) = \frac{1}{|\mathcal{C}|} \left[1 + (q-1)x\right]^{\mathbf{n}} \mathrm{hwe}_{\mathcal{C}^\perp} \left(\frac{1-x}{1+(q-1)x} \right).$$

This is reason why we would like to have closed codes over rings as well.

Another important theorem about linear codes over fields is named also after J. MacWilliams. This theorem gives us a condition under which two codes are

equivalent. First we need to define when two codes are equivalent. A monomial transformation of $\mathbb{F}_q^n$ is a $\mathbb{F}_q-$linear homomorphism $f : \mathbb{F}_q^{\mathbf{n}} \to \mathbb{F}_q^{\mathbf{n}}$ of the form

$$f(x_1, \ldots, x_{\mathbf{n}}) = \left(u_1 x_{\sigma(1)}, \ldots, u_{\mathbf{n}} x_{\sigma(\mathbf{n})}\right),$$

where σ is permutation of $\{1, \ldots, \mathbf{n}\}$ and $u_1, \ldots, u_{\mathbf{n}}$ are nonzero elements of $\mathbb{F}_q$. Or equivalently

$$f(\mathbf{x}) = \mathbf{x}PD,$$

for $\mathbf{x}$ from $\mathbb{F}_q^{\mathbf{n}}$, where P is a coordinate permutation matrix and D is an invertible diagonal matrix in $M_{\mathbf{n}}(\mathbb{F}_q)$.

Definition 1.9. *Two linear codes $\mathcal{C}, \mathcal{C}'$ in $\mathbb{F}_q^{\mathbf{n}}$ are equivalent, when there exists a monomial transformation $\varphi : \mathbb{F}_q^{\mathbf{n}} \to \mathbb{F}_q^{\mathbf{n}}$ taking $\mathcal{C}$ to $\mathcal{C}'$, $\varphi(\mathcal{C}) = \mathcal{C}'$.*

Since an inverse and even a composition of monomial transformations are also monomial transformations, this equivalence is equivalence relation on linear codes over $\mathbb{F}_q^{\mathbf{n}}$.

The first version of MacWilliams theorem gives us exact condition for the equivalence of two codes. It is taken from [14].

Theorem 1.10 (MacWilliams equivalence theorem)**.** *Two linear codes $\mathcal{C}, \mathcal{C}'$ in $\mathbb{F}_q^{\mathbf{n}}$ are equivalent if and only if there is a $\mathbb{F}_q-$linear isomorphism $f : \mathcal{C} \to \mathcal{C}'$ preserving the Hamming weight, $\omega_{\mathcal{H}}(f(c)) = \omega(c)$ for all $c \in \mathcal{C}$.*

It is easy to see that any monomial transformation preserves the Hamming weight so the "only if" part of theorem is clear. The second portion of the theorem can be proven by second version MacWilliams equivalence theorem. The number of versions of MacWilliams theorems are only illustrational, it depends on a publication which of the version is called MacWilliams equivalence theorem. We need to mention another important mapping to state the theorem.

Definition 1.11. *An $\mathbb{F}_q-$linear map preserving the Hamming weight is called the Hamming isometry.*

Now we can formulate the theorem, which is taken from [7, p.226].

Theorem 1.12 (MacWilliams equivalence theorem)**.** *If $\mathbb{F}_q$ is a finite field and $\mathcal{C} \leq \mathbb{F}_q^{\mathbf{n}}$ a linear code, then every Hamming isometry $\mathcal{C} \to \mathbb{F}_q^{\mathbf{n}}$ can be extended to a monomial transformation of $\mathbb{F}_q^{\mathbf{n}}$.*

1.2 Linear codes over rings

As a linear code over a finite field has the structure of a vector space, a linear code over a finite ring R is right (or left) submodule of V^n, where V is some suitable right (left) module of R. We will assume right modules in this section and in the rest of thesis. We want to define linear codes over ring but we still want them to have some properties as linear codes over fields. The good properties are definitely the ones which are the subjects of MacWilliams theorems, conditions of equivalence of codes and MacWilliams identity. The importance of the first one is obvious, the second one will help us better see the dual codes.

We start with a general ring R and we will denote right modules over R as V_R. To define a dual code we need to generalize the inner product which is used in coding theory over fields. The main reason is that an arbitrary ring is not necessarily commutative and integer domain. We will start with a general bilinear form as defined in [9, p.84] and later we restrict to a useful algebraic structure.

Definition 1.13 ($\mathcal{A}$-valued Bilinear Form)**.** *Let R, S be rings, V is a right $R-$module , W is a right $S-$module and A is a right $R \otimes S-$module. Then an $\mathcal{A}-$valued bilinear form on $V \otimes W$ is an $R \otimes S-$homomorphism*

$$\beta : \ V_R \otimes_{\mathbb{Z}} W_S \longrightarrow \mathcal{A}_{R \otimes S}.$$

In the following, we omit the $\otimes$ and write simply (x, y).

Definition 1.14. *An $\mathcal{A}-$valued bilinear form $\beta : V \times W \to A$ is left non-singular if the induced homomorphism $V \to \mathrm{Hom}_S(W, \mathcal{A})$ is an isomorphism. Similarly, β is right non-singular if the induced homomorphism $W \to \mathrm{Hom}_R(V, \mathcal{A})$ is an isomorphism. If β is left and right non-singular it is said to be non-singular, otherwise it is called singular.*

In the words of the previous definitions we can define a term of dual group with respect to β. For C subgroup of V we define dual subgroup by

$$C^{\perp} = \{x \in W \mid \beta(c, x) = 0 \ \forall \ c \in C\}$$

and similarly for subgroup D of W

$$D^{\perp} = \{y \in V \mid \beta(y, d) = 0 \ \forall \ d \in D\}.$$

There is a simple lemma about relations of subgroup of V, W and their duals.

Lemma 1.15. *Let C be a subgroup of V and let D be subgroup of W. If $C \subset D^{\perp}$ then $D \subset C^{\perp}$.*

Proof. Let d be an element of D, then for every $x \in D^{\perp}$ is $\beta(x, d) = 0$. Since $C \subset D^{\perp}$, for every $c \in C$ is $\beta(c, d) = 0$. According to definition, this gives us, that d belongs to $C^{\perp}$. So $D \subset C^{\perp}$.

□

For subgroup C of V we define the code generated by C to be CR, the smallest submodule of V containing C. Similarly for D, we define DS the smallest submodule of W containing D.

Lemma 1.16. *Let C be a subgroup of V_R, CR the code generated by C and β the $\mathcal{A}-$valued bilinear form defined in 1.13, then $C^{\perp} = (CR)^{\perp}$.*

Proof. Directly from the previous lemma we get that $(CR)^{\perp} \subset C^{\perp}$, since $C \subset CR$. Now let d be an element of $C^{\perp}$ then for every $c \in C$ is $\beta(c, d) = 0$. Since $\mathcal{A}$ is $R\otimes$ module, we know that for every $r \in R$ $0 = 0(r, 0) = \beta(c, d)(r, 0) = \beta(c, d)$. We get that for every $r \in R$ and for every $c \in C$ $\beta(cr, d) = 0$, hence $c \in (CR)^{\perp}$. This gives that $C^{\perp} \subset (CR)^{\perp}$. Putting it together with the previous result we get equality of $C^{\perp}$ and $(CR)^{\perp}$. □

For any subgroup $C \subset V$, it is easy to see that the dual subgroup $C^{\perp}$ is a submodule of W which means that it is also a code. The previous lemma gives that the code $C^{\perp}$ can be called dual to CR. So if $\mathcal{C}$ is a code then $\mathcal{C}^{\perp}$ is its dual code.

Now we get the dual codes but we want to be sure that these codes are closed which means $\mathcal{C} = \left(\mathcal{C}^{\perp}\right)^{\perp}$ as we mention in the previous section. To get closed codes over rings we need to restrict on certain classes of rings and suitable bilinear forms. For any ring R there is a certain injective $R-$module called minimal injective cogenerator.

Definition 1.17. *Let R be a ring.*

- *A module M_R is cogenerated by a module N if there exists a monomorphism $N \to M^A$, for some set A.*
- *A module I_R is injective if for all $R-$modules M_R, N_R, for any injective homomorphism $f : M \to N$ and any homomorphism $g : M \to I$ there exists a homomorphism $h : N \to I$ such that $g = hf$.*
- *The injective cogenerator Q is minimal if for each injective cogenerator Q' there exists a monomorphism $Q \to Q'$.*

In general, a ring need not to have a minimal injective cogenerator, for more about injective cogenerators see [1]. For example $\mathcal{U}(\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$ and for a field $\mathcal{K}$ $\mathcal{U}(\mathcal{K}) \cong \mathcal{K}$. From [9, p.88] we obtain that for a ring R and a non-singular bilinear form $\beta : V_R \otimes W_R$ which takes values in $\mathcal{U}(R)$, all codes over ring R are closed.

Important class of rings are quasi-Frobenius and Frobenius ring. Before defining the terms we will mention two important terms of the ring theory. The first one - the Jacobson radical of a ring R, denoted $\operatorname{rad} R$, is defined as intersection of all maximal ideals of R. As a dual term to the radical is the socle which is defined for a module M_R as the sum of all minimal submodules of M. The duality of the terms comes from the following fact for an Artinian ring R from [5]

$$\operatorname{soc}(M_R) = \{m \in M \mid m \operatorname{rad} R = 0\}.$$

Definition 1.18 (Frobenius Ring)**.** *A ring R is quasi-Frobenius if R is Artinian and self-injective, which means that R as an $R-$module is injective over R.*

A ring R is Frobenius if R is quasi-Frobenius and $\operatorname{soc}(R_R) \cong R/\operatorname{rad} R$ as right $R-$modules.

There are many other equivalent definitions but for us it is important their main property, the self-injectiveness. With using results from [9, p.89], for R a commutative Quasi-Frobenius ring and β which takes values from R all codes over R is closed with respect to β. Quasi-Frobenius rings are the largest class of rings having this property.

From [7, p.228] we get the following lemmas, which confirm that codes over Frobenius rings are the most appropriate rings for coding theory. First lemma is analogy of MacWilliams theorem for rings, followed by similar lemma for complete weight enumerator.

Lemma 1.19. *Let R be a finite Frobenius ring and let $\mathcal{C} \leq R^{\mathbf{n}}$ be a linear code with Hamming weight enumerator* $\mathrm{hwe}_{\mathcal{C}}(x)$. *Then the complete weight enumerator of $\mathcal{C}^{\perp}$ is given as*

$$\mathrm{hwe}_{\mathcal{C}^{\perp}}(x) = \frac{1}{|\mathcal{C}|}\left[1 + (|R| - 1)x\right]^{\mathbf{n}} \mathrm{hwe}_{\mathcal{C}}\left(\frac{1-x}{1+(|R|-1)x}\right).$$

Lemma 1.20. *Let R be a finite Frobenius ring and let $\mathcal{C} \leq R^{\mathbf{n}}$ be a linear code with complete weight enumerator* $\mathrm{cwe}_{\mathcal{C}}(\mathbf{x})$. *Then the complete weight enumerator of $\mathcal{C}^{\perp}$ is given as*

$$\mathrm{cwe}_{\mathcal{C}^{\perp}}(\mathbf{x}) = \frac{1}{|\mathcal{C}|}\,\mathrm{cwe}_{\mathcal{C}}(M\mathbf{x})$$

where M is the matrix with entry $M_{i,j} = \chi(ij)$ and χ is a generating character of R.

For proofs of both lemmas see [15]. We denote $\widehat{R}$ the set of characters of R, $\widehat{R} = \mathrm{Hom}\,(R, (C, *))$, where $(C, *)$ denotes a group of the complex characters. The element χ is called a right generating character if $\chi \cdot R = \widehat{R}$. The character which is left and right generating is called a generating character. From [5, p.255] we get the following lemma.

Lemma 1.21. *For a finite ring R every left (or right) generating character is generating. Moreover R is Frobenius if and only if R has generating character χ.*

More important is the theorem about equivalence of codes which is a generalization of the MacWilliams equivalence theorem. We say that two linear codes $\mathcal{C}, \mathcal{C}' \subset R^{\mathbf{n}}$ are equivalent if there exists a monomial transformation $f : R^{\mathbf{n}} \to R^{\mathbf{n}}$ with $f(\mathcal{C}) = \mathcal{C}'$, where the monomial transformation of $R^{\mathbf{n}}$ is an $R-$linear homomorphism $f : R^{\mathbf{n}} \to R^{\mathbf{n}}$ of the form

$$f(x_1, \ldots, x_{\mathbf{n}}) = \left(u_1 x_{\sigma(1)}, \ldots, u_{\mathbf{n}} x_{\sigma(\mathbf{n})}\right),$$

where σ is a permutation of $\{1, \ldots, \mathbf{n}\}$ and u_i are units of R.

Definition 1.22. *A ring R has extension property for Hamming weight if for any linear code $\mathcal{C} \leq R^{\mathbf{n}}$ and any $R-$linear homomorphism $f : \mathcal{C} \to R^{\mathbf{n}}$ preserving the Hamming weight, f can be extended to a monomial transformation $f : R^{\mathbf{n}} \to R^{\mathbf{n}}$.*

Theorem 1.23. *Every finite Frobenius ring has the extension property for Hamming weight.*

This comes from work of Jay A. Wood who studied Frobenius ring and their applications. In [13] he made a proof of this and the converse of the previous theorem.

Theorem 1.24. *Every finite ring, that has extension property for Hamming weight, is Frobenius.*

However Hamming weight is not the only weight used in coding theory. Generally the question whether also other weight functions on finite Frobenius rings lead to results like MacWilliams equivalence theorem, has not been answered. But in [7, p.227] we can find at least one result for a homogeneous weight. We will define and use homogeneous weight in Chapter 4.

Theorem 1.25. *If R is a finite Frobenius ring and $\mathcal{C} \leq R^{\mathbf{n}}$ a linear code, then every homogeneous isometry (homomorphism preserving homogeneous weight) $\mathcal{C} \to R^{\mathbf{n}}$ can be extended to a monomial transformation of $R^{\mathbf{n}}$.*

Based on the results of this chapter we would like to define codes over Frobenius rings to have an opportunity to compare their properties with the properties of linear codes over fields.

2. Quivers and Path Algebras

In this chapter we introduce a class of rings which we will use to construct codes over them. They are called path algebras. From second chapter of [8] we get that every finite dimensional algebra over an algebraically closed field corresponds to a graphic structure, called a quiver. Conversely to every quiver we can construct a finite dimensional $\mathcal{K}-$algebra with identity. This view of $\mathcal{K}-$algebras through quivers gives us an option to visualize a finitely generated modules over $\mathcal{K}-$algebra as a set of vector spaces connected with $\mathcal{K}-$linear maps.

2.1 Quivers

We start with definition of the graphic structures - quivers.

Definition 2.1. *A quiver $\mathcal{Q} = (Q_0, Q_1, \mathbf{s}, \mathbf{t})$ consists of two sets Q_0, Q_1 and two maps, $\mathbf{s}$ and $\mathbf{t}$.*

- *Elements of set Q_0 are called points.*
- *Elements of set Q_1 are called arrows.*
- *Maps $\mathbf{s}, \mathbf{t} : Q_1 \to Q_0$ associate an arrow α with its source $\mathbf{s}(\alpha)$ and its target $\mathbf{t}(\alpha)$.*

Instead of writing an arrow $\alpha \in Q_1$ with a source $a = \mathbf{s}(\alpha)$ and a target $b = \mathbf{t}(\alpha)$ we will use a notation $\alpha : a \to b$. It allows us to write the quiver (Q_0, Q_1, s, t) just as (Q_0, Q_1) or even simplier $\mathcal{Q}$.

In fact a quiver is an oriented graph without any restriction on number of arrows between two points or number of loops of any point. By the underlying graph $\underline{\mathcal{Q}}$ of quiver we mean a graph obtained from quiver by ignoring the orientation of the arrows. The opposite quiver $\mathcal{Q}^{op}$ is obtained from $\mathcal{Q}$ by changing the orientation of all arrows.

A quiver $\mathcal{Q}$ is connected if $\underline{\mathcal{Q}}$ is a connected graph. In this thesis we assume that every quiver is connected. If Q_0 and Q_1 are finite sets we call quiver $\mathcal{Q}$ finite.

Definition 2.2. *Let $\mathcal{Q} = (Q_0, Q_1, s, t)$ be a quiver and $a, b \in Q_0$. A path of length $l \geq 1$ with source a and target b is a sequence*

$$(a|\alpha_1 \dots \alpha_l|b),$$

where $\alpha_i \in Q_1$ for all $1 \leq i \leq l$ and $a = \mathbf{s}(\alpha_1)$, $(\alpha_{\mathtt{i}}) = \mathbf{s}(\alpha_{\mathtt{i+1}})$ for all $1 \leq i < l$ and $(\alpha_{\mathtt{1}}) = \mathtt{b}$.

We denote Q_l as a set of all paths of length l in $\mathcal{Q}$. We also associate each point $a \in Q_0$ with a path of length 0 and denote it by

$$\epsilon_a = (a||a).$$

The paths ϵ_a are called stationary paths.

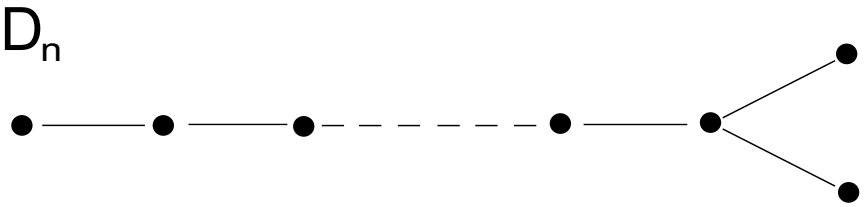
A path of length $l \geq 1$ is called a cycle if its source and target are the same and a cycle of length 1 is called a loop. A quiver is acyclic if it does not contain any cycle.

Remark 2.3. *Let $\mathcal{Q}$ be a finite acyclic quiver. Then there is only a finite number of paths in $\mathcal{Q}$.*

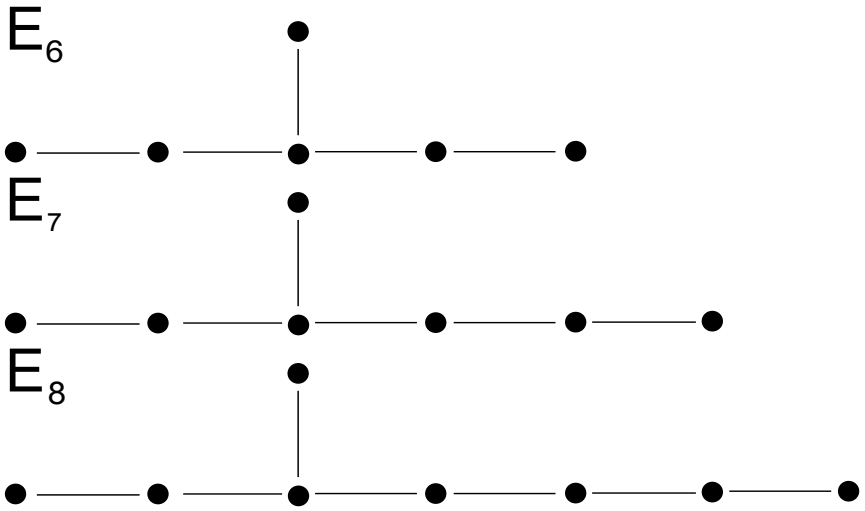
Special cases of quiver are quivers whose underlying graph is so called Dynkin diagrams. For us only the Dynkin diagrams of types A, D, E are interesting. These types is often denoted as ADE Dynkin diagrams.

Definition 2.4. *The Dynkin diagram A_n, where n is number of points*

Dynkin diagram D_n:



and finally E_6, E_7, E_8:



The Dynkin diagram A_n with oriented edges from left to right is one of the simplest quiver and so we will use them in examples, but very often we will give a lead to generalization of situation. Since we will use notation quiver A_n we will mean the quiver whose underlying graph is the Dynkin diagram A_n with arrow oriented from left to right.

At the end we mention an interesting theorem which says that Dynkin diagrams are not only a special case of quivers, they have an important property, which is mentioned in definition below.

Definition 2.5. *A quiver is of finite type if it has only finitely many isomorphism classes of indecomposable representations.*

Theorem 2.6 (Gabriel's Theorem)**.** *A quiver is of finite type if and only if its underlying graph is one of the ADE Dynkin Diagrams.*

The proof of this theorem can be found in [3, p.288-294].

2.2 Path Algebra

Now we use notation of quivers to define path algebras.

Definition 2.7. *Let $\mathcal{Q}$ a be quiver. The path algebra $\mathcal{K}\mathcal{Q}$ is the $\mathcal{K}-$algebra whose underlying vector space has as its set of basic vectors all paths of length $l \geq 0$ in $\mathcal{Q}$ and multiplication defined on two basic vectors $(a|\alpha_1 \dots \alpha_l|b)$ and $(c|\beta_1 \dots \beta_k|d)$, as*

$$(a|\alpha_1 \dots \alpha_l|b)(c|\beta_1 \dots \beta_k|d) = \delta_{bc}(a|\alpha_1 \dots \alpha_l\beta_1 \dots \beta_k|d),$$

where δ_{bc} is the Kronecker delta which is function

$$\delta_{bc}(x) = \begin{cases} x, & \text{for } b = c \\ 0, & \text{for } b \neq c. \end{cases}$$

Since path algebras have a structure of vector spaces with multiplication we can view them as non-commutative rings.

Definition 2.8. *Let A be a $\mathcal{K}-$algebra. The opposite algebra A^{op} of A is a algebra whose underlying set and a vector space structure are identical with A, but the multiplication is defined by*

$$a \cdot b = ba.$$

Lemma 2.9. *Let $\mathcal{Q}$ be quiver. Then $\mathcal{K}\mathcal{Q}^{op} \cong (\mathcal{K}\mathcal{Q})^{op}$.*

Proof. There is a natural bijective map between arrows of $\mathcal{Q}$ and $\mathcal{Q}^{op}$ which assigns to each arrow from $\mathcal{Q}$ the same arrow in $\mathcal{Q}^{op}$ with an opposite orientation. We can extend this map to the map between paths in $\mathcal{Q}$ and $\mathcal{Q}^{op}$ so we have the bijective map between elements of bases of $\mathcal{K}\mathcal{Q}^{op}$ and $(\mathcal{K}\mathcal{Q})^{op}$. Extending this map by linear combination of basis elements we get the isomorphism between underlying vector spaces of $\mathcal{K}\mathcal{Q}^{op}$ and $(\mathcal{K}\mathcal{Q})^{op}$.

To prove that this natural isomorphism is compatible with the multiplication defined for path algebras it will be sufficient to prove this for two paths or even just for two arrows from basis $(\mathcal{K}\mathcal{Q})^{op}$. Let α, β be arrows in $\mathcal{Q}$. Then $\alpha \cdot_{(\mathcal{K}\mathcal{Q})^{op}} \beta = \beta \cdot_{\mathcal{K}\mathcal{Q}} \alpha$ by definition of opposite algebra. In $\mathcal{Q}^{op}$ there are images of α and β by natural bijective map, let us denote them α^{op} and β^{op} then $\alpha^{op} \cdot_{\mathcal{K}\mathcal{Q}^{op}} \beta^{op} = (\beta \cdot_{\mathcal{K}\mathcal{Q}} \alpha)^{op}$.

Hence the isomorphism constructed by natural map between arrows $\mathcal{Q}$ and $\mathcal{Q}^{op}$ is a isomorphism between $\mathcal{K}\mathcal{Q}^{op}$ and $(\mathcal{K}\mathcal{Q})^{op}$.

□

A $\mathcal{K}-$algebra is finitely generated if the dimension of underlying vector space over $\mathcal{K}$ is finite. From the Lemma 2.3 and Definition 2.7 we easily get the following statement.

Remark 2.10. *Let $\mathcal{Q}$ be a quiver. $\mathcal{K}\mathcal{Q}$ is finite dimensional if and only if $\mathcal{Q}$ is finite and acyclic.*

An important role in studying path algebras is played by elements called idempotents. Idempotents will help us study decompositions of path algebras and their modules.

Definition 2.11. *Let $\mathcal{K}\mathcal{Q}$ be a path algebra.*

- *An element $e \in \mathcal{K}\mathcal{Q}$ is an idempotent if $e^2 = e$.*
- *Idempotents $e, f \in \mathcal{K}\mathcal{Q}$ are orthogonal if $ef = fe = 0$.*
- *An idempotent e is primitive if e cannot be written as a sum $e = e_1 + e_2$, where e_1, e_2 are nonzero orthogonal idempotents of $\mathcal{K}\mathcal{Q}$.*

Every algebra contains trivial idempotents 0 and 1. Generally, for algebra A there holds that if e is a nontrivial idempotent then $1 - e$ is also an idempotent, even the idempotents $e, 1 - e$ are orthogonal, which gives us a decomposition of algebra $A = Ae \oplus A(1 - e)$.

Let $\mathcal{Q}$ be a finite quiver. We can see that identity element of $\mathcal{K}\mathcal{Q}$ is a sum of basis vectors corresponding to stationary paths in the quiver $\mathcal{Q}$. An important set of idempotents of path algebras is described in the following remark taken from [2, p.46].

Remark 2.12. *Let $\mathcal{Q}$ be a finite quiver. $\mathcal{K}-$algebra $\mathcal{K}\mathcal{Q}$ has identity element $\sum_{a \in Q_0} \epsilon_a$ and set $\{\epsilon_a \mid a \in Q_0\}$ is a complete set of primitive orthogonal idempotents of $\mathcal{K}\mathcal{Q}$.*

The complete set of primitive orthogonal idempotents of KQ $\{\epsilon_1, \ldots, \epsilon_n\}$ generates an indecomposible decomposition of $\mathcal{K}\mathcal{Q}_{\mathcal{K}\mathcal{Q}}$ as $\epsilon_1\mathcal{K}\mathcal{Q} + \ldots + \epsilon_n\mathcal{K}\mathcal{Q}$.

Because path algebras have structure of rings it is a natural way to continue our study with ideals of path algebras.At first we need to recall some terms.

Definition 2.13. *Let I be an ideal of ring R. We say that I is nilpotent if there exists $n \geq 1$ that $I^n = 0$.*

A maximal ideal I of ring R is such that each ideal J, which lies between I and R, which means $I \subseteq J \subseteq R$, has to be equal to I or R. The intersection of all maximal ideals of ring is called the (Jacobsons) radical $\operatorname{rad} R$ of ring R.

Let $\mathcal{Q}$ be a finite quiver. The two-sided ideal of path algebra $\mathcal{K}\mathcal{Q}$ generated by arrows of $\mathcal{Q}$ is called an arrow ideal of $\mathcal{K}\mathcal{Q}$ and it is denoted by $R_{\mathcal{Q}}$. Immediately from definition we get that an arrow ideal $R_{\mathcal{Q}}$ contains all linear combination of basis elements corresponding to paths of length ≥ 1.

Lemma 2.14. *Let $\operatorname{rad} R$ be the radical of R. If I is a two-sided nilpotent ideal of R, then $I \subset \operatorname{rad} R$. If the algebra R/I is isomorphic to a product $\mathcal{K} \times \ldots \times \mathcal{K}$ of copies $\mathcal{K}$, then $I = \operatorname{rad} R$.*

The proof of this lemma can be seen in [2, p.5].

Lemma 2.15. *Let $\mathcal{Q}$ be a finite quiver and let $R_{\mathcal{Q}}$ be the arrow ideal of $\mathcal{K}\mathcal{Q}$. Then $\mathcal{K}\mathcal{Q}/R_{\mathcal{Q}}$ is isomorphic to a product of $|Q_0|$ copies of $\mathcal{K}$ as $\mathcal{K}-$algebra.*

The proof of this lemma can be seen in [2, p.49].

Theorem 2.16. *For a finite dimensional algebra $\mathcal{K}\mathcal{Q}$ is $\operatorname{rad}\mathcal{K}\mathcal{Q}$ nilpotent and the arrow ideal $R_{\mathcal{Q}} = \operatorname{rad}\mathcal{K}\mathcal{Q}$.*

Proof. The fact, that $\operatorname{rad}\mathcal{KQ}$ is nilpotent, comes from [2, p.8]. Since we assume that the algebra $\mathcal{KQ}$ is finite dimensional, we have from Remark 2.10 that the quiver $\mathcal{Q}$ is acyclic. Hence there exists the largest $l \geq 1$ such that $\mathcal{Q}$ contains path of length l. However this implies that any product of $l+1$ elements of $R_{\mathcal{Q}}$ is zero, so $R_{\mathcal{Q}}^{l+1} = 0$. Consequently, the ideal $R_{\mathcal{Q}}$ is nilpotent and hence, by Lemma 2.14, $R \subset \operatorname{rad}\mathcal{KQ}$. By Lemma 2.15 $\mathcal{KQ}/R_{\mathcal{Q}}$ is isomorphic to a product of copies of $\mathcal{K}$, it follows from Lemma 2.14 that $R_{\mathcal{Q}} = \operatorname{rad}\mathcal{KQ}$. □

Now we put our results together in the following theorem:

Theorem 2.17. *Let $\mathcal{Q}$ be an acyclic finite quiver. The path algebra $\mathcal{KQ}$ is finite dimensional $\mathcal{K}-$algebra with an identity, that has the arrow ideal as radical and the set $\{\epsilon_a \mid a \in Q_0\}$ as a complete set of primitive orthogonal idempotents.*

By definition of multiplication in path algebra $\mathcal{KQ}$ is clear that for $a, b \in Q_0$ is $\epsilon_a\mathcal{KQ}\epsilon_b$ a vector space with basis of all paths whose source is a and whose target is b. Using this observation we get a decomposition of path algebra $\mathcal{KQ}$

$$\mathcal{KQ} = \oplus_{a,b\in Q_0}\epsilon_a\mathcal{KQ}\epsilon_b.$$

From [2, p.51] we get even more:

Theorem 2.18. *Let $\mathcal{Q}$ be an acyclic finite quiver with $Q_0 = \{1, \ldots, n\}$ such that, whenever there exists a path from i to j in $\mathcal{Q}$ then $j \leq i$. The path algebra $\mathcal{KQ}$ is isomorphic to lower triangular matrix algebra*

$$A = \begin{bmatrix} \epsilon_1(\mathcal{KQ})\epsilon_1, & 0 & \ldots & 0 \\ \epsilon_2(\mathcal{KQ})\epsilon_1, & \epsilon_2(\mathcal{KQ})\epsilon_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \epsilon_n(\mathcal{KQ})\epsilon_1, & \epsilon_n(\mathcal{KQ})\epsilon_2 & \ldots & \epsilon_n(\mathcal{KQ})\epsilon_n \end{bmatrix}$$

Simple consequence of the previous theorem is that if we restrict ourselves to finite acyclic quivers with no multiple arrows then $\mathcal{KQ}$ is isomorphic to a subalgebra of the full lower triangular matrix algebra. In case of Dynkin quiver A_n the $\mathcal{KQ}$ is isomorphic to the complete full lower triangular matrix algebra.

For a cyclic finite quiver $\mathcal{Q}$ the path algebra $\mathcal{KQ}$ is not generally finitely generated. For example the quiver $\mathcal{Q}$ where $|Q_0| = 1$ and Q_1 contains one loop then the path algebra $\mathcal{KQ}$ is isomorphic to $\mathcal{K}[x]$ polynomial algebra of one variable which is not finite dimensional because the basis is $\{1, x, x^2, \ldots\}$. But we show that for a suitable ideal I of a non-finite dimensional path algebra $\mathcal{KQ}$ the quotient algebra $\mathcal{KQ}/I$ is finite dimensional. We focus on these ideals now.

For $m \geq 1$ we define

$$R_{\mathcal{Q}}^m = \oplus_{l\geq m}\mathcal{KQ}_l$$

it is ideal of $\mathcal{KQ}$ generated by all paths of length m in $\mathcal{Q}$.

We call an ideal I admissible if there exists $m \geq 2$ such that $R_{\mathcal{Q}}^m \subseteq I \subseteq R_{\mathcal{Q}}^2$. Hence I is admissible if and only if it contains all paths whose length is long enough. In other words, for each cycle β in $\mathcal{Q}$ there exists $m \geq 1$ such that $\beta^m \in I$. In particular, if $\mathcal{Q}$ is acyclic then every ideal of $\mathcal{KQ}$ contained in $R_{\mathcal{Q}}^2$ is admissible.

Definition 2.19. *For I an admissible ideal of $\mathcal{KQ}$ a pair $(\mathcal{Q}, I)$ is called a bound quiver. The quotient algebra $\mathcal{KQ}/I$ is said to be algebra of the bound quiver $(\mathcal{Q}, I)$ or simplier a bound quiver algebra.*

It will be useful to define an admissible ideal in terms of its generators. We will call these generators relations.

Definition 2.20. *Let $\mathcal{Q}$ be a finite quiver. A relation in $\mathcal{Q}$ is $\mathcal{K}-$linear combination of paths of length at least two having the same source and target.*

It means a relation ρ is an element of $\mathcal{KQ}$ which can written as

$$\rho = \sum_{i=1}^{n} \lambda_i w_i$$

where $\lambda_i \in \mathcal{K}$ and w_i are paths in $\mathcal{Q}$ with the same target and source and their length is at least two.

At the end of the chapter we state two important theorems about bound quiver algebras taken from [2].

Theorem 2.21. *For a finite quiver $\mathcal{Q}$ and an admissible ideal I of $\mathcal{KQ}$ the set $\{\epsilon_a + I \mid a \in Q_O\}$ is a complete set of primitive orthogonal idempotents of the bound quiver algebra $\mathcal{KQ}/I$ and the bound quiver algebra $\mathcal{KQ}/I$ is finite dimensional.*

Theorem 2.22. *Let $\mathcal{Q}$ be a finite quiver, let $R_\mathcal{Q}$ the arrow ideal of $\mathcal{KQ}$ and let I be an admissible ideal of KQ. Then* $\mathrm{rad}(\mathcal{KQ}/I) = R_\mathcal{Q}/I$.

Both proofs can be found in [2, p.56-57]

3. Modules of path algebras

Since codes over rings are submodules of module R^n over ring R we now focus on modules over path algebras.

3.1 Modules over algebras

In the elementary definition of modules over algebra and describing their properties we will use notation of right modules. Left modules of algebra A can be seen as right $A^{op}-$modules and conversely, where A^{op} denote opposite algebra defined in the previous chapter.

In studying the codes over algebras we need to remember that algebras have a structure of a vector space over $\mathcal{K}$. Hence modules over algebras also have a structure of vector space. The multiplication is natural as the following definition shows.

Definition 3.1 (Modules over $\mathcal{K}-$Algebra)**.** *Let A be $\mathcal{K}-$algebra. A right $A-$module is $(M, \cdot)$, where M is a vector space over $\mathcal{K}$ and a multiplication $\cdot$ satisfies the following conditions:*

- $(m+n)\cdot a = m\cdot a + n\cdot a$
- $m\cdot(a+b) = m\cdot a + m\cdot b$
- $m\cdot(ab) = (m\cdot a)\cdot b$
- $(m\cdot k)\cdot a = m\cdot(ak) = (m\cdot a)\cdot k$

$\forall m, n \in M$, $\forall a, b \in A$, $\forall k \in \mathcal{K}$.

Instead of $(M, \cdot)$ we will write M_A for a right module M over $\mathcal{K}-$algebra A. If we look of the algebra A as a right module we will write A_A.

We say that a module M is finite dimensional if the dimension M over $\mathcal{K}$ is finite. Elements $m_1, \ldots, m_n$ of M generate the $A-$module M_A if any element m of M can be written as $m = m_1a_1 + \ldots, m_na_n$ for some $a_1, a_n \in A$. We will describe this situation by notation $M = m_1A + \ldots + m_nA$. The module M_A is finitely generated if it is generated by finite subset of elements of M.

Remark 3.2. *A module over a finite dimensional $\mathcal{K}-$algebra is finitely generated if and only if it is finite dimensional.*

The direct sum M of the right $A-$modules $M_1, \ldots, M_n$ is defined to be a module with structure of the $\mathcal{K}-$vector space $M_1 \oplus \ldots \oplus M_n$ and with an $A-$module structure defined by $(m_1, \ldots, m_n)a = (m_1a, \ldots, m_na)$ for $m_1 \in M_1, \ldots, m_n \in M_n$ and $a \in A$. The modules $M_1, \ldots, M_n$ are called direct summands of M, we will call them simple summands. Let M be a $A-$module then we call M indecomposable if M is nonzero module and M has no direct sum decomposition $M \cong N_1 \oplus N_2$ where N_1, N_2 are nonzero $A-$modules.

Since a right $A-$module M has the structure of the vector space over $\mathcal{K}$ we can find the dual vector space M^* consisted of $\mathcal{K}-$linear forms $\mathrm{Hom}(M, \mathcal{K})$. We can endow M^* with the left $A-$module structure given by the formula $(a\phi)(m) = \phi(ma)$ for $a \in A$, $\phi \in \mathrm{Hom}(M, \mathcal{K})$ and $m \in M$. This assignment of M^* to M is called the standard $\mathcal{K}-$duality and denoted by $\mathcal{D}$. As we mention at the beginning of the chapter a left $A-$module can be seen as a right A^{op} module. We get that $\mathcal{D}$ is a functor between category of right $A-$modules and right A^{op}modules. The quasi-inverse of the duality $\mathcal{D}$ is also denoted by $\mathcal{D}$ and is defined as above only with using left $A-$modules.

Now we recall some important modules in category of modules over $\mathcal{K}-$algebra. First of them are simple modules.

Definition 3.3. *Right $A-$module M is simple if M is nonzero and any submodule of M is either zero or M.*

For an $A-$module M we define $\operatorname{rad} M$ as the intersection of all maximal submodules of M. Radical of right $A-$module A_A is the radical $\operatorname{rad} A$ of algebra A. The radical of algebra is identical to term of the radical of the ring because submodules of R are ideals. The following lemma will lead us to important property of radical of modules mentioned in [2, p.14].

Lemma 3.4. *Let L and M be submodules of N. If $L \subseteq \operatorname{rad} N$ and $L + M = N$ then $M = N$.*

Proof. For contradiction we assume that $M \neq N$. So M is submodule of some maximal submodule of N. Denote one of them P. It is clear that $L \subset \operatorname{rad} N \subset P$. We get $N = L + M \subset P + M = P$, contrary to our assumption. □

Definition 3.5. *An N submodule of M is called superfluous if for every submodule L of M an equation $L + N = M$ implies $L = M$.*

Using the previous lemma we get that for any module M is $\operatorname{rad} M$ superfluous. This statement we will use in Chapter 5.

As a dual notion to the radical of a modules we define a socle of modules M $\operatorname{soc}(M)$ by sum of the minimal nonzero submodules. By definition of simple modules we get that

$$\operatorname{soc}(M) = \sum \{S \mid S \text{ is a simple submodule of M}\}.$$

If M is an Artinian module, which means that satisfies the descending chain condition on its poset of submodules, $\operatorname{soc}(M)$ is an essential submodule of M, which means that every nonzero submodule of M has non trivial intersection with $\operatorname{soc}(M)$.

The following class of modules will be the most important for us, the class of projective and injective modules.

Definition 3.6. *An $A-$module $\mathcal{P}$ is called projective if for every epimorphism $h : M \to N$ and every homomorphism $f : \mathcal{P} \to N$ there exists a homomorphism $g : \mathcal{P} \to M$ such that*

$$\forall m \in \mathcal{P} \quad h(g(m)) = f(m).$$

An $A-$module $\mathcal{I}$ is called injective if for every monomorphism $h : M \to N$ and every homomorphism $f : M \to \mathcal{I}$ there exists a homomorphism $g : N \to \mathcal{I}$ such that

$$\forall m \in \mathcal{I} \quad g(h(m)) = f(m).$$

It follows a useful remark from the theory of category of modules which helps us define injective modules over $\mathcal{K}\mathcal{Q}-$algebras.

Remark 3.7. *Let A be a $\mathcal{K}-$algebra and let M be a right projective $A-$module. Then $\mathcal{D}(M)$ is a left injective $A-$module.*

Because we can view left $A-$modules as right A^{op} modules, we will consider $\mathcal{D}(m)$ as right injective A^{op}-module. Naturally using quasi-inversion $\mathcal{D}$ we get the remark for left projective $A-$modules.

Now we turn attention to modules over path algebras. As finite algebra we can visualize their modules as a set of vector spaces over $\mathcal{K}$ connected by $\mathcal{K}-$linear maps. This visualization is called representation M of quiver $\mathcal{Q}$.

Definition 3.8. *Let $\mathcal{Q}$ be a finite quiver. A representation M of $\mathcal{Q}$ is defined by:*

- *To each point $a \in Q_0$ is associated a $\mathcal{K}-$linear vector space M_a.*
- *To each arrow $\alpha \in Q_1$, $\alpha : a \to b$, is associated $\mathcal{K}-$linear map $\varphi_\alpha : M_a \to M_b$.*)*

This representation is denoted $M = (M_a, \varphi_\alpha)$. It is called finite dimensional if each vector space M_a is finite dimensional.

For a nontrivial path $w = \alpha_1, \ldots, \alpha_l$ from a to b in a quiver $\mathcal{Q}$ we define the evaluation of representation M of $\mathcal{Q}$ on the path w to be $\mathcal{K}-$linear map from M_a to M_b defined by

$$\varphi_w = \varphi_{\alpha_l} \cdots \varphi_{\alpha_1}.$$

We can extend the definition of evaluation to $\mathcal{K}-$linear combination of paths with the same source and the same target, this combinations we called relations. For a relation

$$\rho = \sum_{i=1}^{n} \lambda_i w_i$$

where $\lambda_i \in K$ and w_i are paths in $\mathcal{Q}$ we get

$$\varphi_\rho = \sum_{i=1}^{n} \lambda_i \varphi_{w_i}.$$

This will allow us to define a representation of a bound quiver. Let $\mathcal{Q}$ be a finite quiver and I be an admissible ideal $\mathcal{K}\mathcal{Q}$. A representation M of $\mathcal{Q}$ is bound by I if for every relation ρ in I is $\varphi_\rho = 0$.

The category of $\mathcal{K}-$linear representations over quiver $\mathcal{Q}$ is denoted as $\mathrm{Rep}(\mathcal{Q})$. We denote by $\mathrm{rep}(\mathcal{Q})$ the full subcategory of $\mathrm{Rep}(\mathcal{Q})$ consisting of the finite dimensional representations. We denote by $\mathrm{Rep}(\mathcal{Q}, I)$ (resp. $\mathrm{rep}(\mathcal{Q}, I)$) the full

subcategory of $\mathrm{Rep}(\mathcal{Q})$ (resp. of $\mathrm{rep}(\mathcal{Q})$) consisting of the representation of $\mathcal{Q}$ bound by I.

As we mentioned in the previous chapter for a finite dimensional $\mathcal{K}-$algebra A there exists a quiver $\mathcal{Q}_A$ and admissible ideal I such that $A \cong \mathcal{K}\mathcal{Q}_A/I$. The following theorem, taken from [2, p.72-73], shows that there is a equivalence between $\mathrm{rep}(\mathcal{Q}, I)$ and the category $\mathrm{mod}\, A$, which denotes the subcategory of the category of all right $A-$modules whose objects are finite generated. The category of all right $A-$modules is denoted by $\mathrm{Mod}\, A$.

Theorem 3.9. *Let $A = \mathcal{K}\mathcal{Q}/I$, where Q is finite quiver and I is an admissible ideal of $\mathcal{K}\mathcal{Q}$. There exists a $K-$linear equivalence of categories*

$$F : \mathrm{Mod}\, A \xrightarrow{\cong} \mathrm{Rep}(\mathcal{Q}, I)$$

that restrict to an equivalence of categories $F\,\mathrm{mod}\, A \xrightarrow{\cong} \mathrm{rep}(\mathcal{Q}, I)$.

The proof of this theorem shows how we can construct the representation of $A-$modules and how we obtain from a representation an $A-$module. The proof can be find in [2, p.72-73]. Since we will use representation to graphically visualize modules we will show how we can obtain a module from a representation.

Let $M = (M_a, \varphi_\alpha)$ be a representation from the category $\mathrm{Rep}(\mathcal{Q}, I)$. We set $G(M) = \bigoplus_{a \in Q_0} M_a$, by definition of representations $G(M)$ is $\mathcal{K}-$vector space. Let thus $(x_a)_{a \in Q_0}$ belong to $G(M)$. To define $\mathcal{K}\mathcal{Q}$ module structure on $G(M)$, it suffices to define the products of the form $x\beta$ where β is a path in $\mathcal{Q}$. If $\beta = \epsilon_a$ is the stationary path in a, we put

$$x\epsilon_a = x_a.$$

If $\beta = \alpha_1 \dots \alpha_l$ is a nontrivial path from a to b, we consider the $\mathcal{K}-$linear map $\varphi_\beta = \varphi_{\alpha_1} \dots \varphi_{\alpha_l} : M_a \to M_b$. We put

$$(x\beta)_c = \delta_{b,c}\varphi_\beta(x_a).$$

In other words, $x\beta$ is the element of $G(M) = \bigoplus_{a \in Q_0} M_a$ whose only nonzero coordinate is $(x\beta)_b = \varphi_\beta(x_a) \in M_b$. Thus shows that $G(M)$ is a $\mathcal{K}\mathcal{Q}-$module. Moreover, it follows from the definition of $G(M)$ that, for each $\rho \in I$ and $x \in G(M)$, we have $x\rho = 0$. Thus $G(M)$ becomes a $\mathcal{K}\mathcal{Q}/I-$ module under assignment $x(u + I) = xu$ for $x \in G(M)$ and $u \in \mathcal{K}\mathcal{Q}$.

3.2 Injective modules

Since a general path algebra is not Frobenius ring, we focus on injective modules of path algebras as they are described in [2, p.76-81]. Let $\mathcal{Q}$ be a finite quiver. For $a \in Q_0$ we denote $S(a)$ a representation $(S(a)_b, \varphi_\alpha)$ of $\mathcal{Q}$ defined by

$$S(a)_b = \begin{cases} K, & \text{if } b = a \\ 0, & \text{if } b \neq a \end{cases}$$

$$\varphi_\alpha = 0 \text{ for all } \alpha \in Q_1.$$

$S(a)$ seen as $\mathcal{K}\mathcal{Q}-$module is the simple $\mathcal{K}\mathcal{Q}-$module corresponding to the point $a \in Q_0$. Next we show the construction of indecomposable projective and injective module. We have the complete set of primitive orthogonal idempotents of $\mathcal{K}\mathcal{Q}$ $\{\epsilon_a | a \in Q_0\}$ then decomposition

$$A_A = \oplus_{a \in Q_0} \epsilon_a A$$

is a direct sum of pairwise non-isomorphic indecomposable projective $\mathcal{K}\mathcal{Q}-$modules. The following theorem describe these projective modules $\mathcal{P}(a) = \epsilon_a A$.

Theorem 3.10. *Let $\mathcal{Q}$ be a finite acyclic quiver. Then for $a \in Q_0$ the representation $\mathcal{P}(a) = (P(a)_b, \varphi_\beta)$ holds:*

- *For a point b, $P(a)_b$ is $\mathcal{K}-$vector space with basis the set of all paths from a to b*
- *For an arrow $\beta : b \to c$, the $\mathcal{K}-$linear map $\varphi_\beta : P(a)_b \to P(a)_c$ is given by the right multiplication by β.*

If we assume a general quiver $\mathcal{Q}$ and a bound quiver $(\mathcal{Q}, I)$ for an admissible ideal I, the representation $(P(a)_b, \varphi_\beta)$ holds:

- *For a point b, $P(a)_b$ is $\mathcal{K}-$vector space with basis the $\mathcal{K}-$linear independent subset of the set of all the $\widehat{w} = w + I$ where w is a path from a to b.*
- *For an arrow $\beta : b \to c$, the $\mathcal{K}-$linear map $\varphi_\beta : P(a)_b \to P(a)_c$ is given by the right multiplication by $\widetilde{\beta} = \beta + I$.*

Now we describe the indecomposable injective $\mathcal{K}\mathcal{Q}-$modules. A complete list of pairwise non-isomorphic indecomposable injective $\mathcal{K}\mathcal{Q}-$module is given by modules $\mathcal{I}(a) = \mathcal{D}(A\epsilon_a)$ where D is the standard duality defined in the previous section. We mentioned that a duality image of a left projective $\mathcal{K}\mathcal{Q}-$module is a right injective $\mathcal{K}\mathcal{Q}-$module so the $\mathcal{I}(a)$ is indeed injective.

Theorem 3.11. *Let $\mathcal{Q}$ be a finite acyclic quiver. Then socle of $\mathcal{I}(a)$ is isomorphic to the simple module $S(a)$ for each $a \in Q_0$. If we denote representation $\mathcal{I}(a)$ as $(I(a)_b, \varphi\beta)$ then*

- *for a point, b $I(a)_b$ is the dual of the $\mathcal{K}-$vector space with basis the $\mathcal{K}-$linear independent subset of the set of all path from b to a*
- *for an arrow $\beta : b \to c$, the $\mathcal{K}-$linear map $\varphi_\beta : I(a)_b \to I(a)_c$ is given by the dual of the left multiplication by β.*

For a bound quiver $(\mathcal{Q}, I)$, where $\mathcal{Q}$ is a general quiver and I is an admissible ideal, the representation $\mathcal{I}(a)$ holds:

- *For a point, b $I(a)_b$ is the dual of the $\mathcal{K}-$vector space with basis the set of all the $\widehat{w} = w + I$ where w is a paths from b to a*
- *For an arrow $\beta : b \to c$, the $\mathcal{K}-$linear map $\varphi_\beta : I(a)_b \to I(a)_c$ is given by the dual of the left multiplication by $\widetilde{\beta} = \beta + I$.*

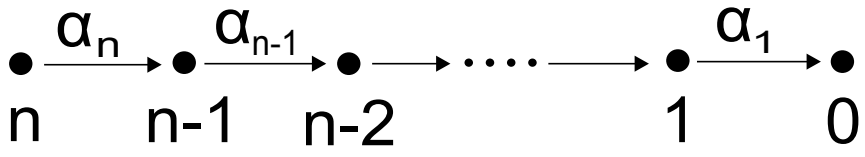
In the case when $\mathcal{Q}$ is acyclic finite quiver $P(a)_b$ is nothing but the $\mathcal{K}-$vector space having as base the set of all paths from a to b and $I(a)_b$ is the dual of the $\mathcal{K}-$vector space with basis the set of all paths from b to a. In general the dual of vector space is mention as space of linear forms. The basis of the dual is obtain from the basis of original vector space applying the rule

$$f_i(b_j) = \begin{cases} 1, & \text{for } i = j \\ 0, & \text{for } i \neq j. \end{cases}$$

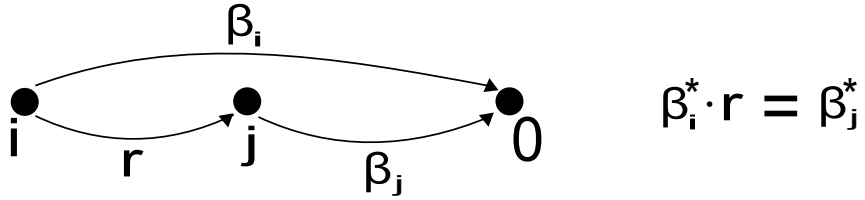
where $\{b_1, \ldots, b_n\}$ is original base, then $\{f_1, \ldots, f_n\}$ is basis of the dual space. In case of path algebras the basis vectors, all paths from b to a, form the vector space $\epsilon_b \mathcal{K}\mathcal{Q}\epsilon_a$. Let $\alpha_1, \ldots, \alpha_n$ are all path from b to a then $\alpha_1^*, \ldots, \alpha_n^*$ is the basis of the dual space $I(a)_b$ when $\alpha_i^*(\alpha_j) = \delta_{i,j}(1)$.

A multiplication by element r from $\mathcal{K}\mathcal{Q}$ is given by the dual of the left multiplication by β. This means that for the element α^* of $\mathcal{I}(a)$ and the element r of $\mathcal{K}\mathcal{Q}$ there is $\alpha \cdot r(s) = \alpha(rs)$ which implies that $\alpha^* \cdot r = \beta^*$ if $\alpha = r\beta$ otherwise $\alpha^* \cdot r = 0$. The structure of the injective module $\mathcal{I}(a)$ is important for us so we will show the structure and multiplication in an example.

Example. *As we mention in the previous chapter, for examples we will use Dynkin quivers A_n. We numbered the points of A_n from right to left and the the arrows are denoted α_i if its source is the point i then its target is $i - 1$.*



For $i \in \{1, \ldots, n\}$ we denote β_i the composition $\alpha_i \ldots \alpha_1$ and β_0 the trivial path ϵ_0. Then by the previous theorem for all $i \in \{0, \ldots, n\}$ the $I(0)_i$ is dual of the vector space $\epsilon_i \mathcal{K}\mathcal{Q}\epsilon_0$ which is in our case one dimensional $\mathcal{K}-$vector space with basis β_i. We denote the basis vector of the dual space β_i^*. Then any element of $\mathcal{I}(0)$ can be written as $\sum_{i=0}^{n} k_i \beta_i^*$ where k_i are elements of field $\mathcal{K}$. The multiplication by element of $\mathcal{K}\mathcal{Q}$ is nonzero only for $\beta_i^* \in \mathcal{I}(a)$ and $r \in \mathcal{K}\mathcal{Q}$ such that r and β_i has the same source as we discuss above. Then the multiplication can be easily understood by using the following picture:



Hence $\beta_i^* \cdot \epsilon_j = \delta_{ij}(\beta_i^*)$ and $\beta_i^* \cdot \alpha_j = \delta_{ij}\left(\beta_{i-1}^*\right)$ and the rest of cases can be obtained by associative and distributive laws.

The example gives us an idea, what the general $\mathcal{I}(a)$ looks like, mainly how multiplication by elements of $\mathcal{KQ}$ acts on $\mathcal{I}(a)$. Generally let $\gamma_1, \ldots, \gamma_n$ be all paths in quiver $\mathcal{Q}$ with the same source b and the same target a and let δ be any path with source $c \neq b$ and target a, then by definition of injective module $\mathcal{I}(a)$ $\gamma_1^*, \ldots, \gamma_n^*, \delta^*$ are elements of $\mathcal{I}(a)$. There are two important results for multiplication by elements of $\mathcal{KQ}$.

- $\gamma_i^* \epsilon_b = \gamma_i$ for all i.
- $\delta^* \epsilon_b = 0$.
- $\gamma_i^* \gamma_j = \delta_{ij} \, (\epsilon_a^*)$
- $\delta^* \gamma_j = 0$ for all j.

4. Codes over path algebras

From the previous chapters we get the instruments to construct linear codes over path algebras $\mathcal{K}\mathcal{Q}$ for finite acyclic quivers $\mathcal{Q}$. Generally an algebra $\mathcal{K}\mathcal{Q}$ seen as ring does not have to be self-injective which means $\mathcal{K}\mathcal{Q}$ is not Frobenius ring. So we need take some injective $\mathcal{K}\mathcal{Q}$-modules $\mathcal{I}$ and study codes which are submodules of $\mathcal{I}^n$. From the previous chapter we have indecomposable injective $\mathcal{K}\mathcal{Q}-$modules $\mathcal{I}(a)$ for a from $\mathcal{Q}$.

Since for acyclic finite quivers an injective ideal $\mathcal{I}(a)$ has representation $(I(a)_b, \varphi_\alpha)$ where $I(a)_b$ is the vector space with basis the set of all paths from b to a in $\mathcal{Q}$ we can assume that quiver $\mathcal{Q}$ has structure of an oriented tree where arrows go towards a root. We can denote the root a and we will assume only the injective module $\mathcal{I}(a)$. Then the module $\mathcal{I}(a)$ is the biggest injective indecomposable $\mathcal{K}\mathcal{Q}-$module and the quiver $\mathcal{Q}$ is the smallest quiver such that module $\mathcal{I}(a)$ is an indecomposable injective $\mathcal{K}\mathcal{Q}-$module. In other words, if we get an indecomposable injective $\mathcal{K}\mathcal{Q}-$module $\mathcal{I}$ we can find a uniquely determined quiver $\widehat{\mathcal{Q}}$ with the oriented tree structure with a root a such that $\mathcal{K}\widehat{\mathcal{Q}} \subset \mathcal{K}\mathcal{Q}$ and $\mathcal{K}\widehat{\mathcal{Q}}-$module $\mathcal{I}(a)$ is $\mathcal{K}\widehat{\mathcal{Q}}-$isomorphic to $\mathcal{I}$. An example is the Dynkin quiver A_n with the indecomposable injective module $\mathcal{I}(0)$.

Now we have the alphabet for our codes but we need some bilinear form which would generalize an inner product. Since a path algebra $\mathcal{K}\mathcal{Q}$ is not an integral domain and is not necessarily commutative we would like to have a form which preserves these properties instead of the inner product which does not. Since we want that dual codes would be a submodule of $\mathcal{I}(a)^n$ as well, we will define bilinear form β as a map

$$\beta : \quad \mathcal{I}(a)_{\mathcal{K}\mathcal{Q}} \otimes_{\mathbb{Z}} \mathcal{I}(a)_{\mathcal{K}\mathcal{Q}} \to \mathcal{A}_{\mathcal{K}\mathcal{Q}\otimes\mathcal{K}\mathcal{Q}}$$

where $\mathcal{A}$ is a right $\mathcal{K}\mathcal{Q} \otimes \mathcal{K}\mathcal{Q}-$module. This general definition is taken from [9, p.84] where the authors discuss the proper choice of $\mathcal{A}$. Based on their results we take the tensor product of two copies of $\mathcal{I}(a)$. Then $\mathcal{A}$ has structure of $(\dim_K (I(a)))^2$ dimensional $\mathcal{K}-$vector space with structure of right $\mathcal{K}\mathcal{Q} \otimes \mathcal{K}\mathcal{Q}-$module. We will use simplier notation (a, b) instead of $(a \otimes b)$. Then β is an isomorphism

$$\beta : I(a)^n_{\mathcal{K}\mathcal{Q}} \otimes_{\mathcal{K}} I(a)^n_{\mathcal{K}\mathcal{Q}} \to (I^n(a) \otimes I^n(a))_{\mathcal{K}\mathcal{Q}\otimes\mathcal{K}\mathcal{Q}}$$

with intuitive definition, $\beta(x, y) = (x \otimes y) = (x, y)$ with our new notation, for $x, y \in I(a)$.

For better understanding of structure of $\mathcal{A}$ we focus on the structure of path algebra $\mathcal{K}\mathcal{Q} \otimes_{\mathcal{K}} \mathcal{K}\mathcal{Q}$. Let $\overline{\mathcal{Q}}$ be quiver with the following properties:

- $\overline{Q}_0 = Q_0 \otimes Q_0$.
- Let $\alpha : a \to b$ be an arrow in Q_1 and let x be a point from Q_0, then there are arrows $\beta, \gamma \in \overline{Q}_1$ such that $\beta : (a, x) \to (b, x)$ and $\gamma : (x, a) \to (x, b)$.

Let I be an ideal of $\mathcal{K}\overline{\mathcal{Q}}$ generated by relations, which describe the following situation: for $a \to b$ and $c \to d$ from Q_1 the compositions $(a, c) \to (b, c) \to (b, d)$

and $(a,c) \to (a,d) \to (b,d)$ are the same. Now we define a map $f : \mathcal{KQ} \otimes_{\mathcal{K}} \mathcal{KQ} \to \mathcal{K}\overline{\mathcal{Q}}/I$ by the prescription

$$f(x \otimes y) = (x, y).$$

By properties of the tensor product we get $(a \otimes b)(c \otimes d) = (ac \otimes bd)$ which implies that

$$f(ac \otimes bd) = f\left((a \otimes b)(c \otimes d)\right) = f(a \otimes b) f(c \otimes d) = (a,b)(c,d) = (ac, bd)$$

and hence f is a homomorphism of rings (algebras) since similarly there holds that $(a \otimes b) + (a \otimes d) + (c \otimes b) + (c \otimes d) = (a + c \otimes b + d)$.

We can easily see that f is an epimorphism since for each $(a,b) \in \mathcal{K}\overline{\mathcal{Q}}/I$ there exists $(a \otimes b) \in \mathcal{KQ} \otimes_{\mathcal{K}} \mathcal{KQ}$ such that $f(a \otimes b) = (a,b)$.

As the last step to prove that f is even an isomorphism of algebras, we compare dimensions of the $\mathcal{K}-$vector spaces $\mathcal{K}\overline{\mathcal{Q}}/I$ and $\mathcal{KQ} \otimes_{\mathcal{K}} \mathcal{KQ}$. By the definition of the tensor product we get that $\dim_{\mathcal{K}} \mathcal{KQ} \otimes_{\mathcal{K}} \mathcal{KQ} = \left(\dim_{\mathcal{K}} \mathcal{KQ}\right)^2$. By the definition of path algebras the basis of $\mathcal{K}\overline{\mathcal{Q}}$ contains all paths in $\overline{\mathcal{Q}}$. By the definition of $\overline{\mathcal{Q}}$ above, a path $\beta : (a_0, b_0) \to (a_n, b_n)$ can be written as

$$\beta = (a_0, b_0) \to (a_1, b_1) \to \ldots \to (a_n, b_n),$$

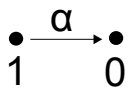
where either $a_i = a_{i+1}$ and there exists an arrow $b_i \to b_{i+1} \in Q_1$ or $b_i = b_{i+1}$ and there exists an arrow $a_i \to a_{i+1} \in Q_1$ for each $i \in \{0, \ldots, n-1\}$. By the definition of the admissible ideal I, the elements of $\mathcal{K}\overline{\mathcal{Q}}/I$ which corresponds to the basis vectors of $\mathcal{K}\overline{\mathcal{Q}}$ are form

$$\beta + I = (a_0,b_0)(a_0,b_1)\ldots(a_0,b_n)(a_1,b_n)\ldots(a_n,b_n) = (a_0,b_0)(a_0,b_n)(a_n,b_n).$$

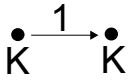
Hence the number of $K-$linear independent elements of $\mathcal{K}\overline{\mathcal{Q}}/I$ is equal to $\left(\dim_{\mathcal{K}}(\mathcal{KQ})\right)^2$. We get that $\dim_{\mathcal{K}} \mathcal{K}\overline{\mathcal{Q}}/I = \dim_{\mathcal{K}} \mathcal{KQ} \otimes_{\mathcal{K}} \mathcal{KQ}$, which implies that f is isomorphism of the algebras.

Since $\mathcal{KQ} \otimes \mathcal{KQ}$ is isomorphic to $\mathcal{K}\overline{\mathcal{Q}}/I$. And as a consequence the $\mathcal{KQ} \otimes \mathcal{KQ}$-module $\mathcal{A}$ is isomorphic to the injective indecomposible $\mathcal{K}\overline{\mathcal{Q}}/I-$ module which correspond to the point $(a,a) \in \overline{Q}_0$.

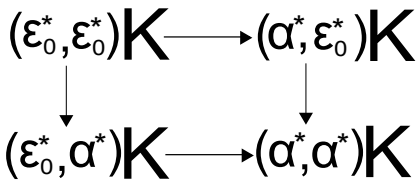
Example. *For a quiver* $\mathcal{Q}$



and binary field $\mathcal{K}$ *we define* $3-$*dimensional path algebra* $\mathcal{KQ}$ *with basis* $\{e_0, \alpha, e_1\}$. *An injective indecomposable* $\mathcal{KQ}-$*module* $\mathcal{I}(0)$ *can be graphically represented as*



The elements of $\mathcal{I}(0)$ *are of form* $k_1\alpha^* + k_0 e_0^*$ *for* $k_1, k_0 \in K$. *Here the module* $\mathcal{A}$ *can be graphically represented as*



Hence $\mathcal{A}$ has structure isomorphic to $M_2(K)$ with actions of multiplication of element of $\mathcal{KQ} \otimes \mathcal{KQ}$ which act by the following laws:

$$\begin{array}{lll}
\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\epsilon_1, 0) = \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} & , & \begin{pmatrix} a & b \\ c & d \end{pmatrix}(0, \epsilon_1) = \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\alpha, 0) = \begin{pmatrix} b & 0 \\ d & 0 \end{pmatrix} & , & \begin{pmatrix} a & b \\ c & d \end{pmatrix}(0, \alpha) = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \\
\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\epsilon_0, 0) = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} & , & \begin{pmatrix} a & b \\ c & d \end{pmatrix}(0, \epsilon_0) = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}
\end{array}$$

Then we define a $\mathcal{KQ}-$isomorphism $\varphi : I(a) \otimes I(a) \to A$ by a prescription

$$\varphi\left(a\epsilon_0^*, b\epsilon_0^*\right) = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \quad , \quad \varphi\left(a\alpha^*, b\epsilon_0^*\right) = \begin{pmatrix} 0 & ab \\ 0 & 0 \end{pmatrix}$$

$$\varphi\left(a\epsilon_0^*, b\alpha^*\right) = \begin{pmatrix} 0 & 0 \\ ab & 0 \end{pmatrix} \quad , \quad \varphi\left(a\alpha^*, b\alpha^*\right) = \begin{pmatrix} 0 & 0 \\ 0 & ab \end{pmatrix}$$

where $a, b \in K$. Finally the bilinear map $\beta : I(a)^n \otimes I(a)^n \to A$ is defined for $c, d \in I(a)^n$ by

$$\beta(c, d) = \sum_{i=1}^{n} \varphi\left(c_i, d_i\right).$$

The situation for Dynkin quiver A_n is analogous only we take $\mathcal{A}$ isomorphic to $M_n(K)$ and we need to generalize the multiplication by the element of the path algebra $\mathcal{K}A_n$. If we keep the idea of the notation of the previous example then the multiplication in $\mathcal{A}_{\mathcal{K}A_n \otimes \mathcal{K}A_n}$ looks like

$$\begin{pmatrix} k_{0,0} & k_{0,1} & \dots & k_{0,n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{i-1,0} & k_{i-1,1} & \dots & k_{i-1,n} \\ k_{i,0} & k_{i,1} & \dots & k_{i,n} \\ k_{i+1,0} & k_{i+1,1} & \dots & k_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{n,0} & k_{n,1} & \dots & k_{n,n} \end{pmatrix}(\epsilon_i, 0) = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \\ k_{i,0} & k_{i,1} & \dots & k_{i,n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$$\begin{pmatrix} k_{0,0} & k_{0,1} & \dots & k_{0,n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{i-2,0} & k_{i-2,1} & \dots & k_{i-2,n} \\ k_{i-1,0} & k_{i-1,1} & \dots & k_{i-1,n} \\ k_{i,0} & k_{i,1} & \dots & k_{i,n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{n,0} & k_{n,1} & \dots & k_{n,n} \end{pmatrix} (\alpha_i, 0) = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \\ k_{i,0} & k_{i,1} & \dots & k_{i,n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$$\begin{pmatrix} k_{0,0} & k_{0,1} & \dots & k_{0,n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{i,0} & k_{i,1} & \dots & k_{i,n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{n,0} & k_{n,1} & \dots & k_{n,n} \end{pmatrix} (\beta_i, 0) = \begin{pmatrix} k_{i,0} & k_{i,1} & \dots & k_{i,n} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

The rest we obtain from linearity and associativity.

For a general quiver $\mathcal{Q}$ and its indecomposable injective module $\mathcal{I}(a)$, the $(\mathcal{K}\mathcal{Q} \otimes \mathcal{K}\mathcal{Q})-$module $\mathcal{A}$ can have quite complex structure which can be still represented by matrix, only indexes of row and columns cannot be denoted by numbers but by basis elements of $\mathcal{I}(a)$ and the computation is defined with respect to the structure of a quiver, so this bilinear form can work in a general case.

4.1 Homogeneous weight

Now we have an alphabet and a bilinear map for gaining a dual code but as we mentioned before we will use more complex weight function than Hamming weight, we will use homogeneous weight which better describes the structure of modules, especially a lattice of submodules. The definition below shows the main properties of homogeneous weight.

Definition 4.1. *Let M be a right $R-$module. A function $\omega : M \to \mathbb{R}$ is called homogeneous weight if*

- $\omega(0) = 0$.
- *If $xR = yR$, then $\omega(x) = \omega(y)$.*
- *There exists $\gamma \in \mathbb{R}$ such that*

$$\sum_{m \in xR} \omega(m) = \gamma |xR| \quad \forall x \in M - \{0\}\,.$$

The number γ may be called the average of homogeneous weight ω.

For obtaining a formula for computing homogenous weight more easily we use the Möbius inversion on a finite partially ordered set $(B, \leq)$.

Definition 4.2. *Let $(B, \leq)$ be a finite partially ordered set, the Möbius function $\mu : B \times B \to \mathbb{Q}$ is defined by*

- $\mu(x,x) = 1$.
- $\mu(x,y) = 0$ *if* $x \not\leq y$.
- $\sum_{y \leq t \leq x} \mu(t,x) = 0$ *if* $y < x$.

Using the Möbius function we get a result from [7, p.224].

Theorem 4.3. *Let μ denote the Möbius function. A real-valued function* $\mathbf{w}$ *on the finite module M_R is homogeneous weight if and only if there exists a real number γ such that*

$$\mathbf{w}(x) = \gamma \left(1 - \frac{\mu\left(O, xR\right)}{|x^*R|}\right),$$

where x^*A is set of all generating elements of the submodule xR.

Proof. Let γ be a real number and $\mathbf{w}$ be the real-valued function from theorem

$$\mathbf{w}(x) = \gamma \left(1 - \frac{\mu\left(O, xR\right)}{|x^*R|}\right).$$

We will prove that the function $\mathbf{w}$ satisfies the conditions for homogeneous weight defined in Definition 4.1. By definition of the Möbius function we get that $\mu(0,0) = 1$ and the module $0R$ is generated only by the element 0, hence

$$\mathbf{w}(0) = \gamma \left(1 - \frac{1}{1}\right) = 0$$

and the first condition holds. For $x, y \in M$ such that $xR = yR$ its trivial that the number of generating elements of module xR is the same as the number of generating elements of yR and the values of the Möbius function is the same as well. Hence $\mathbf{w}(x) = \mathbf{w}(y)$.

For a nonzero element x of M we denote $x_1, \ldots, x_n$ the generating elements of all submodules xR. Then $0 \subseteq x_iR \subseteq xR$ for all i and let us suppose that $x_1R = 0R$ and $x_nR = xR$. Hence

$$\begin{aligned}\sum_{m \in xR} \mathbf{w}(m) &= \sum_{m \in xR} \gamma \left(1 - \frac{\mu(0, mR)}{|m * R|}\right) = \gamma\,|xR| - \sum_{m \in xR} \frac{\mu(0, mR)}{|m * R|} = \\ &= \gamma\,|xR| - \sum_{i=1}^{n} |x_i^*R|\,\frac{\mu(0, x_iR)}{|x_i^*R|} = \gamma\,|xR| - \sum_{i=1}^{n} \mu(0, x_iR).\end{aligned}$$

Since x_iR are all submodules between $0R$ and xR, by definition of the Möbius function μ, we get that $\sum_{i=1}^{n} \mu(0, x_iR) = 0$ and finally $\mathbf{w}(x) = \gamma\,|xR|$ for a general nonzero element of M.

Now let ω be a homogenous weight by Definition 4.1. Let $\mathbf{w}$ be a real-valued function defined as

$$\mathbf{w}(x) = \gamma \left(1 - \frac{\mu\left(O, xR\right)}{|x^*R|}\right),$$

where γ is the average of homogeneous weight ω. We get easily that $\omega(0) = 0 = \mathbf{w}(0)$. Now let assume that a element $x \in M$ generates a minimal one-generated

module of M which means that for every nonzero $y \in M$ such, that $0 \subseteq yR \subseteq xR$, is $yR = xR$. Since xR is a module, the zero element is in xR and from submodule minimality of xR we have $|x * R| + 1 = |xR|$. By applying of all three properties of homogeneous weight from definition we get

$$\gamma\,|xR| = \gamma\,(|x^*R| + 1) = \sum_{y \in xR} \omega(y) = \omega(0) + \sum_{y \in x^*R} \omega(y) = 0 + |x^*R|\,\omega(x).$$

Since xR is minimal submodule of M from the properties of the Möbius function we have that $\mu(0, xR) = 0 - \mu(0, 0) = -1$. Hence

$$\omega(x) = \gamma\left(\frac{|x * R| + 1}{|x * R|}\right) = \gamma\left(1 - \frac{\mu(0, xR)}{|x * R|}\right) = \mathbf{w}(x).$$

Finally let x be an arbitrary nonzero element of M and let us suppose that for each $y \in M$ such, that $yR \subsetneq xR$, we have that $\omega(y) = \mathbf{w}(y)$. Let Y denote the set $xR - x^*R$.

$$\begin{aligned}
\sum_{m \in xR} \omega(m) &= \sum_{m \in x^*R} \omega(m) + \sum_{y \in Y} \mathbf{w}(y) = |x^*R|\,\omega(x) + \sum_{y \in Y} \gamma\left(1 - \frac{\mu(0, yR)}{y^*R}\right) \\
&= |x^*R|\,\omega(x) + \gamma\,|Y| - \gamma \sum_{0 \subset yR \subsetneq xR} \left(|x^*R|\ \frac{\mu(0, yR)}{|x^*R|}\right) \\
&= |x^*R|\,\omega(x) + \gamma\,|Y| + \gamma\left(-\sum_{0 \subset yR \subsetneq xR} \mu(0, yR)\right)
\end{aligned}$$

Similarly, one of the properties of the Möbius function implies that

$$\mu(0, xR) = -\sum_{0 \subset yR \subsetneq xR} \mu(0, yR).$$

Hence

$$\gamma\,|xR| = \sum_{m \in xR} \omega(m) = |x^*R|\,\omega(x) + \gamma\,|xR - x^*R| + \gamma\mu(0, xR)$$

and we finally get that

$$\omega(x) = \gamma\frac{|xR| - |xR - x^*R| - \mu(0, xR)}{|x*^R|} = \gamma\left(1 - \frac{\mu(0, xR)}{|x^*R|}\right) = \mathbf{w}(x).$$

□

In our case M is injective module $\mathcal{I}(a)$. This module has only one simple module $S(a)$ hence socle $\mathrm{soc}(\mathcal{I}_a) = S(a)$ and as we presume $\mathcal{KQ}$ is Artinian so $S(a)$ is essential submodule. This means that every submodule N of $\mathcal{I}(a)$ contains submodule $S(a)$,

$$0 \subset S(a) \subseteq N \subseteq I(a).$$

Now we can define the Möbius function for partially ordered set of submodules of $\mathcal{I}(a)$.For our purpose (to obtain homogeneous weight) we need only values of the Möbius function with argument $(0, N)$ for all submodules N of $\mathcal{I}(a)$.

By definition $\mu(0,0) = 1$ and $\mu(0,0) + \mu(0, S(a)) = 0$, thus $\mu(0, S(a)) = -1$. For any other submodule N of $\mathcal{I}(a)$ which has to be bigger than $S(a)$ is easy to see (for example by induction on number of submodules of N) that $\mu(0, N) = 0$.

Theorem 4.4. *If we denote S^* as set of the generating elements of $S(a)$ then we can define homogeneous weight of $\mathcal{I}(a)$ by the following prescription:*

$$\omega(x) = \begin{cases} 0, & \text{for } x = 0 \\ \gamma\left(1 + \frac{1}{|S^*|}\right), & \text{for } x \in S^* \\ 1, & \text{else} \end{cases}$$

The proof of the theorem simply comes from the paragraph above. So we get that the homogeneous weight is quite similar to Hamming weight in cases of codes over injective modules $\mathcal{I}(a)$.

5. Dimension and minimal distance of linear codes over $\mathcal{I}(a)$

Now we have everything to define linear codes over path algebras and we can be curious what parameters the code will have. If we define code over $\mathcal{I}(a)$ as a submodule of $\mathcal{I}^n(a)$ then the length of the code is trivially n. Since the code is not a vector space, a dimension of the code cannot be defined properly. But we will prove that if we have a code $\mathcal{C}$ such that $\mathcal{I}^n(a)$ is a direct sum of $\mathcal{C}$ and some module N, we can get some variation on the dimension of the code $\mathcal{C}$.

We will prove that if C is a summand of $\mathcal{I}^n(a)$ then $C \cong \mathcal{I}^m(a)$ for some $m \leq n$. The value m will be called the rank of code C, then the code C contains $|I^m(a)| = |I(a)|^m$ codewords which reminds us the term of dimension in linear codes theory over finite field $\mathbb{F}_q$, where the number of codewords of code C is equal to $q^{\dim C}$.

At first we focus on indecomposable decomposition of $\mathcal{I}^n(a)$. We will use the theorem for a general module, known as the Krull-Schmidt theorem. We took it from [4] where its poof can be found.

Theorem 5.1 (Krull-Schmidt)**.** *Let M be a right $R-$module of finite length. Then M is a direct sum of indecomposable modules. The indecomposable components are uniquely determined up to isomorphism*

If we have a decomposition of module L on indecomposable modules $L_1, \ldots, L_l$ and we get two modules M and N such that $M \oplus N = L$ we get from the Krull-Schmidt theorem the decompositions $M = \oplus_{i=1}^{m} M_i$ and $N = \oplus_{i=1}^{n} N_i$ and from the uniqueness of notation we get that $(M_1, \ldots M_m, N_1, \ldots, N_n) = (L_1, \ldots, L_l)$ up to an isomorphism and a permutation.

Since the module $\mathcal{I}(a)$ is indecomposible, then as a consequence of the Krull Schmidt theorem we get that any summand of $\mathcal{I}^n(a)$ is isomorphic to $\mathcal{I}^m(a)$ for some $m \leq n$.

Definition 5.2. *Let $\mathcal{C}$ be a linear code of length n, which is a summand of $I(a)^n$ as submodule. Then the rank of the code $\mathcal{C}$ is m, where $\mathcal{C} \cong \mathcal{I}^m(a)$.*

Next we want to know when the code is a summand or how we can find out if the code is a summand or not. A trivial condition for the code to be a summand comes from the indecomposability of $I(a)$.

Lemma 5.3. *If a code $\mathcal{C}$ of length n and of rank m is a summand if $\mathcal{I}^n(a)$, then the number of codewords of $\mathcal{C}$ is equal to $|I(a)|^m$.*

Proof. Since $\mathcal{C}$ is isomorphic to $\mathcal{I}^m(a)$ from definition of rank, we get that the number of codewords is $|I^m(a)| = |I(a)|^m$. □

However the previous condition does not say whether a code is a summand, we can only find out that code is not a summand. To obtain exact condition for summands of $\mathcal{I}^n(a)$ we define the following closure operator of subsets of $\mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a))$.

Definition 5.4. *For a set $M \subset \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a))$ we define closure of M $\langle M \rangle$ by*

$$r \in \langle M \rangle \;\Leftrightarrow\; rx \in M \cup \{0\} \text{ for all } x \in \mathcal{KQ} \text{ such that } rx \in \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)).$$

A trivial fact, which comes straight from the definition of the closure, is that

$$\langle \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)) \rangle = \mathcal{I}^{\mathbf{n}}(a).$$

Before we will finally state the condition when a code is a summand of $\mathcal{I}^n(a)$, we need to focus on properties of the socle of $\mathcal{I}(a)$. We start we theorem which describe a structure of the socle. This theorem is taken from [2, p.81].

Theorem 5.5 (Socle of $\mathcal{I}(a)$)**.** *Let $\mathcal{I}(a)$ be an indecomposible injective ideal of a path algebra $\mathcal{KQ}$ for some $a \in \mathbb{Q}_0$. The simple module $S(a)$ is isomorphic to the simple socket of $\mathcal{I}(a)$.*

The simple modules $S(a)$ are defined at the beginning of Section 3.2 and hence we get that $\mathrm{soc}(\mathcal{I}(a)) \cong K$. We mention that the socle is in general case an essential module, now we get that in case of $\mathcal{I}(a)$ is even simple. It gives us that each submodule of $\mathcal{I}(a)$ contains the socle of $\mathcal{I}(a)$ as a submodule.

Theorem 5.6. *Let $\mathcal{C}$ be a code of length n. Then $\mathcal{C}$ is a summand of $\mathcal{I}^n(a)$ if and only if $\mathcal{C} = \langle \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle$.*

Proof. At first let us take an element c from $\mathcal{C}$. Since $\mathcal{C}$ is code which by definition means that $\mathcal{C}$ is $\mathcal{KQ}-$module, for each $r \in \mathcal{KQ}$ $cr \in \mathcal{C}$ as well. This implies for all $r \in \mathcal{KQ}$ that if $cr \in \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)$ then $cr \in \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)$, which is equivalent by Definition 5.4 to $c \in \langle \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle$. We get that $\mathcal{C} \subset \langle \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle$.

By Theorem 5.5 we know that the socle of $\mathcal{I}(a)$ is essential simple submodule of $\mathcal{I}(a)$. Hence $\mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \cong \mathrm{soc}^m(\mathcal{I}(a)) \cong \mathrm{soc}(\mathcal{I}^m(a)$ for some $m \leq n$. For some submodule D of $\mathrm{soc}(\mathcal{I}^n(a)$ we get that

$$\mathrm{soc}(\mathcal{I}^n(a)) = \mathrm{soc}(\mathcal{I}^m(a)) \oplus \mathrm{soc}(\mathcal{I}^{n-m}(a)) \cong \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \oplus D.$$

The trivial property of the closure operator, which we mention also above, is $\langle \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle = \mathcal{I}^{\mathbf{n}}(a)$, which holds for any $n \geq 1$. Hence

$$\mathcal{I}(a) = \langle \mathrm{soc}(\mathcal{I}^n(a)) \rangle = \langle \mathrm{soc}(\mathcal{I}^m(a)) \rangle \oplus \langle \mathrm{soc}(\mathcal{I}^{n-m}(a)) \rangle \cong \langle \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle \oplus \langle D \rangle,$$

which gives us that $\langle \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle$ is a summand of $\mathcal{I}^n(a)$. Trivially we get that if $\mathcal{C} = \langle \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle$ then $\mathcal{C}$ is a summand as well.

Finally let us assume that $\mathcal{C} \subsetneq \langle \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle$ and let c be an element from $\langle \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle - \mathcal{C}$. From the definition of the closure we get that there exist $r \in \mathcal{KQ}$ such that $cr \in \mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)$ and hence $cr \in \mathcal{C}$. Now let us suppose that the code $\mathcal{C}$ is a summand of $\mathcal{I}^n(a)$ so there exists some submodule D of $\mathcal{I}^n(a)$ such that $\mathcal{I}^n(a) = \mathcal{C} \oplus D$ and $\mathcal{C} \cap D = \{0\}$. Since $c \notin C$ there must hold that $c \in D$. The fact D is module implies that $cr \in D$ but we mentioned above $cr \in C$ as well, which gives us contradiction with properties of direct summands and hence $\mathcal{C}$ is not a summand. □

The previous proof gives us a method how we prove that the code is a summand. If we know that C is a summand and we only want to compute its rank we use the following procedure. Since in our situation the socle of $\mathcal{I}$ is an essential module and for direct sum holds that $\mathrm{soc}(\mathcal{I}^n) = \mathrm{soc}(\mathcal{I})^n$, we get that $\mathrm{soc}(C) \subset \mathrm{soc}(\mathcal{I})^n$ and since $\mathrm{soc}(\mathcal{I})$ is a simple module there is some m such that $\mathrm{soc}(C) \cong \mathrm{soc}(\mathcal{I})^m$. From essentiality of $\mathrm{soc}(\mathcal{I})$ and the fact that C is a summand of $\mathcal{I}$ we finally get that $C \cong \mathcal{I}^m$.

The minimal distance of a code $\mathcal{C}$ can be computed as minimal Hamming weight of codeword since $\mathcal{C}$ is assumed be linear. But we can transfer the computation to socle of code since the following theorem from [5, p.258] holds.

Theorem 5.7. *Let $\mathcal{C}$ be a linear code over $\mathcal{I}(a)$ of length n than $\mathrm{soc}(\mathcal{C})$ is code over $\mathcal{I}(a)$ and for the Hamming minimal distance $\mathbf{d}$ of $\mathcal{C}$, we have the equality*

$$\mathbf{d}(\mathcal{C}) = \mathbf{d}(\mathrm{soc}(\mathcal{C})).$$

5.1 Bounds on number of codewords

The method from the previous section will not give us rank of a code in all cases, it is more probable that randomly chosen code will not be a summand. In these cases we have to suffice with the number of codewords. Now we get all the parameters and we would like to know, whether the code is optimal, which means whether there is no code with better parameters. Traditionally we get a length $\mathbf{n}$ and a minimal distance $\mathbf{d}$ and we ask how many codewords the code with length n and minimal Hamming distance d can have .

In the theory of codes over field $\mathbb{F}_q$ there are many of these bounds. Let us denote $A_q(\mathbf{n}, \mathbf{d})$ a maximal number of words that a code of length $\mathbf{n}$ over $\mathbb{F}_q$ with minimum Hamming distance $\mathbf{d}$ can have. The first bound is called Singleton bound and states that

$$A_q(\mathbf{n}, \mathbf{d}) \leq q^{\mathbf{n}+1-\mathbf{d}}$$

If we denote $\alpha = \frac{q-1}{q}$ and assume that $\alpha\mathbf{n} < \mathbf{d}$ then the Plotkin bound holds. It says that

$$A_q(\mathbf{n}, \mathbf{d}) \leq \frac{\mathbf{d}}{\mathbf{d} - \alpha\mathbf{n}}$$

Now we denote $\mathrm{vol}_q(\mathbf{n}, t)$ the volume of the sphere of radius t in the space $F_q^{\mathbf{n}}$ and it is easy to prove that

$$\mathrm{vol}_q(\mathbf{n}, t) = \sum_{i=0}^{t} \binom{\mathbf{n}}{i} (q-1)^i.$$

An extensive refinement of the Plotkin bound, the Elias bound says that for every $t \in \mathbb{R}$ with $t < \alpha\mathbf{n}$ and $t^2 - 2t\alpha\mathbf{n} + \mathbf{d}\alpha\mathbf{n} > 0$ it holds

$$A_q(\mathbf{n}, \mathbf{d}) \leq \frac{\alpha\mathbf{n}\mathbf{d}}{t^2 - 2t\alpha\mathbf{n} + \mathbf{d}\mathbf{n}\alpha} \cdot \frac{q^{\mathbf{n}}}{\mathrm{vol}_q(\mathbf{n}, t}.$$

The previous bounds can be found with their proofs in [10].

Of course there were studies whether these bounds can be stated for codes over rings especially Frobenius rings. It is also clear that we need to generalize these bounds for weight functions that differ from the Hamming weight. We will focus on homogeneous weight as we did in the previous chapters. Let R be a finite Frobenius ring and let ω be a homogeneous weight on R of average value γ. We denote $A_{hom}(\mathbf{n}, \mathbf{d})$ the maximal number of codewords of a code of length $\mathbf{n}$ over R with minimum homogeneous distance $\mathbf{d}$ and $\mathrm{vol}_\omega(\mathbf{n}, t)$ the volume of the sphere of homogeneous radius t in the space $R^{\mathbf{n}}$.

Then we can state the Plotkin bound

$$A_{hom}(\mathbf{n}, \mathbf{d}) \leq \frac{\mathbf{d}}{\mathbf{d} - \gamma\mathbf{n}}$$

and the Elias bound

$$A_{hom}(\mathbf{n}, \mathbf{d}) \leq \frac{\gamma\mathbf{nd}}{t^2 - 2t\alpha\mathbf{n} + \mathbf{dn}\gamma} \cdot \frac{|R|^{\mathbf{n}}}{\mathrm{vol}_q(\mathbf{n}, t)}.$$

Both these bounds are studied in [6] by Marcus Greferath and Michael E. O'Sullivan.

6. Dual codes over $\mathcal{I}(a)$

Since we defined the bilinear form on $\mathcal{I}(a) \otimes \mathcal{I}(a)$ we should look at the dual codes of codes over $\mathcal{I}(a)$.

Definition 6.1. *For a code $\mathcal{C} \leq \mathcal{I}(a)^{\mathbf{n}}$ we define the dual code*

$$\mathcal{C}^{\perp} = \{x \in \mathcal{I}(a) \mid \beta(c, x) \text{ for all } c \in \mathcal{C}\}$$

where β is the bilinear form defined in the Chapter 4.

From the definition of the bilinear form β and the choice of $\mathcal{A}$ with multiplication by elements of $\mathcal{KQ} \otimes \mathcal{KQ}$ it is easy to see that $\mathcal{C}^{\perp}$ is indeed a code since if $\beta(c, d) = 0$ then for all $x \in \mathcal{KQ}$ $\beta(c, dx) = \beta(c, d)(1, x) = 0$ as well.

After definition of the dual code there arises question whether the codes over $\mathcal{I}(a)$ are closed which means whether $\mathcal{C} = \mathcal{C}^{\perp\perp}$. The answer is "no" in general case but we will prove that there is a simple condition for a code to be closed. First we state and prove a theorem about structure of dual codes.

Theorem 6.2. *Let $\mathcal{C}$ be a linear code of length $\mathbf{n}$ then code $\mathcal{C}^{\perp}$ is a summand of $\mathcal{I}(a)^{\mathbf{n}}$.*

Proof. To prove this theorem we use the closure operator defined in the Definition 5.4. From the proof of the Theorem 5.6 we get that for every code $\mathcal{C} \leq \mathcal{I}^n(a)$ the set $\langle \mathcal{C} \cap \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle$ is a summand of $\mathcal{I}^n(a)$ and $\mathcal{C} \subset \langle \mathcal{C} \cap \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle$. So all we need to prove is the inequality $\langle \mathcal{C}^{\perp} \cap \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle \subset \mathcal{C}^{\perp}$, then the equality $\langle \mathcal{C}^{\perp} \cap \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a) \rangle = \mathcal{C}^{\perp}$ implies that $\mathcal{C}^{\perp}$ is a summand of $\mathcal{I}^n(a)$.

We assume that $r \in \langle \mathcal{C}^{\perp} \cap \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a)) \rangle$. The assumption of $r \in \langle \mathcal{C}^{\perp} \cap \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a)) \rangle$ gives us that for $y \in \mathcal{KQ}$ there holds that if $ry \in \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a))$ then $ry \in \mathcal{C}^{\perp} \cap \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a))$ which implies that $ry \in \mathcal{C}^{\perp}$. Let us suppose that $r \notin \mathcal{C}^{\perp}$ so there exists $d \in \mathcal{C}$ such that $\beta(d, r) \neq 0$ where $0 \in \mathcal{A}_{\mathcal{KQ} \otimes \mathcal{KQ}}$. Since $1 = \sum_{b \in Q_0} \epsilon_b$ in $\mathcal{KQ}$ there exists a point $b \in Q_0$ such that $\beta(d, r\epsilon_b) \neq 0$. From definition of $\mathcal{I}(a)$ in Theorem 3.11 we get that $r\epsilon_b$ is element of dual space to vector space $\epsilon_b \mathcal{KQ} \epsilon_a$, let $\gamma \in \epsilon_b \mathcal{KQ} \epsilon_a$ is one of its basis vector for which $r\epsilon_b \gamma \neq 0$. Since $r\epsilon_b \neq 0$ there has to exist such γ. As $r\epsilon_b \gamma \neq$ we get that $r\epsilon_b \gamma = k\epsilon_a^*$ for $k \in \mathcal{K} - \{0\}$ and so $r\epsilon_b \gamma \in \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a))$. From definition of multiplication of $\mathcal{A}$ by basis elements of $\mathcal{KQ} \otimes \mathcal{KQ}$ we know that $\beta(d, r\epsilon_b \gamma) = \beta(d, r)(1, \epsilon_b \gamma) = \beta(d, r)(1, \gamma) \neq 0$ since $\beta(d, r) \neq 0$. This implies that $r\epsilon_b \gamma \notin \mathcal{C}^{\perp}$ what gives us contradiction with our original assumption of $r \in \langle \mathcal{C}^{\perp} \cap \operatorname{soc}(\mathcal{I}^{\mathbf{n}}(a)) \rangle$.

□

Now we can state the theorem about condition for closed codes.

Theorem 6.3. *A code $\mathcal{C}$ of length $\mathbf{n}$ is closed if and only if $\mathcal{C}$ is a summand of $\mathcal{I}(a)^{\mathbf{n}}$.*

Proof. From the previous theorem we know that dual code is a summand of $\mathcal{I}(a)^{\mathbf{n}}$ so $\mathcal{C}^{\perp\perp}$ is also a summand, hence if code $\mathcal{C}$ is not a summand then $\mathcal{C} \neq \mathcal{C}^{\perp\perp}$.

Now we need to prove that if $\mathcal{C}$ is a summand of $\mathcal{I}(a)^{\mathbf{n}}$ then the code $\mathcal{C}$ is closed. A trivial general property of dual codes is $\mathcal{C} \leq \mathcal{C}^{\perp\perp}$. Since we assume

that $\mathcal{C}$ is a summand of $\mathcal{I}(a)$, there exists $m \leq \mathbf{n}$ that $\mathcal{C} \cong \mathcal{I}(a)^m$. Hence $\mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)) \cong \mathcal{K}^m$ and by a value of dimension of dual code over field we get that

$$\mathcal{C}^{\perp} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)) \cong \mathcal{K}^{\mathbf{n}-m}$$

. Using this property once more we finally get that

$$\mathcal{C}^{\perp\perp} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)) \cong \mathcal{K}^m$$

and since $\mathcal{C}^{\perp\perp}$ is a summand of $\mathcal{I}(a)^{\mathbf{n}}$ by Theorem 6.2 then $\mathcal{C}^{\perp\perp} \cong \mathcal{I}(a)^m$. Now we summarize our results. We know that $\mathcal{C} \leq \mathcal{C}^{\perp\perp}$ and $\mathcal{C} \cong \mathcal{C}^{\perp\perp}$ which implies $\mathcal{C} = \mathcal{C}^{\perp\perp}$. □

6.1 MacWilliams Identity

After definition of the duality we will focus on variation of MacWilliams identity theorem. Since we will use the version for the complete weight enumerator, where a generating character plays a significant role, we have to start studying characters over $\mathcal{I}(a)$.

Let M be a union over points $b \in Q_0$ of sets of the basis vectors of duals $I(a)_b$ from representation $\mathcal{I}(a)$ as we defined in Theorem 3.11. This set is $\mathcal{K}-$generating set of $\mathcal{I}(a)$ which means that each element of $\mathcal{I}(a)$ is $\mathcal{K}-$linear combination of elements from M. According the general definitions of characters for each element β^* of M we define a character χ_{β^*} as

$$\chi_{\beta^*}(x) = \begin{cases} \zeta, & \text{for } x = \beta^* \\ 1, & \text{for } x \neq \beta^*, \end{cases}$$

where ζ is primitive p^{th} complex root of unity and p is characteristic of field $\mathcal{K}$. If it is not clear, we assume the complex characters. Since characters are group homomorphisms we can extend χ_{β^*} on the whole $\mathcal{I}(a)$ by rule

$$\chi_{\beta^*}(x + y) = \chi_{\beta^*}(x) + \chi_{\beta^*}(y).$$

Then we define a character χ_{γ^*} for general element γ^* of $\mathcal{I}(a)$, which has the form $\gamma^* = \sum_{\beta^* \in M} k_{\beta^*}\beta^*$ where $k_{\beta^*} \in \mathcal{K}$, by

$$\chi_{\gamma^*}(x) = \sum_{\beta^* \in M} k_{\beta^*}\chi_{\beta^*}(x).$$

From [5, p.253] we get that there can be defined a left multiplication on the set of all characters of $\mathcal{I}(a)$ by elements from $\mathcal{I}(a)$. If we define the multiplication for elements of M then by $\mathcal{K}-$linearity of $\mathcal{I}(a)$ and the set of characters we can obtain the multiplication by general element of $\mathcal{I}(a)$. Let β^* be a element of M and let β be the element of $\mathcal{KQ}$ such that β^* is dual to basis elements β of vector space $\mathbf{s}(\beta)\mathcal{KQ}\mathbf{t}(\beta)$ where $\mathbf{s}, \mathbf{t}$ are source and target functions from the Definition of quiver 2.1. Similarly we have $\gamma^* \in M$ and its dual γ. Then

$$\beta^*\chi_{\gamma^*}(x) = \chi_{\delta^*}(x)$$

for δ^* which is a dual to $\beta\gamma \in \mathcal{KQ}$. Since $M \subset I(a)$ contains only the duals of the path with target a we easily get that for $\beta^*, \gamma^* \in M$

$$\beta^*\chi_{\gamma^*}(x) = \begin{cases} \chi_{\beta^*}(x), & \text{for } \gamma^* = \epsilon_a^* \\ \chi_0(x) = 0, & \text{else .} \end{cases}$$

Hence $\chi_{\epsilon_a^*}$ is so called a generating character of $\mathcal{I}(a)$ which means that $\mathcal{I}(a)\chi_{\epsilon_a^*} = \mathcal{I}(a)^\chi$ where $\mathcal{I}(a)^\chi$ denotes the set of all characters of $\mathcal{I}(a)$. Now we can state the theorem which is variation of MacWilliams identity for complete weight enumerator.

Theorem 6.4. *Let $\mathcal{I}(a)$ be an injective indecomposable $\mathcal{KQ}-$module with a bilinear form β which defines the duality of codes over $\mathcal{I}(a)$. Let $\mathcal{C} \leq \mathcal{I}(a)^{\mathbf{n}}$ be a linear code with complete weight enumerator* $\mathrm{cwe}_{\mathcal{C}}(\mathbf{x})$. *Then the complete weight enumerator of $\mathcal{C}^\perp$ is given by*

$$\mathrm{cwe}_{\mathcal{C}}^{\perp}(\mathbf{x}) = \frac{1}{|\mathcal{C}|}\,\mathrm{cwe}_{\mathcal{C}}(M\mathbf{x})$$

where M is the matrix with entry $M_{i,j} = \chi_{\epsilon_a^*}(ij)$.

The character $\chi_{\epsilon_a^*}$ is a generating character of $\mathcal{I}(a)$, it is the reason why is chosen for definition of the matrix M. Since $\mathcal{I}(a)$ is module over $\mathcal{KQ}$ there is no multiplication of two elements of $\mathcal{I}(a)^\chi$ but since $\mathcal{I}(a)$ has the structure of right $\mathcal{KQ}-$module we can define left multiplication of $\mathcal{I}(a)^\chi$ by elements of $\mathcal{I}(a)$ as

$$\chi(\gamma\delta) = \delta\chi(\gamma).$$

The proof of this theorem can be found in [15]. The proof is quite complicated and for the purpose of this thesis it is more important the theorem. For an illustration we give an example.

Example. *We consider $\mathcal{I}(0)$ for Dynkin quiver A_2 over field $\mathcal{K} = \mathbb{Z}_2$. Hence the elements of $\mathcal{I}(a)$ are $\{0, \epsilon_a^*, \alpha^*, \epsilon_a^* + \alpha^*\}$. For easier notation we denote $\epsilon_a^* = e, \alpha^* = a$. Then we have four characters with values by the following table.*

$\chi_i(j)$	*0*	*e*	*a*	*e+a*
0	*1*	*1*	*1*	*1*
e	*1*	*-1*	*1*	*-1*
a	*1*	*1*	*-1*	*-1*
e+a	*1*	*-1*	*-1*	*1*

From the table we obtain the matrix M with entries $M_{i,j} = \chi_e(ij)$ using that $\chi_e(ij) = j\chi_e(i) = \chi_j(i)$.

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Now for the code $\mathcal{C} = \{0000, 0a0a, aaa0, a0aa, 0e0e, eee0, e0ee, 0b0b, bbb0, b0bb, aeab, abae, eaeb, ebea, babe, beba\}$ which is a summand of dimension 2 and where b denotes $e + a = \epsilon_0^* + \alpha^*$ we have complete weight enumerator

$$\mathrm{cwe}_{\mathcal{C}}(\mathbf{x}) = x_0^4+x_0^2x_a^2+x_0^2x_e^2+x_0^2x_b^2+2x_0x_a^3+2x_0x_e^3+2x_0x_b^3+2x_ax_ex_b^2+2x_ax_e^2x_b+2x_a^2x_ex_b.$$

$\mathrm{cwe}_{\mathcal{C}^\perp}(x_0, x_e, x_a, x_b) = \frac{1}{16}\,\mathrm{cwe}_C(M(x_0, x_e, x_a, x_b)^T)$
$= \frac{1}{16}\,\mathrm{cwe}_C(x_0 + x_e + x_a + x_b, x_0 - x_e + x_a - x_b, x_0 + x_e - x_a - x_b, x_0 - x_e - x_a + x_b)$
$= x_0^4 + x_0^2x_a^2 + x_0^2x_e^2 + x_0^2x_b^2 + 2x_0x_a^3 + 2x_0x_e^3 + 2x_0x_b^3 + 2x_ax_ex_b^2 + 2x_ax_e^2x_b + 2x_a^2x_ex_b$

which is indeed a complete weight enumerator of $\mathcal{C}^\perp$ *since* $\mathcal{C}^\perp = \{0000, a0a0, 0aaa, aa0a, e0e0, 0eee, ee0e, b0b0, 0bbb, bb0b, baea, eaba, beae, aebe, ebab, abeb\}$.

7. Equivalence of codes

In this chapter we will focus on a modification of the MacWilliams equivalence theorem for linear codes over path algebras equipped with homogeneous weight. We start with a definition of monomial transformation and then we define an equivalence of codes.

Definition 7.1 (Monomial Transformation on $\mathcal{I}^n(a)$)**.** *The monomial transformation over $\mathcal{I}(a)$ is called each function $f : \mathcal{I}^n(a) \to \mathcal{I}^n(a)$ which is the form*

$$f(x_1, \ldots, x_{\mathbf{n}}) = \left(f_1\left(x_{\sigma(1)}\right), \ldots, f_n\left(x_{\sigma(\mathbf{n})}\right)\right),$$

where σ is a permutation from $S(n)$ and $f_1, \ldots, f_n$ are $\mathcal{KQ}-$automorphisms of $\mathcal{I}(a)$.

Definition 7.2. *Two linear coded $\mathcal{C}, \mathcal{C}'$ over $\mathcal{I}(a)^{\mathbf{n}}$ are equivalent when there exists a monomial transformation $\varphi : \mathcal{I}(a)^{\mathbf{n}} \to \mathcal{I}(a)^{\mathbf{n}}$ taking $\mathcal{C}$ to $\mathcal{C}'$, $\varphi(\mathcal{C}) = \mathcal{C}'$.*

For a better understanding to monomial transformations we should now focus on the form of $\mathcal{KQ}-$ automorphisms of $\mathcal{I}(a)$. Let f be a $\mathcal{KQ}-$automorphism on $\mathcal{I}^n(a)$ and let $\beta_1^*, \ldots, \beta_p^*$ denote all elements of $\mathcal{I}(a)$ such that β_i is a basis vector of $\mathcal{KQ}$ for all $i = 1, \ldots, p$. Then for each element x of $\mathcal{I}(a)$ holds

$$x = x\left(\epsilon_1 + \ldots + \epsilon_m\right) = x\epsilon_1 + \ldots + x\epsilon_m = k_1\beta_1^* + \ldots k_p\beta_p^*, \tag{7.1}$$

where k_i are taken from $\mathcal{K}$ and $\epsilon_1, \ldots, \epsilon_m$ are all trivial (stationary) paths in $\mathcal{Q}$. Now we suppose that β_j has as its source the point b and as its target point a and $f(\beta_j^*) = x$ for $x \in \mathcal{I}^n(a)$. From the $\mathcal{KQ}-$linearity of f we get that

$$f(\beta_j^*\epsilon_i) = f(\delta_{ib}(\beta_j^*)) = \delta_{ib}\left(f(\beta_j^*)\right) = \delta_{ib}(x)$$

where δ is again the Kronecker delta. Hence, in the decomposition by 7.1 of $\omega\left(\beta_j^*\right) = x$ the only nonzero coefficients are by the elements β_i^* such that the source of β_i is b. This implies that x is a element of dual space to vector space $\epsilon_b\mathcal{KQ}\epsilon_a$. Using the $\mathcal{KQ}-$linearity of f once more we get

$$x\beta_i = f(\beta_j^*)\beta_j = f(\beta_j^*\beta_i) = f(\delta_{ij}(\epsilon_a^*) = \delta_{ij}\left(f(\epsilon_a)\right)$$

because of f is isomorphism $f(\epsilon_a) \neq 0$. Hence the only one nonzero coefficient in the decomposition of x is k_j by the element β_j^*. Since $f(\beta_j^*) = k_j\beta_j^*$.

We got that for any element β_j^* from $\mathcal{I}^n(a)$ the $\mathcal{KQ}-$automorphism f satisfy $f(\beta_j^*) = k_j\beta_j^*$. By $\mathcal{KQ}-$linearity we get that

$$f(\epsilon_a^*) = f(\beta_j^*\beta_j) = k_j\beta_j^*\beta_j = k_j\epsilon_a^*.$$

Hence the automorphism has the form $f(x) = k_i x$ for some nonzero k_i from field $\mathcal{K}$.

Theorem 7.3 ($\mathcal{KQ}-$automorphisms of $\mathcal{I}(a)$)**.** *Let f be a $\mathcal{KQ}-$automorphism then there exists nonzero k from $\mathcal{K}$ such that $f(x) = kx$.*

Since the socle of $\mathcal{I}(a)$ is an essential simple module of $\mathcal{I}(a)$, any module generated by elements of $\mathcal{I}(a)$ over $\mathcal{KQ}$ contains the socle as a submodule, especially one generated modules. Hence for every $x \in \mathcal{I}(a)$ there exists $r \in \mathcal{KQ}$ such that xr lies in $\mathrm{soc}(\mathcal{I}(a))$ and $xr \neq 0$. This is an important fact and it will help us to prove the following lemma.

Lemma 7.4. *Let $\mathcal{C}$ be a code over $\mathcal{I}(a)$ of length $\mathbf{n}$. Let $\mathcal{D}$ denotes $\mathcal{C} \cap \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)) = \mathcal{C} \cap \mathrm{soc}^{\mathbf{n}}(\mathcal{I}(a))$. Then $\mathcal{D} \leq \mathcal{C}$ is also code over $\mathcal{I}(a)$ of length $\mathbf{n}$, and for each codeword $c \in \mathcal{C}$ and for each coordinate i holds that if $c_i \neq 0$ then there exists $d \in \mathcal{D}$ such that $d_i \neq 0$ as well.*

Proof. Since $\mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a)) = \mathrm{soc}^{\mathbf{n}}(\mathcal{I}(a))$ is module over $\mathcal{KQ}$, $\mathcal{D}$ is a code trivially. The second part of the lemma comes from paragraph right above the lemma. □

Now we focus on the equivalency theorem.

Theorem 7.5. *Let $\mathcal{C}_1, \mathcal{C}_2$ be two linear codes over $\mathcal{I}(a)$, which are summands of $\mathcal{I}^n(a)$. These codes are equivalent if and only if there exists a $\mathcal{KQ}-$linear isomorphism $f : \mathcal{C}_1 \to \mathcal{C}_2$ preserving the homogeneous weight.*

Proof. Since a monomial transformation is $\mathcal{KQ}-$automorphism of $\mathcal{I}^n(a)$ and preserves the homogeneous weight then the straight implication is clear.

We assume that for codes $\mathcal{C}_1, \mathcal{C}_2$ we have $\mathcal{KQ}-$isomorphism φ preserving the homogeneous weight. We intersect each code with socle of $\mathcal{I}(a)^n$ to obtain codes $\mathcal{D}_1$ (resp. $\mathcal{D}_2$) as in the previous Lemma 7.4. Let us assume that $\varphi(\mathcal{D}_1) \neq \mathcal{D}_2$ it means that there exists $d \in \mathcal{D}_1$ such that $\varphi(d) = c \notin D_2 \subset \mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a))$. As $0 \in \mathrm{soc}(\mathcal{I}^n(a))$ and $c = c\,(\epsilon_1 + \ldots + \epsilon_n)$, then there exists a point j from $\mathcal{Q}$ such that $c\epsilon_j \neq 0$. Since for each element x from $\mathcal{I}(a)$ there holds that $x\epsilon_a \in \mathrm{soc}(I(a))$, there exists a point $i \neq a$ such that $c\epsilon_i \neq 0$. We also know that for y an element of socle $\mathcal{I}(a)$ $y\epsilon_a = y$ which implies that $y\epsilon_i = 0$ for $i \neq a$. This gives us that $\varphi(d\epsilon_i) = \varphi(0) = c\epsilon_i \neq 0$ which is contradiction with the $\mathcal{KQ}-$linearity of φ.

Hence $\varphi(\mathcal{D}_1) = \mathcal{D}_2$ and we can restrict the isomorphism φ on $\mathcal{D}_1$ to get an isomorphism $\phi : \mathcal{D}_1 \to \mathcal{D}_2$. Since $\mathrm{soc}(\mathcal{I}(a))^{\mathbf{n}} \cong \mathcal{K}^n$ and $\mathcal{D}_1$ and $\mathcal{D}_2$ lies in $\mathrm{soc}(\mathcal{I}(a))^{\mathbf{n}}$ there exist linear codes $\mathcal{L}_1, \mathcal{L}_2$ over $\mathcal{K}$ equipped with Hamming weight which are isomorphic to $\mathcal{D}_1, \mathcal{D}_2$ respectively and there exists isomorphism $\phi_{\mathcal{K}} : \mathcal{L}_1 \to \mathcal{L}_2$ induced by isomorphism ϕ. Since homogeneous weight is constant on nonzero elements of socle of $\mathcal{I}(a)$ there is no problem in transition to Hamming weight. From the MacWilliams equivalence theorem we get that for isomorphism $\phi_{\mathcal{K}}$ there exists a monomial transformation $\eta_{\mathcal{K}} : \mathcal{K}^{\mathbf{n}} \to \mathcal{K}^{\mathbf{n}}$ such that $\eta_{\mathcal{K}}(\mathcal{L}_1) = \mathcal{L}_2$ and its form is

$$\eta_K\,(x_1, \ldots, x_{\mathbf{n}}) = \left(x_{\sigma(1)}k_1, \ldots, x_{\sigma(\mathbf{n})}k_{\mathbf{n}}\right)$$

for $k_1, \ldots, k_{\mathbf{n}}$ from $\mathcal{K}$ and the permutation $\sigma \in S_{\mathbf{n}}$. Now we go back to codes $\mathcal{D}_1$ and $\mathcal{D}_2$. Because of isometry between $\mathrm{soc}(\mathcal{I}^{\mathbf{n}}(a))$ and $\mathcal{K}^{\mathbf{n}}$ we get monomial transformation $\eta_{socle} : \mathrm{soc}(\mathcal{I}(a)^{\mathbf{n}}) \to \mathrm{soc}(\mathcal{I}(a)^{\mathbf{n}})$ such that $\eta_{socle}(\mathcal{D}_1) = \mathcal{D}_2$ and its form is the same as $\eta_{\mathcal{K}}$.

The last step is an extension of η_{socle} on the entire $\mathcal{I}(a)^{\mathbf{n}}$. As we can see the monomial transformation η_{socle} has the form of a monomial transformation on $\mathcal{I}^n(a)$ since the $\mathcal{KQ}$ isomorphism of $\mathcal{I}(a)$ are form kx, according the Theorem 7.3. So we would like to prove that η_{socle} is in fact the required monomial trasnformarion of $\mathcal{I}^n(a)$.

Since $\mathrm{soc}(\mathcal{I}^n(a)) \cong K^n$ we can see codes $\mathcal{D}_1$ and $\mathcal{D}_2$ as $\mathcal{K}-$subspaces of $\mathrm{soc}(\mathcal{I}^n(a))$. Let $u_1, \ldots, u_s$ be a basis of $\mathcal{D}_1$ and let $v_1, \ldots, u_t$ be a basis of $\mathcal{D}_2$. Since there exists isomorphism between $\mathcal{D}_1$ and $\mathcal{D}_2$ then $t = s$ and let us suppose that $\eta_{socle}(u_i) = v_i$ for each i. Using the closure operator from Definition 5.4 we easily get

$$\mathcal{C}_1 \subset \langle u_1 \rangle \oplus \ldots \oplus \langle u_s \rangle \quad \mathcal{C}_2 \subset \langle v_1 \rangle \oplus \ldots \oplus \langle v_s \rangle.$$

Generally there holds

$$\mathcal{C}_1 \supseteq (\mathcal{C}_1 \cap \langle u_1 \rangle) \oplus \ldots \oplus (\mathcal{C}_1 \cap \langle u_s \rangle)$$

respectively for $\mathcal{C}_2$. As we assumes the codes $\mathcal{C}_1, \mathcal{C}_2$ are summands, which implies by the Theorem 5.6 that $\mathcal{C}_1 \cap \langle u_i \rangle = \langle u_i \rangle$ for u_i from $\mathrm{soc}(\mathcal{C}_1) = \mathcal{D}_1$, respectively for $\mathcal{C}_2$. Hence we get that

$$\mathcal{C}_1 = \langle u_1 \rangle \oplus \ldots \oplus \langle u_s \rangle \quad \mathcal{C}_2 = \langle v_1 \rangle \oplus \ldots \oplus \langle v_s \rangle.$$

We can suppose that η_{socle} is identity on $\mathrm{soc}(\mathcal{I}^n(a))$ so $u_i = v_i$ for each i and then there is trivial identity $\mathcal{KQ}-$isomorphism between $\langle u_i \rangle$ and $\langle v_i \rangle$. Now we can each element of C_1 decompose on the sum $c = w_1 + \ldots + w_s$, where w_i lies in $\mathcal{C}_1 \cap \langle u_i \rangle$ and we know that w_i lies in $\mathcal{C}_2 \cap \langle u_i \rangle$ as well, hence c lies also in $\mathcal{C}_2$ by properties of modules. We get that if we define $\eta : \mathcal{I}^n(a) \to \mathcal{I}^n(a)$ as identity then η is trivially a monomial transformation and $\eta(C_1) = C_2$. We see that the extension of η_{socle} on $\mathcal{I}^n(a)$ is equal to η_{socle}, so if η_{socle} is not identity, the situation is not more complicated since η has the same form as η_{socle}. □

The situation when the codes are not summands is more difficult since the permutation is not uniquely determined. It may happen that we cannot obtain the monomial transformation η from η_{socle} as the following example shows.

Example. *We use simple A_1 quiver with binary field $\mathbb{F}_2$, then $\mathcal{I}(0)$ has elements $0, \beta_0^*, \beta_1^*, \beta_0^* + \beta_1^*$. Let us denote the elements as $a = \beta_0^*$,$b = \beta_1^*$ and $c = \beta_0^* + \beta_1^*$. The codes are $C_1 = \{0000, 0101, 1110, 1011, 2220, 3330, 3231, 1213\}$ and $C_2 = \{0000, 0101, 1011, 1110, 2022, 3033, 3132, 1312\}$.*

The $\mathcal{KQ}-$isomorphism preserving the homogeneous weight is obvious and the monomial transformation is easy to find as well, since the $\mathcal{KQ}-$isomorphisms used in the monomial transformation have to be identities because we are in the binary field. So we need to find only the permutation.

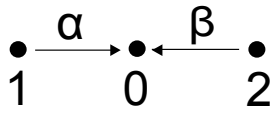
The codes $\mathcal{D}_1$ and $\mathcal{D}_2$ are the same and their elements are $\{0000, 0101, 1110, 1011\}$. Since they are the same we can take the required permutation as the identity. However the monomial transformation with trivial permutation and trivial $\mathcal{KQ}-$automorphism of $\mathcal{I}(a)$ does not meet the requirement of equality $\eta(C_1) = C_2$.

However as we can see the permutation $(2, 4)$ is the permutation, which gives us the required monomial transformation.

Generally for codes which are not summands, we cannot say whenever the obtained monomial transformation η_{socle} can be extended on the entire $\mathcal{I}^n(a)$. The general proof for Frobenius rings from [15] assumes only commutative rings so it cannot be use in this case as well.

At the following example shows that using $\mathcal{KQ}-$isomorphism for equivalence of codes would not be the best choice.

Example. *Let $\mathcal{K}$ be the binary field $\mathbb{F}_2$ and $\mathcal{Q}$ be a quiver*



then the elements of $\mathcal{I}(0)$ have form $k_0\epsilon_0^* + k_1\alpha^* + k_2\beta^*$ for $k_0, k_1, k_2 \in K$. From the properties of multiplication in $\mathcal{I}(a)$ by element of $\mathcal{KQ}$ we know that there is no such r in $\mathcal{KQ}$ that $\alpha^* r = \beta^*$.

Now we assume two codes over $\mathcal{I}(a)$ of length 1 to avoid doubts about potential influence of permutation of coordinates. We denote them $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ such that $\mathcal{C}_\alpha = \{0, \epsilon_0^*, \alpha^*, \epsilon_0^* + \alpha^*\}$ and $\mathcal{C}_\beta = \{0, \epsilon_0^*, \beta^*, \epsilon_0^* + \beta^*\}$. It is obvious that the map ω defined by

$$\begin{aligned} \omega(0) &= 0 \\ \omega(\epsilon_0^*) &= \epsilon_0^* \\ \omega(\alpha^*) &= \beta^* \\ \omega(\epsilon_0^* + \alpha^*) &= \epsilon_0^* + \beta^* \end{aligned}$$

is $\mathcal{K}-$isomorphism preserving the homogeneous weight. If there exists some monomial transformation φ it has to have a form $\varphi(x) = kx$ where k is a element of $\mathcal{K}$ but as we mention before $\beta^* \notin \alpha^*\mathcal{KQ}$ not even in $\alpha\mathcal{K}$ what implies that there is no monomial transformation such that $\varphi(C_\alpha) = C_\beta$.

With this result we should change the definition of equivalence of codes since the codes from the example above should be equivalent as they distinguish only in a choice of character from the alphabet $\mathcal{I}(a)$. If we change the definition of monomial transformation such that we require $\mathcal{K}-$isomorphisms instead of $\mathcal{KQ}-$isomorphisms then the codes from the previous example will be equivalent.

Definition 7.6 ($\mathcal{K}-$linear Monomial Transformation on $\mathcal{I}^n(a)$)**.** *The $\mathcal{K}-$linear monomial transformation over $\mathcal{I}(a)$ is called each function $f : \mathcal{I}^n(a) \to \mathcal{I}^n(a)$ which is the form*

$$f(x_1, \ldots, x_{\mathbf{n}}) = \left(f_1\left(x_{\sigma(1)}\right), \ldots, f_n\left(x_{\sigma(\mathbf{n})}\right)\right),$$

where σ is a permutation from $S(n)$ and $f_1, \ldots, f_n$ are $\mathcal{K}-$automorphisms of $\mathcal{I}(a)$ which preserves the homogeneous weight.

On the other side there is no variation on the Theorem 7.5 for $\mathcal{K}-$isomorphism between two codes. The following example shows that there may not be a $K-$linear monomial transformation for two $K-$isomorphic codes.

Example. *We assume the Dynkin quiver A_1 over binary field $\mathbb{F}_2$. As in the Example 7 we denote the elements of $\mathcal{I}(0)$ $0, a, b$ and c. The values of homogeneous weight of elements of $\mathcal{I}(0)$ are*

$$\omega_{hom}(0) = 0, \quad \omega_{hom}(a) = 2, \quad \omega_{hom}(b) = 1, \quad \omega_{hom}(c) = 1 \tag{7.2}$$

If we take codes $C_1 = \{00, aa, 0a, a0\}$ and $C_2 = \{00, aa, bb, cc\}$ then there exists $K-$isomorphism between C_1 and C_2 which preserves the homogeneous weight. The prescription of this isomorphism is

$$f(0,0) = (0,0), \quad f(a,a) = (a,a), \quad f(b,b) = (a,0), \quad f(c,c) = (0,a). \tag{7.3}$$

It is easy to see that there is no $K-$linear monomial transformation which maps C_1 onto C_2.

We get two possibilities how we can see the equivalence of codes over indecomposible injective ideal $\mathcal{I}(a)$. The first one allowed us to state a variation of the MacWilliams equivalency theorem and it sees the codes as the modules. The second one extends equivalence classes of codes but the codes are there rather $\mathcal{K}-$vector spaces and there is no equivalence theorem.

8. Other approaches

The previous constructions of codes were not exactly codes over rings so we now focus on the question when a path algebra or some ring defined over a quiver is self-injective. The self-injective algebras, with some exceptions, are infinite dimensional, which means that their quivers are not acyclic, which makes their studying quite complicated. One option is use bound quivers with some admissible ideal. By Theorem 2.21, we will obtain the finite dimensional bound quivers algebra which is self-injective as well as original infinite dimensional path algebra.

Second option is taken from [11, p397-398]. The authors say that there exists some deformation of self-injective algebras so we can study corresponding objects of finite dimension. These objects are describe by the following definition but first we recall a term of category.

A category K is an algebraic structure containing a set of objects O_K and a set of morphisms Mor_K, each morphism f has a unique source object a and target object b, $a, b \in O_K$ and we denote that f is from $\mathrm{Mor}_K(a, b)$, and a binary associative operation called composition of morphisms. For objects $a, b, c \in O_K$ the composition of morphisms is a map $\mathrm{Mor}_K(a, b) \times \mathrm{Mor}_K(b, c) \to \mathrm{Mor}_K(a, c)$. We can write $f : a \to b$ for $f \in \mathrm{Hom}_K(a, b)$ so the composition operation of $f : a \to b$ and $g : b \to c$ is written $g \circ f$ or simplier gf. Moreover for each object $a \in O_K$ there exists an identity morphism in $\mathrm{Mor}_K(a, a)$.

Definition 8.1. *Let B be a algebra and $1 = e_1 + \ldots + e_n$ a decomposition of identity of B into sum of orthogonal primitive idempotents then we define*

I. The repetitive category $\widehat{B}$ of B is category with the objects $e_{m,i} \in \mathbb{Z} \times \{1, \ldots, n\}$ and the morphism space

$$\widehat{B}\left(e_{m,i}, e_{r,j}\right) = \begin{cases} e_j B e_i, & \text{if } r = m \\ D\left(e_i B e_j\right), & \text{if } r = m+1 \\ 0, & \text{else.} \end{cases}$$

II. A group G of $K-$linear automorphisms of the category $\widehat{B}$ is said to be admissible if G has finitely many orbits and acts freely on the objects of $\widehat{B}$ which means that $g \cdot e_{i,j} = e_{i,j}$ forces $g = 1$.

III. The orbit category $\widehat{B}/G$, for an admissible group G of automorphisms of $\widehat{B}$, has natural structure of a finite dimensional self-injective $K-$algebra, called the orbit algebra of $\widehat{B}$ with respect to G.

IV. The Nakayama automorphism $\nu_{\widehat{B}}$ of $\widehat{B}$ is defined by $\nu_{\widehat{B}}(e_{m,i}) = e_{m+1,i}$ for all $(m, i) \in \mathbb{Z} \times \{1, \ldots, n\}$.

V. The orbit algebra with respect to the admissible infinite cyclic group $\left(\nu_{\widehat{B}}\right)$ generated by Nakayama automorphism $\nu_{\widehat{B}}$ is denoted $T(B) = \widehat{B}/\left(\nu_{\widehat{B}}\right)$.

The [11, p.396] gives us that a finite dimensional self-injective $K-$algebra is the Frobenius algebra.

Definition 8.2. *Let A be $\mathcal{K}-$algebra. Then A is a Frobenius algebra if there exists non-degenerated $\mathcal{K}-$bilinear form β*

$$\beta : A \times A \to \mathcal{K}$$

satisfying $\beta(ab, c) = \beta(a, bc)$ for all $a, b, c \in A$.

From [12] we get that every finite dimensional Frobenius algebra is Frobenius ring.

Theorem 8.3. *Let A be a finite dimensional $\mathcal{K}-$algebra over field $\mathcal{K}$. The following conditions are equivalent.*

- *A is Frobenius ring.*
- *There exists a non-degenerated associative $\mathcal{K}-$bilinear form $(-,-) : A \times A \to K$.*
- *There exists an isomorphism $\theta : A_A \to D(A)_A$ of right $A-$modules.*
- *There exists an isomorphism $\theta' :_A A \to_A D(A)$ of left $A-$modules.*

The most of results for codes over Frobenius algebras can be found in [5], where the authors define duality via character module or by using the bilinear form. They study also an equivalence of codes and the MacWilliams identity theorem over Frobenius rings.

Conclusion

Our goal in this thesis was to find and describe codes over path algebras. We found out that for our cause it would be better to study codes over indecomposible injective modules of path algebras. For these modules we define a bilinear form which allows us to define dual codes, a homogeneous weight which is not too different from classic Hamming weight in this case and the theorem which gives us the condition when a code is closed. Based on these definition we studied variation of elementary properties from theory of codes over fields. The MacWilliams identity and the MacWilliams equivalence theorem. We showed that for these codes there exists properly defined dual codes with exact condition for closed codes and we state the theorem about a relation between complete weight enumerator of these codes and theirs duals. The situation about equivalence of codes is not so accurate since the codes are not defined over Frobenius ring only over injective modules which has structure of $\mathcal{K}-$ vector space. We defined equivalence as J.MacWilliams mentioned in [7] or J.Wood [13] in theirs works. However we found out that we would use only $\mathcal{K}-$linear monomial transformation instead of $\mathcal{KQ}-$linear monomial transformation to obtain more accurate equivalence of codes. Finally with respect to the name of the thesis we take a look at which path algebras could be interesting in the coding theory over rings.

Bibliography

[1] Anderson, Frank W. Fuller, Kent R. *Rings and Categories of Modules* Springer-Verlag, 1992. Second Edition ISBN 3-540-97845-3.

[2] Assem, Ibrahim. Simon, Daniel. Skowroński, Andrzej. *Elements of the Representation Theory of Associative Algebras: Volume I Techniques of Representation Theory* Cambridge University Press, 2006. ISBN-13 978-0-521-58423-4.

[3] Auslender, Maurice. Reiten, Idun. Smalø, Sverre O. *Representation Theory of Artin Algebras* Cambridge University Press, 1997. ISBN-0 521 59923 7

[4] Brookfield, Gary. *Journal of Algebra: A Krull-Schmidt Theorem for Noetherian Modules** Electronically published, 2002. `http://www.calstatela.edu/faculty/gbrookf/pubs/BNoeth.pdf`

[5] Greferath, Marcus. Nechaev, Alexandr. Wisbauer, Robert. *Journal of Algebra and Its Applications: Finite Quasi-Frobenius Modules and Linear Codes*. World Scientific Company, 2004. `http://www.math.uni-duesseldorf.de/~wisbauer/quasi.pdf`

[6] Greferath, Marcus. O'Sullivan, Michael E. *On bounds for codes over Frobenius rings under homogeneous weights*. Electronically published, 2004. `http://www.sciencedirect.com/science/article/pii/S0012365X04003851`

[7] Greferath, Marcus. *Gröbner bases, Coding and Cryptography: An Introduction to Ring-Linear Coding Theory*. Springer, 2009. ISBN-978-3-540-93805-7

[8] Lei, Zhao. *Representations of Finite-Dimensional Algebras via Quivers* `http://www.math.virginia.edu/~ww9c/lzhao.pdf`

[9] Nebe, Gabriele. Rains, Eric M. Sloane, Neil J.A. *Self-dual Codes and Invariant Theory* Springer, 2006. ISBN-10 3-540-30729-X.

[10] MacWilliams, F.J. Sloane, N.J. *The Theory of Error-Correcting Codes* North-Holland, 1983. First Edition. ISBN: 9780444851932.

[11] Simon, Daniel. Skowroński, Andrzej. *Elements of the Representation Theory of Associative Algebras: Volume III Representation-Infinite Tilted Algebras* Cambridge University Press, 2007. ISBN-13 978-0-521-88218-7.

[12] Skowroński, Andrzej. Yamagata, Kunio. *Frobenius Algebras I* European Mathematical Society, 2012. ISBN 978-3-03719-102-6

[13] Wood, Jay A. *Code Equivalence Characterizes Finite Frobenius Rings* Electronically published, 2007. `http://homepages.wmich.edu/~jwood/eprints/wood-code-equivalence.pdf`

[14] Wood, Jay A. *Equivalence of Linear Codes over Finite Rings* Electronically published, 2006. http://homepages.wmich.edu/~jwood/eprints/oct22.pdf

[15] Wood, Jay A. *American Journal of Mathematics: Duality For Modules Over Finite Rings And Applications To Coding Theory* The Johns Hopkins University Press, 1999 Electronically published: http://muse.jhu.edu/journals/ajm/summary/v121/121.3wood.html