Error Correcting Codes in a Frobenius Algebra Ambient

José Gómez-Torrecillas, Erik Hieta-aho*, Javier Lobillo, Sergio R. López-Permouth, Gabriel Navarro

Aalto University, Finland

15.7.2022

Coding Theory and Cryptography: A conference in the honor of Joachim Rosenthal's 60th birthday

Outline

- Coding theory definitions
- MacWilliams Identity
- Ambient
- Cyclic, Negacyclic, Constacyclic, Polycyclic, Skewcyclic codes
- Frobenius Algebra
- Annihilator Dual
- Frobenius Algebra Ambient
- Examples

Coding Theory Definitions

Traditionally a code C is considered to be a subset of A^n for A a finite set. To filter the amount of codes we then focus on linear codes.

Coding Theory Definitions

Traditionally a code C is considered to be a subset of A^n for A a finite set. To filter the amount of codes we then focus on linear codes.

Definition (Linear Code)

A linear code C is a subspace $C \subseteq K^n$ for finite field K with length n and $\dim C = k$.

With a vector space one also uses the traditional dot product, $\langle ., . \rangle : K^n \times K^n \to K$ to define the Dual or Orthogonal code.

Definition (Dual Code)

The Dual Code of C denoted as $C^{\perp}$ with $\dim(C^{\perp}) = n - k$ is defined as

$$C^{\perp} = \{d \in K^n : \langle c, d \rangle = 0, \forall c \in C\}$$

Definition (Dual Code)

The Dual Code of C denoted as $C^{\perp}$ with $\dim(C^{\perp}) = n - k$ is defined as

$$C^{\perp} = \{d \in K^n : \langle c, d \rangle = 0, \forall c \in C\}$$

One can check whether a codeword is in C by implementation of the generator matrix of $C^{\perp}$. This property is also equivalent to:

$$(C^{\perp})^{\perp} = C$$

Which in ring theory is known as the double annihilator condition.

Definition (Dual Code)

The Dual Code of C denoted as $C^{\perp}$ with $\dim(C^{\perp}) = n - k$ is defined as

$$C^{\perp} = \{d \in K^n : \langle c, d \rangle = 0, \forall c \in C\}$$

One can check whether a codeword is in C by implementation of the generator matrix of $C^{\perp}$. This property is also equivalent to:

$$(C^{\perp})^{\perp} = C$$

Which in ring theory is known as the double annihilator condition.

Definition (Hamming Weight)

The Hamming weight, $wt(c)$, of a codeword c is defined as the number of non-zero components in c.

Weight Enumerators and MacWilliams Identity

Weight Enumerators and MacWilliams Identity

Definition (Weight Enumerator)

The weight enumerator polynomial of a code $C \subseteq K^n$ is

$$W_C(x, y) = \sum_{c \in C} x^{n - wt(c)} y^{wt(c)} = \sum_{i=0}^{n} A_i x^{n-i} y^i.$$

where A_i counts the number of codewords of weight i.

Weight Enumerators and MacWilliams Identity

Definition (Weight Enumerator)

The weight enumerator polynomial of a code $C \subseteq K^n$ is

$$W_C(x, y) = \sum_{c \in C} x^{n - wt(c)} y^{wt(c)} = \sum_{i=0}^{n} A_i x^{n-i} y^i .$$

where A_i counts the number of codewords of weight i.

The MacWilliams identities correlate the weight enumerators between C and $C^\perp$.

Theorem (MacWilliams Identity)

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y)$$

Algebra structure and the Ambient

Often one filters codes further by considering additional algebraic structures.

Algebra structure and the Ambient

Often one filters codes further by considering additional algebraic structures.

Terminology (Ambient)

Define an algebra structure A on K^n ($A \cong K^n$ with additional multiplication on A), you may focus on those linear codes C which are (left) ideals of A. Then we say that A is the **ambient** *of that family of codes.*

Algebra structure and the Ambient

Often one filters codes further by considering additional algebraic structures.

Terminology (Ambient)

Define an algebra structure A on K^n ($A \cong K^n$ with additional multiplication on A), you may focus on those linear codes C which are (left) ideals of A. Then we say that A is the **ambient** *of that family of codes.*

Something to note regarding the left ideal C and the right annihilator $ann_r(C) = \{a \in A : Ca = 0\}$, is that
$ann_r(C) \triangleleft_r A$ and note $ann_l(ann_r(C)) \supseteq C$.

Cyclic codes:

$$C \subset K^n \leftrightarrow C \triangleleft_I \mathcal{R} = \frac{K[x]}{\langle x^n - 1 \rangle}$$

Cyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle x^n - 1 \rangle}$$

Negacyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle x^n + 1 \rangle}$$

Cyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle x^n - 1 \rangle}$$

Negacyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle x^n + 1 \rangle}$$

Constacyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle x^n - a \rangle}$$

Cyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle x^n - 1 \rangle}$$

Negacyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle x^n + 1 \rangle}$$

Constacyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle x^n - a \rangle}$$

Polycyclic codes:

$$C \subset K^n \leftrightarrow C \lhd_I \mathcal{R} = \frac{K[x]}{\langle f \rangle}$$

Definition (Skew Cyclic Code)

For σ an automorphism of K. A linear code C is a $\sigma-$cyclic code with the property that $(a_0, a_1, \ldots, a_{n-1}) \in C$ implies $(\sigma(a_{n-1}), \sigma(a_0), \ldots, \sigma(a_{n-2})) \in C$.

A code C is a *skew cyclic* code if it is an ideal of the quotient ring $\dfrac{K[x,\sigma]}{\langle f \rangle}$ where σ is an automorphism of K.

Ambient properties

There are two important properties which seem desirable for an ambient:

Ambient properties

There are two important properties which seem desirable for an ambient:

1. A Double Annihilator Condition (d.a.c.) to serve the same purpose as $(C^{\perp})^{\perp} = C$.

Ambient properties

There are two important properties which seem desirable for an ambient:

1. A Double Annihilator Condition (d.a.c.) to serve the same purpose as $(C^{\perp})^{\perp} = C$.
2. MacWilliams Identity Analogue - The weight distribution of a code is determined by the dual.

Ambient properties

There are two important properties which seem desirable for an ambient:

1. A Double Annihilator Condition (d.a.c.) to serve the same purpose as $(C^{\perp})^{\perp} = C$.
2. MacWilliams Identity Analogue - The weight distribution of a code is determined by the dual.

Therefore we need to determine what conditions on the ambient are necessary or sufficient to satisfy these two properties.

Quasi-Frobenius ring

Definition (Double Annihilator Condition)

Let A be a ring. Then A satisfies the double annihilator condition if for any left ideal $C \triangleleft_l A$, $ann_l(ann_r(C)) = C$ and for any right ideal $D \triangleleft_r A$, $ann_r(ann_l(D)) = D$.

Quasi-Frobenius ring

Definition (Double Annihilator Condition)

Let A be a ring. Then A satisfies the double annihilator condition if for any left ideal $C \triangleleft_l A$, $ann_l(ann_r(C)) = C$ and for any right ideal $D \triangleleft_r A$, $ann_r(ann_l(D)) = D$.

In our setting of finite rings there are multiple ways to characterize a Quasi-Frobenius ring, one of which is that the ring satisfies the double annihilator condition.

Quasi-Frobenius ring

Definition (Double Annihilator Condition)

Let A be a ring. Then A satisfies the double annihilator condition if for any left ideal $C \lhd_l A$, $ann_l(ann_r(C)) = C$ and for any right ideal $D \lhd_r A$, $ann_r(ann_l(D)) = D$.

In our setting of finite rings there are multiple ways to characterize a Quasi-Frobenius ring, one of which is that the ring satisfies the double annihilator condition. So one should look for Quasi-Frobenius ambients however...

Quasi-Frobenius ring

Definition (Double Annihilator Condition)

Let A be a ring. Then A satisfies the double annihilator condition if for any left ideal $C \triangleleft_l A$, $ann_l(ann_r(C)) = C$ and for any right ideal $D \triangleleft_r A$, $ann_r(ann_l(D)) = D$.

In our setting of finite rings there are multiple ways to characterize a Quasi-Frobenius ring, one of which is that the ring satisfies the double annihilator condition. So one should look for Quasi-Frobenius ambients however... we have a second condition.

Frobenius Algebra

Definition (Frobenius Algebra)

Let A be a K-algebra then A is a Frobenius K-algebra if and only if $A \cong A^*$ as a right A-module, where $A^* = Hom_K(A, K)$.

Frobenius Algebra

Definition (Frobenius Algebra)

Let A be a K-algebra then A is a Frobenius K-algebra if and only if $A \cong A^*$ as a right A-module, where $A^* = Hom_K(A, K)$.

If A is a finite dimensional Frobenius K-algebra then A is a Quasi-Frobenius ring and thus satisfies d.a.c.

Frobenius Algebra

Definition (Frobenius Algebra)

Let A be a K-algebra then A is a Frobenius K-algebra if and only if $A \cong A^*$ as a right A-module, where $A^* = Hom_K(A, K)$.

If A is a finite dimensional Frobenius K-algebra then A is a Quasi-Frobenius ring and thus satisfies d.a.c.

A well known property which is equivalent to A being a Frobenius algebra follows:

Theorem

A is a Frobenius K-algebra $\iff$ there exists a K-bilinear nondegenerate map

$$B : A \times A \to K$$

which is associative (for $x, y, z \in A$, $B(x, zy) = B(xz, y)$).

Definition (Bilinear form)

A map $B : A \times A \to K$ is a bilinear form if it satisfies the following axioms: Let $x, y, z \in A$ and $r \in K$,

1. B(x+y,z)=B(x,z)+B(y,z)
2. B(x,y+z)=B(x,y)+B(x,z)
3. B(rx,y)=rB(x,y)
4. B(x,ry)=rB(x,y)

Furthermore a bilinear form is *nondegenerate*

$$\text{if } B(x,y) = 0 \text{ for all } y \in A \text{ then } x = 0$$

$$\text{and if } B(x,y) = 0 \text{ for all } x \in A \text{ then } y = 0.$$

Annihilator Dual

With A a Frobenius K-algebra and the nondegenerate associative bilinear form $\langle ., . \rangle : A \times A \to K$ we define two dual structures:

Annihilator Dual

With A a Frobenius K-algebra and the nondegenerate associative bilinear form $\langle .,. \rangle : A \times A \to K$ we define two dual structures:

Definition (Annihilator Dual)

Let $S \subset A$ a subset.

$$S^\circ = \{a \in A : \langle s, a \rangle = 0 \text{ for all } s \in S\}$$

$$^\circ S = \{a \in A : \langle a, s \rangle = 0 \text{ for all } s \in S\}$$

Annihilator Dual

With A a Frobenius K-algebra and the nondegenerate associative bilinear form $\langle ., . \rangle : A \times A \to K$ we define two dual structures:

Definition (Annihilator Dual)

Let $S \subset A$ a subset.

$$S^\circ = \{a \in A : \langle s, a \rangle = 0 \text{ for all } s \in S\}$$

$$^\circ S = \{a \in A : \langle a, s \rangle = 0 \text{ for all } s \in S\}$$

Now of course one wonders whether these duals are related to the annihilator of the ideal.

Annihilator Dual

With A a Frobenius K-algebra and the nondegenerate associative bilinear form $\langle ., . \rangle : A \times A \to K$ we define two dual structures:

Definition (Annihilator Dual)

Let $S \subset A$ a subset.

$$S^\circ = \{a \in A : \langle s, a \rangle = 0 \text{ for all } s \in S\}$$

$$^\circ S = \{a \in A : \langle a, s \rangle = 0 \text{ for all } s \in S\}$$

Now of course one wonders whether these duals are related to the annihilator of the ideal. By a well known result in ring theory, which can be found in 'Lectures on Modules and Rings' by T.Y. Lam, they are:

Theorem

For S a left ideal, $S^\circ = Ann_r(S)$ and for S a right ideal, $^\circ S = Ann_l(S)$.

Frobenius Algebra Ambient

With the implementation of these annihilator duals we have the following result which is from our joint work with José Gómez-Torrecillas, Javier Lobillo, Sergio R. López-Permouth, and Gabriel Navarro.

Frobenius Algebra Ambient

With the implementation of these annihilator duals we have the following result which is from our joint work with José Gómez-Torrecillas, Javier Lobillo, Sergio R. López-Permouth, and Gabriel Navarro.

Theorem (Frobenius Algebra Ambient)

Let A be a finite dimensional Frobenius K-algebra, K a finite field of characteristic p, and C a left ideal of A, then the d.a.c. is satisfied by the annihilator duals and the following MacWilliams identity analogue holds:

$$W_{C^\circ}(x, y) = \frac{1}{|C|} \sum_{a \in C} \sum_{b \in A} \psi(\langle a, b \rangle) x^{n - wt(b)} y^{wt(b)}$$

for ψ a standard complex character on K and $wt : A \to \mathbb{N}$ a weight function.

Frobenius Algebra Ambient

With the implementation of these annihilator duals we have the following result which is from our joint work with José Gómez-Torrecillas, Javier Lobillo, Sergio R. López-Permouth, and Gabriel Navarro.

Theorem (Frobenius Algebra Ambient)

Let A be a finite dimensional Frobenius K-algebra, K a finite field of characteristic p, and C a left ideal of A, then the d.a.c. is satisfied by the annihilator duals and the following MacWilliams identity analogue holds:

$$W_{C^\circ}(x, y) = \frac{1}{|C|} \sum_{a \in C} \sum_{b \in A} \psi(\langle a, b \rangle) x^{n - wt(b)} y^{wt(b)}$$

for ψ a standard complex character on K and $wt : A \to \mathbb{N}$ a weight function.

The proof of the MacWilliams identity analogue includes the implementation of the Discrete Fourier Transform.

In particular, our result contains the following result that can be found in the paper by Alhamadi, Dougherty, Solé, and Leroy in AMC 2016.

In particular, our result contains the following result that can be found in the paper by Alhamadi, Dougherty, Solé, and Leroy in AMC 2016.

Theorem

Let $A = \frac{K[x]}{\langle f \rangle}$, $f(0) \neq 0$ *then the bilinear form* $\langle ., . \rangle_f$ *defined in the following manner:*

$$\langle g, h \rangle_f = gh(0) := (gh)_0 \text{ for } g, h \in A$$

is nondegenerate and there exists a MacWilliams identity analogue with respect to the annihilator dual defined by the bilinear form.

In particular, our result contains the following result that can be found in the paper by Alhamadi, Dougherty, Solé, and Leroy in AMC 2016.

Theorem

Let $A = \dfrac{K[x]}{\langle f \rangle}$, $f(0) \neq 0$ *then the bilinear form* $\langle ., . \rangle_f$ *defined in the following manner:*

$$\langle g, h \rangle_f = gh(0) := (gh)_0 \text{ for } g, h \in A$$

is nondegenerate and there exists a MacWilliams identity analogue with respect to the annihilator dual defined by the bilinear form.

This result is an example of polycyclic codes and is an example of our result since A is a Frobenius K-algebra.

Skewcyclic Polynomial Ring Example

The following is another result of our work and is an illustration of how extensive our result is.

Skewcyclic Polynomial Ring Example

The following is another result of our work and is an illustration of how extensive our result is.

Theorem

Let $A = \frac{B[x;\sigma]}{\langle f \rangle}$*, with* B *a Frobenius* K*-algebra,* $\sigma \in Aut_K(B)$*,* f *monic with non zero divisor constant coefficient.*

Skewcyclic Polynomial Ring Example

The following is another result of our work and is an illustration of how extensive our result is.

Theorem

Let $A = \frac{B[x;\sigma]}{\langle f \rangle}$, with B a Frobenius K-algebra, $\sigma \in Aut_K(B)$, f monic with non zero divisor constant coefficient. Then A is a Frobenius K-algebra with non degenerate bilinear form

$$\langle .,. \rangle_A : A \times A \to K$$

$$\langle a, b \rangle_A = \langle 1, (ab)_0 \rangle$$

Skewcyclic Polynomial Ring Example

The following is another result of our work and is an illustration of how extensive our result is.

Theorem

Let $A = \frac{B[x;\sigma]}{\langle f \rangle}$, with B a Frobenius K-algebra, $\sigma \in Aut_K(B)$, f monic with non zero divisor constant coefficient. Then A is a Frobenius K-algebra with non degenerate bilinear form

$$\langle ., . \rangle_A : A \times A \to K$$

$$\langle a, b \rangle_A = \langle 1, (ab)_0 \rangle$$

The fact that the coefficients are from B, a Frobenius K-algebra, plays a roll in the proof of the nondegeneracy of $\langle ., . \rangle_A$.

Bibliography

- José Gómez-Torrecillas, Erik Hieta-aho*, Javier Lobillo, Sergio R. López-Permouth, Gabriel Navarro.
  Some remarks on non projective Frobenius algebras and linear codes.
  Designs, Codes, and Cryptography, Vol. 69, No. 3, 2019
- Adel Alahmadi, Steven Dougherty, Andre Leroy, Patrick Sole.
  On the Duality and the Direction of Polycyclic Codes.
  Advances in Mathematics of Communications, Vol. 10, No. 2016, pp. 921-929.
- T.Y. Lam.
  Lectures on Modules and Rings.
  Springer-Verlag New York, 1999.

The end

Thank you
Happy Birthday Joachim!