Mattson-Solomon transform and Gröbner bases: applications to association schemes and codes

Edgar Martínez-Moro

Workshop D1: Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics
May 01 - May 06

Abstract

The Mattson-Solomon transform of a semisimple algebra has been a valuable tool both in the theory of commutative association schemes and coding theory. In this talk we will review the relation between the structure of the Gröbner bases associated to these structures and some properties of the semisimple algebra related to the combinatorics of association schemes and codes.

Introduction

Eigenvalues of elements of semisimple finite-dimensional commutative algebras have been extensively used in many areas, for example, values of characters of finite groups, eigenvalues of generalized circulant matrices, Mattson-Solomon coefficients of a codeword of a cyclic code [2], and elementary properties of commutative association schemes [11, 12].

In this seminar we shall adopt an approach using the language of Gröbner bases which, although not strictly necessary, leads to concise arguments and gives a common background for dealing with these structures. Eigenvalue techniques have been used already for solving zero-dimensional systems of equations (see, for example [16]). We take a different approach and translate the eigenvalue problem into a system of equations. This allows us to define an ideal $\mathcal{I} \subset \mathbb{F}[x_1, \ldots, x_n]$ such that the algebra being considered is isomorphic to $\mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}$ (since it is finite dimensional), and moreover we describe $\mathcal{I}$ in terms of a Gröbner basis with respect to a total degree lexicographic ordering. The reader is assumed to be familiar with tha basic definitions and facts of association schemes, codes and Gröbner basis.

1 A primer in representation theory

Representation Theory is the study of concrete realizations (specially matrix and permutation realizations) of axiomatic objects of abstract algebra, in par-

ticular of groups and algebras. The theory of group representations was fully established by Frobenius in the 19th century. In this section we will only concern with the representation of separable commutative algebras. For an account on classical representation theory see [3, 4].

Commutative separable semisimple algebras over a field

We will start with the basic theory of representations of commutative separable semisimple finite dimensional algebras. Most of it can be found in classical accounts on algebra and representation theory as [4] or [7]. A concise idea about diagonalization can be found in [2].

In this section let $\mathbb{F}$ be a commutative field (in most of the cases it will be a finite field as in the rest of the seminar).

Definition 1. An associative algebra $\mathcal{A}$ over the field $\mathbb{F}$ is a pair consisting on a ring $(\mathcal{A}, +, \cdot)$ and a vector space $\mathcal{A}$ over $\mathbb{F}$ such that the addition is the same in the ring and in the vector space and:

$$\alpha(ab) = (\alpha a)b = a(\alpha b) \qquad \forall \alpha \in \mathbb{F}, a, b \in \mathcal{A} \tag{1}$$

If the dimension of $\mathcal{A}$ over $\mathbb{F}$ is finite we say that it is finite dimensional. If the operation $\cdot$ in the ring is commutative we say that the algebra $\mathcal{A}$ is commutative.

From now on $\mathcal{A}$ will be an n-dimensional commutative algebra with identity 1 over a field $\mathbb{F}$. A map from an algebra $\mathcal{A}$ into an algebra $\mathcal{B}$ over the same field is an *homomorphism* (of algebras) if it is both a ring homomorphism and a linear mapping.

Let V be a vector space over $\mathbb{F}$, and let $\mathrm{End}_{\mathbb{F}}(V) = \mathrm{Hom}(V, V)$ the set of $\mathbb{F}$-linear transformations of V into itself. $\mathrm{End}_{\mathbb{F}}$ can be endowed with and algebra structure given by the usual addition and product of linear transformations and the multiplication by scalars in $\mathbb{F}$. A homomorphism of an algebra $\mathcal{A}$ over $\mathbb{F}$ into an algebra $\mathrm{End}_{\mathbb{F}}(V)$ of linear transformations of a vector space V is called a *representation* of $\mathcal{A}$.

For each element $a \in \mathcal{A}$ we have the linear mapping T_a given by

$$\begin{array}{rccc} T_a : & \mathcal{A} & \longrightarrow & \mathcal{A} \\ & u & \mapsto & au \end{array} \tag{2}$$

The homomorphism

$$\begin{array}{ccc} \mathcal{A} & \longrightarrow & \mathrm{End}_{\mathbb{F}}(\mathcal{A}) \\ a & \mapsto & T_a \end{array} \tag{3}$$

is called *the regular representation* of the algebra $\mathcal{A}$.

If $\mathfrak{B} = \{b_1, \ldots, b_n\}$ is a basis of $\mathcal{A}$ as vector space over $\mathbb{F}$ then, for every element $a \in \mathcal{A}$, we define the $n \times n$ matrix

$$M(a; \mathfrak{B}) := (m_{i,j}(a, \mathfrak{B}))_{i,j=1}^{n}, \; ab_i = \sum_{j=1}^{n} m_{i,j}(a, \mathfrak{B}) b_j, \; m_{i,j}(a, \mathfrak{B}) \in \mathbb{F}, \tag{4}$$

that is $M(a; \mathfrak{B})^t$ is the matrix representing T_a with respect to the basis $\mathfrak{B}$.

Theorem 1. *$M(\mathcal{A};\mathfrak{B}) := \{M(a;\mathfrak{B}) \mid a \in \mathcal{A}\}$ is isomorphic to $\mathcal{A}$ as algebras over $\mathbb{F}$.*

Proof. The proof is standard linear algebra. Indeed the map $\rho : a \mapsto T_a$ in equation (3) is an algebra monomorphism of $\mathcal{A}$ into $\mathrm{End}_{\mathbb{F}}(\mathcal{A})$. Clearly fixed a basis $\mathfrak{B}$ the transposes of the matrices in $M(\mathcal{A};\mathfrak{B})$ are isomorphic to the image of ρ. Thus the isomorphism we wanted is just ρ followed by the isomorphism $L \mapsto L^T$ where $L \in \mathrm{End}_{\mathbb{F}}(\mathcal{A})$. □

Let $p(X) = \alpha_0 + \cdots + \alpha_n X^n \in \mathbb{F}[X]$, by $p(a)$ where $a \in \mathcal{A}$ we denote $p(a) = \alpha_0 + \cdots + \alpha_n a^n \in \mathcal{A}$. For each $a \in \mathcal{A}$, let $m_a(x)$ be the *minimal polynomial* of T_a, that is, the unique monic polynomial of minimum degree such that $m_a(a) = 0$. In our discusion below the concept of separability will play a central role:

Definition 2 (Separable algebra).

1. An element $a \in \mathcal{A}$ is called *separable* if the irreducible factors of $m_a(x)$ over $\mathbb{F}$ do not have multiple roots in the splitting field of $m_a(x)$ over $\mathbb{F}$.
2. We say that the algebra $\mathcal{A}$ is *separable* if every element of $\mathcal{A}$ is separable.

If $\mathbb{F}$ is a perfect field then the irreducible factors of any polynomial have no multiple root, therefore the following result holds

Proposition 1. *If the field $\mathbb{F}$ is perfect then all algebras with 1 over $\mathbb{F}$ are separable.*

Definition 3 (Semisimple algebra). An algebra $\mathcal{A}$ is *simple* if its only ideals as a ring are $\{0\}$ and $\mathcal{A}$. An algebra $\mathcal{A}$ is called *semisimple* if it is a direct sum of simple algebras.

The following theorem is a particular instance of Schur's lemma (see for example [5, 2.4])

Theorem 2 (Weiertrass-Dedekind). *If $\mathcal{A}$ is semisimple, commutative algebra over a field $\mathbb{F}$ then $\mathcal{A}$ is a direct sum of finite extensions of $\mathbb{F}$.*

Theorem 3 ([2]). *If $\mathcal{A}$ is a separable, semisimple, finite-dimensional commutative algebra over a field $\mathbb{F}$ and $\mathfrak{B}$ a basis of $\mathcal{A}$, then all the elements of $M(\mathcal{A};\mathfrak{B})$ can be simultaneously diagonalized over some finite extension field of $\mathbb{F}$.*

Proof. From the definition in equation (4) is easy to check that

$$M(a \cdot b;\mathfrak{B}) = M(a;\mathfrak{B}) \cdot M(b;\mathfrak{B}) \quad a, b \in \mathcal{A}$$

and and the fact that the algebra is commutative $a \cdot b = b \cdot a$ then the matrices commute. Moreover, from the proof of theorem 1 follows that if $\mathfrak{B}$ is a basis of the algebra $\mathcal{A}$ then $\{M(a;\mathfrak{B}) \mid a \in \mathfrak{B}\}$ is a basis of $M(\mathcal{A};\mathfrak{B})$. Thus $M(\mathcal{A};\mathfrak{B})$ is a finite dimensional set of commuting matrices, therefore there is a $n \times n$ matrix X over some extension field of $\mathbb{F}$ such that (see [6])

$$X^{-1} M(a;\mathfrak{B}) X = \text{diagonal} \quad \forall a \in \mathcal{A}$$

□

From now on SFCA will stand for semisimple finite-dimensional commutative algebra.

2 SFCA's and Gröbner basis.

The results in this section can be found in [13]. We will make use of the following examples of SFCA's during this section:

Example 1. Consider the matrix algebra $\mathcal{A}_1$ over $\mathbb{C}$ generated by the base $\mathfrak{B}_1 = \{D_0, D_1, D_2\}$ of symmetric 9×9 matrices given by

$$D_k(i,j) = \begin{cases} 1 & \text{if } i - j \in \mathcal{O}_k \bmod 9 \\ 0 & \text{elsewhere} \end{cases}$$

where

$$\mathcal{O}_0 = \{0\},\ \mathcal{O}_1 = \{\pm 3\},\ \mathcal{O}_2 = \{\pm 1, \pm 2, \pm 4\}.$$

$\mathcal{A}_1$ is an SFCA, and following the notation above, we have

$$X^{-1}M(D_0;\mathfrak{B}_1)X = \mathrm{diag}(1,1,1) \quad X^{-1}M(D_1;\mathfrak{B}_1)X = \mathrm{diag}(2,2,-1)$$

$$X^{-1}M(D_2;\mathfrak{B}_1)X = \mathrm{diag}(6,-3,0)$$

$$X = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & -1 \\ 6 & -3 & 0 \end{pmatrix}$$

This algebra arises as the Bose-Mesner algebra of a commutative association scheme. See [11, 12] for a detailed treatment of commutative association schemes using Gröbner basis techniques.

Example 2. Let $\mathcal{A}_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then it is a SFCA of dimension 4 over $\mathbb{Q}$. Let $\mathfrak{B}_2 = \{b_1 = 1, b_2 = \sqrt{2}, b_3 = \sqrt{3}, b_4 = \sqrt{6}\}$. We have the following:

$$\begin{array}{rcl} X^{-1}M(b_1;\mathfrak{B}_2)X & = & \mathrm{diag}(1,1,1,1) \\ X^{-1}M(b_2;\mathfrak{B}_2)X & = & \mathrm{diag}(-\sqrt{2},-\sqrt{2},\sqrt{2},\sqrt{2}) \\ X^{-1}M(b_3;\mathfrak{B}_2)X & = & \mathrm{diag}(-\sqrt{3},\sqrt{3},-\sqrt{3},\sqrt{3}) \\ X^{-1}M(b_4;\mathfrak{B}_2)X & = & \mathrm{diag}(\sqrt{6},-\sqrt{6},-\sqrt{6},\sqrt{6}) \end{array} \tag{5}$$

$$X = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -\sqrt{2} & -\sqrt{2} & \sqrt{2} & \sqrt{2} \\ -\sqrt{3} & \sqrt{3} & -\sqrt{3} & \sqrt{3} \\ \sqrt{6} & -\sqrt{6} & -\sqrt{6} & \sqrt{6} \end{pmatrix}$$

See [2] for more details about this example.

Let $\mathcal{A}$ be a SFCA over $\mathbb{F}$ of dimension n, and let $\mathfrak{B} = \{b_1, b_2, \ldots, b_n\}$ be a basis of $\mathcal{A}$. We have that for each pair $1 \le i, j \le n$:

$$b_i b_j = \sum_{k=1}^{n} m_{i,k}(b_j, \mathfrak{B}) b_k\,. \tag{6}$$

We call equations in (6) the **multiplication table of the algebra $\mathcal{A}$** with respect to the base $\mathfrak{B}$. It is easy to see that any other multiplication table $M(a;\mathfrak{B})$ can be derived from this one just by linearity. Note also that only the products $1 \leq i \leq j \leq n$ are needed since $\mathcal{A}$ is a commutative algebra.

Consider now the set of polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ given by

$$x_i x_j - \sum_{k=1}^{n} m_{i,k}(b_j, \mathfrak{B}) x_k \quad 1 \leq i \leq j \leq n\,. \tag{7}$$

We call these the **structure polynomials of the algebra $\mathcal{A}$**. For the sake of simplicity, since a SFCA always contains 1 (see [2]), we shall let $b_1 = 1$ the unit of $\mathbb{F}$, so the polynomials in (7) become[1]

$$F := \left\{ x_i x_j - m_{i,1}(b_j, \mathfrak{B}) - \sum_{k=2}^{n} m_{i,k}(b_j, \mathfrak{B}) x_k \right\}_{2 \leq i \leq j \leq n} \cup \{x_1 - 1\}\,. \tag{8}$$

We shall denote $\mathcal{I} = \langle F \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$ the ideal generated by F.

Proposition 2. *F is a reduced Gröbner basis of the ideal $\mathcal{I}$ with respect to a total degree lexicographic ordering.*

Proof. This can be shown by computing the S-polynomial for each pair of polynomials in F and checking that it reduces to 0. Let $F_{ij} = x_i x_j - f_{ij}$ where $f_{ij} = m_{i,1}(b_j, \mathfrak{B}) + \sum_{k=2}^{n} m_{i,k}(b_j, \mathfrak{B}) x_k$, $2 \leq i \leq j \leq n$.

1. If i, j, k are pairwise distinct we have

$$S(F_{ij}, F_{jk}) = x_i f_{jk} - x_k f_{ij} \overset{(\star)}{=} \sum_{l=2}^{n} m_{j,l}(b_k, \mathfrak{B}) F_{li} - \sum_{p=2}^{n} m_{i,p}(b_j, \mathfrak{B}) F_{pk} +$$

$$+ (x_i m_{j,1}(b_k, \mathfrak{B}) - x_k m_{i,1}(b_j, \mathfrak{B}))(x_1 - 1)$$

   Hence, $S(F_{ij}, F_{jk}) \rightarrow_{\mathcal{F}} 0$.

   Note that equality $(\star)$ holds because the algebra is associative, and hence

$$\sum_{l=1}^{n} m_{j,l}(b_k, \mathfrak{B}) m_{i,s}(b_l, \mathfrak{B}) = \sum_{p=1}^{n} m_{i,p}(b_j, \mathfrak{B}) m_{p,s}(b_k, \mathfrak{B}) \quad 1 \leq i, j, k, s \leq n\,.$$

2. In the case k, l are different from i and j, we have

$$S(F_{ij}, F_{kl}) = x_i x_j f_{kl} - x_k x_l f_{ij} = (F_{ij} - f_{ij}) f_{kl} - (F_{kl} - f_{kl}) f_{ij} = F_{ij} f_{kl} - F_{kl} f_{ij}$$

   and therefore $S(F_{ij}, F_{kl}) \rightarrow_{\mathcal{F}} 0$.

3. Finally, $S(F_{ij}, x_1 - 1) = F_{ij} + f_{ij}(x_1 - 1)$, hence $S(F_{ij}, x_1 - 1) \rightarrow_{\mathcal{F}} 0$.

[1] The discussion with any other basis can be done the same manner, see Remark 3.

It is straightforward that the Gröbner basis in (8) is a reduced basis since no leading term of any of the polynomials in the basis divides any monomial appearing in the other polynomials in (8). □

By Proposition 2 we can reproduce most of the material in section before in a Gröbner setting. Fixing a monomial ordering $<$ on the terms in $\mathbb{F}[x_1, \ldots, x_n]$, as usual, we will denote by $lt(f)$, where $f \in \mathbb{F}[x_1, \ldots, x_n]$, to the leading term of f with respect to the ordering $<$. The set of terms will be denoted by

$$T = \left\{ x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in \mathbb{N}_0 \right\} .$$

Let us define the normal set of F in a total degree monomial ordering ($<_{tdeg}$) as

$$N(F; <_{tdeg}) = \{t \in T \mid \nexists f \in F \text{ such that } lt(f)|t\} = \{x_i\}_{i=1}^n . \tag{9}$$

This is a basis of $\mathbb{F}[x_1, x_2, \ldots, x_n]/\mathcal{I}$ and its cardinality is just the number of roots of the system of equations given by the polynomials in the set F in a adequate field extension of $\mathbb{F}$, say $\mathbb{K}$. Therefore, if we let $V(F) = \{\vec{z} \in \mathbb{K}^n \mid f(\vec{z}) = 0 \text{ and } f \in \mathcal{I}\}$ be the variety in $\mathbb{K}^n$ defined by the ideal $\mathcal{I}$, then $V(F)$ is zero-dimensional.

We can describe the effect of multiplying an arbitrary element by $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]/\mathcal{I}$ just by multiplying f by each term in $N(F; <_{tdeg})$. Letting $\mathrm{nf}(f; <_{tdeg})$ denote the normal form with respect F, we have that:

$$\mathrm{nf}(f \cdot x_i; <_{tdeg}) = \sum a_{ij}(f) \cdot x_i \quad i = 1, \ldots, n . \tag{10}$$

As usual, the matrix $A(f; <_{tdeg}) = (a_{ij}(f))_{i,j=1}^n$ is the multiplication matrix of f in $\mathbb{F}[x_1, x_2, \ldots, x_n]/\mathcal{I}$. Hence it is clear that we can rebuild any multiplication table from the matrices in the set $\{A(x_i; <_{tdeg})\}_{i=1}^n$. The following lemma is a modified version of a theorem in [16].

Lemma 1. *Let F be the Gröbner basis given above with respect to a total degree monomial ordering, and let $M_1, \ldots M_n$ be the multiplication tables for the normal set $N(F; <_{tdeg})$. Let X be the $n \times n$ matrix whose entries are in some extension $\mathbb{K}$ of $\mathbb{F}$ such that $X^{-1} M_i X = F_i$ is diagonal. Then the diagonal entries of the matrices F_i are the points of $V(F)$ in $\mathbb{K}^n$.*

Proof. Suppose that $\vec{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{K}^n$ is a root of the system given by F. We have that $f(\vec{z}) \cdot x_i = \sum_{j=1}^n a_{ij}(f) \cdot z_j$. Therefore we have

$$(A(f; <_{tdeg}) - f(\vec{z}) Id)\, \vec{z}^{\,t} = \vec{0} . \tag{11}$$

Note that $\vec{z} \neq \vec{0}$ since $z_1 = 1$, thus z_i is an eigenvalue of M_j.

To prove that all eigenvalues are roots is straightforward since for any $p(\vec{x}) \in \mathbb{K}[x_1, x_2, \ldots, x_n]$ we have that $X^{-1} p(M_1, M_2, \ldots, M_n) X$ is diagonal and the conclusion follows from the fact that for all $p \in \mathcal{I}$ the result is $\vec{0}$. □

Remark 1 (Eigenvectors). Note that from equation (11) we have that the vector given by the diagonal entries of the diagonal matrices is also an eigenvector.

This gives the following straightforward consequence:

Theorem 4. *Given a SFCA $\mathcal{A}$ over $\mathbb{F}$ of dimension n, and $\mathfrak{B} = \{b_1 = 1, b_2, \ldots, b_n\}$ a basis of $\mathcal{A}$, the eigenvalues of the matrices $M(b_i; \mathfrak{B})$ in some extension field $\mathbb{K}$ of $\mathbb{F}$ are given by the variety $V(\mathcal{I})$.*

Example 3. Recalling the examples above:

- Let $\mathcal{A}_1$ be the SFCA in Example 1. Let $F_1 = \{{x_2}^2 - 6 - 6x_1 - 3x_2,\ x_0 - 1,\ {x_1}^2 - x_1 - 2,\ x_1x_2 - 2x_2\}$. Then $V(F_1)$ is the variety in Lemma 1.
- Let $\mathcal{A}_2$ be as in Example 2. The variety $V(F_2)$ defined by

  $$F_2 = \left\{x_1 - 1, x_2^2 - 2, x_3^2 - 3, x_4^2 - 6, x_2x_3 - x_4, x_2x_4 - 2x_3, x_3x_4 - 3x_3\right\}$$

  consist of the eigenvalues of the multiplication matrices corresponding to the given basis.

Remark 2 (On ordering the solutions). Let $\mathcal{A}$ be a SFCA over $\mathbb{F}$ of dimension n, let $\mathfrak{B} = \{b_1, b_2, \ldots, b_n\}$ be a basis of $\mathcal{A}$, and let X be a diagonalizing matrix of $\mathcal{A}$ with respect to $\mathfrak{B}$. Let $X^{-1}M(b_i; \mathfrak{B})X = diag(b_i(1), \ldots, b_i(n))$ and $Y = (b_i(j)))$. Then

$$X^{-1}M(b_i; \mathfrak{B})X = Y^{-1}M(b_i; \mathfrak{B})Y\,.$$

See Theorem 2.3 in [2] for non Gröbner basis proof. This result can also be directly obtained from Remark 1. It therefore gives us a set of common right eigenvectors.

Theorem 5. *The ideal $\mathcal{I} \subseteq \mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is an extension field where the algebra diagonalizes, is radical.*

Proof. The algebra $\mathcal{A}$ is commutative and semisimple, hence it contains no nilpotent elements (see [5], Corollary 2.2.7), and the elements in the radical of $\mathcal{I}$ correspond to nilpotent elements in the algebra. □

From the discussion above we have constructed – directly from the structure of a SFCA $\mathcal{A}$ of dimension n over a field $\mathbb{F}$ – a Gröbner basis with respect to a total degree monomial ordering for a radical ideal $\mathcal{I}$ such that $\mathcal{A} \simeq \mathbb{F}[x_1, x_2, \ldots, x_n]/\mathcal{I}$ as $\mathbb{F}$-algebras.

Remark 3 (Change of base). Let $\mathcal{A}$ be a SFCA over $\mathbb{F}$ of dimension n, and let $\mathfrak{B} = \{b_1, b_2, \ldots, b_n\}$ be a basis of $\mathcal{A}$, and $\mathcal{F}$ its associated Gröbner basis with respect to a total degree monomial ordering. Let $0 \neq u = \sum_{i=1}^{n} a_i b_i$ be an element of $\mathcal{A}$. If $a_{i_1} \neq 0$ we can easily rebuild a Gröbner basis $\mathcal{F}'$ for $\mathfrak{B}' = \{b_1, b_2, \ldots, \overbrace{u}^{i_0}, \ldots, b_n\}$, just by replacing $x_{i_0} = \frac{1}{a_{i_0}}\left(u - \sum_{i=1, i\neq i_0}^{n} a_i x_i\right)$ and reducing the degree 2 terms. This is illustrated in the next example.

Example 4. In the same setting as Example 2, let $u = \sqrt{2} + \sqrt{3}$, and consider the base $\mathfrak{B}_2' = \{1, \sqrt{2}, u, \sqrt{6}\}$ of $\mathcal{A}_2$. Taking $x_3 = y - x_2$ in the equations in Example 3 we get:

$$\begin{gathered}\{x_1 - 1, x_2^2 - 2, y^2 + x_2^2 - 2yx_2 - 3, \\ x_4^2 - 6, x_2y - x_2^2 - x_4, x_2x_4 - 2y + 2x_2, yx_4 - x_2x_4 - 3x_2\}\end{gathered}$$

and thus we have the Gröbner basis:

$$\begin{aligned} F_2' = \quad & \{x_1 - 1, x_2^2 - 2, y^2 - 2x_4 - 5, x_4^2 - 6, \\ & x_2y - x_4 - 2, x_2x_4 - 2y + 2x_2, yx_4 - x_2 - 2y\} \end{aligned} . \tag{12}$$

Some other examples and relations between subalgebras and partitions can be found in [13]

3 Applications to association schemes

For a complete account of the results and ideas in this section see [11, 12]. Anyone familiar with association schemes can see a classical example of a Bose-Mesner algebra in Example 1. As an example we will show how our setting can be use to sove the following problem: *to know whether an association scheme is P-polynomial or not.*

Definition 4. An association scheme $\mathcal{S} = (X, \{R_i\}_{i=0}^d)$ is P-polynomial if we can reorder the relations R_i so that the corresponding D_i is a polynomial p_i in D_1 with degree i.

Clearly, if $\mathcal{S}$ is a P-polynomial scheme we have that the set:

$$\{x_0 - 1, p(x_{i_1}), x_{i_2} - p_2(x_{i_1}), \dots x_{i_d} - p_d(x_{i_1})\} \tag{13}$$

is a reduced Gröbner basis for $\mathcal{I}$ for a pure lexicographical order where $x_{i_1} < x_{i_j}$, $j = 2, \dots, d$ ands $p(x_{i_1})$ is a polynomial in x_{i_1} whose roots are the eigenvalues of D_{i_1}. It follows that next proposition holds:

Proposition 3. *Let $\mathcal{S} = (X, \{R_i\}_{i=0}^d)$ be an association scheme and $\mathcal{I}$ its associated ideal. $\mathcal{S}$ is a P-polynomial scheme if and only if there is an pure lexicographical ordering for the variables x_{i_j} with $x_{i_0} = x_0, x_{i_1} < x_{i_j}, j > 1$ such that*

$$\{x_0 - 1, p(x_{i_1}), x_{i_2} - p_2(x_{i_1}), \dots x_{i_d} - p_d(x_{i_1})\} \tag{14}$$

is a Gröbner basis for $\mathcal{I}$ for that ordering, and the following conditions on the degree of the polynomials $p, p_1, \dots, p_d$ are satisfied:

$$degree(p_i) = i \quad \forall i = 2, \dots, d \quad degree(p) = d + 1 \tag{15}$$

Note that for an association scheme to be P-polynomial its Bose-Mesner algebra is the minimal algebra containing one of the relations but the converse is not true in general. The reason for this fact is that maybe that a relation

generates the whole algebra but we can not achieve the conditions on the degree of the polynomials p_i given in 15 (i.e., do not fullfil definition 5). This is the case of the following example taken from [11, ex.19] where any $D_i, i > 0$ generate the Bose-Mesner algebra but the scheme is not P-polynomial:

Example 5. Consider $X = \mathbb{Z}_m, m, r \in \mathbb{N}$ and $r < m$. The subgroup of $\mathbb{Z}_m^*$ generated by r and -1 acts on X by multiplication with orbits $\mathcal{O}_k$. The following relation defines an association scheme (2-orbit association scheme) on X:

$$xR_k y \Leftrightarrow x - y \in \mathcal{O}_k$$

When $m = 31, r = 2$ the orbits are:

$$\begin{aligned}&\mathcal{O}_0 = \{0\},\ \mathcal{O}_1 = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 15\}\\ &\mathcal{O}_2 = \{\pm 3, \pm 6, \pm 7 \pm 12, \pm 14\}, \mathcal{O}_3 = \{\pm 5, \pm 9, \pm 10, \pm 11, \pm 13\}\end{aligned}$$

The ideal $\mathcal{I}$ is given by:

$$\begin{aligned}&\{{x_2}^2 - 2x_1 - 3x_2 - 4x_3 - 10,\ x_2x_3 - 4x_1 - 4x_2 - 2x_3, x_0 - 1,\\ &\ x_1x_3 - 2x_1 - 4x_2 - 4x_3,\ x_1x_2 - 4x_1 - 2x_2 - 4x_3,\\ &\ {x_1}^2 - 3x_1 - 4x_2 - 2x_3 - 10,\ {x_3}^2 - 4x_1 - 2x_2 - 3x_3 - 10\}\end{aligned}$$

Let the plex. order $x_i < x_j, x_k$, $(i, j, k) \in \{(1, 2, 3), (2, 3, 1), (3, 1, 2)\}$, the reduced Gröbner basis arises to the following expressions:

$$\begin{aligned}x_0 &= 1,\\ x_j &= \frac{1}{32}\left(-{x_i}^3 - 6\,x_i + 15{x_i}^2 - 120\right),\\ x_k &= \frac{1}{16}\left({x_i}^3 - 18\,x_i - 7\,{x_i}^2 + 40\right),\\ 0 &= 80 - 20\,{x_i}^2 + 92\,x_i - 9\,{x_i}^3 + {x_i}^4\end{aligned} \tag{16}$$

Therefore, equations in (16), do not fulfill the conditions (on the degree of the polynomials) stated in the definition and hence the scheme is not P-polynomial.

Note also that in the case when the algebra is generated by one of the relations the resulting univariate polynomial is squarefree and it is just the characteristic polynomial of the relation that "spans" the whole algebra[2]. The main profit we get from proposition above is an algorithmic way of checking the P-polynomiality of an association scheme:

Algorithm 1 (Checking P-polynomiality).

- **Input** $\mathcal{F}$ *Structure equations of* $\mathcal{S}$,

[2]This means that any element in the algebra can be expressed by a formula of the generator and J, using the addition, the ordinary multiplication and the Hadamard product.

- **For** *i from* 1 *to d* **do**
  Compute *a reduced Gröbner basis for $\langle \mathcal{F} \rangle$ for a pure lexicographical monomial ordering where $x_i < x_j$ $j \neq i$*
  Check *the conditions on proposition above.*
  If *the conditions are fulfilled then* **Stop** *and*
  Return *The scheme is P-polynomial and the Gröbner basis computed* **fi**
  od
  Stop Return *The scheme is not P-polynomial*

Complexity of the algorithm is placed in the Gröbner basis computation, but since we are dealing 0-dimensional ideals and $\mathcal{F}$ is already a Gröbner basis, these computations can be done by FGLM techniques. Clearly the complexity is at most the same as d FGLM Gröbner basis computations. The algorithm can be easily modified to check whether the scheme is P-polynomial with respect to more than one relation or to check the minimal number of relations spanning the whole algebra. This last fact is important in coding theory for computing the Lloyd polynomials and metric properties of the scheme [11]. In that paper can be found many examples of how to apply this algorithm, we recall just two of them for showing the computations underlying the algorithm.

4 Applications to coding theory

For a complete account of the results and ideas in this section see [14]. The following definition of a code over a SFCA is motivated by the classical definition of cyclic codes. Cyclic codes are one of the classes of codes because they are easy to encode and decode due to their algebraic structure. Moreover, they are use as building blocks of many other codes such that Kerdock, Preparata, Justensen, quasy-cyclic codes and recently as blocks of Low Density Parity Check Codes.

Definition 5 (Code over a SFCA). Let $\mathcal{A}$ be a SFCA. We define a *code* $\mathcal{C}$ over $\mathcal{A}$ as a subalgebra of $\mathcal{A}$.

Example 6 (Cyclic codes). A cyclic code is just the ideal $\langle g(x) \rangle$ in $R = \mathbb{F}_q[x]/\langle x^n - 1 \rangle$ where $g(x) \in \mathbb{F}_q[x]$ and $g(x)|x^n - 1$.

Example 7 (Generalized cyclic codes). Let $f(x) \in \mathbb{F}[x]$ a monic polynomial with no repeated roots in the splitting field over $\mathbb{F}$. An $f(x)$-code is an ideal of the quotien ring $\mathbb{F}[x]/\langle f(x) \rangle$.

- If $f(x) = x^n - 1$ and $(\mathrm{char}(\mathbb{F}), n) = 1$ [3] we are in the case of a cyclic code.
- If $f(x) = x^n - c$ we are in the constan-cyclic case.
- Etc.

[3] Condition of the Maschke theorem. Means that the representation is completely reducible. See for example [3]

The Mattson-Solomon transform

In this section we will generalize the Mattson-Solomon transform. In their paper (see [15] or the book [10]) their defined a sort of "unnatural" multiplication $\star$ on the quotient ring $\mathbb{F}[x]/\langle x^n - 1\rangle$ in order to compute with the idempotents. Chillag [2] remark that $\star$ is equivalent to the multiplication rule in the diagonalization of the algebra $\mathcal{A} = \mathbb{F}[x]/\langle x^n - 1\rangle$. We will generalize this approach to a general SFCA.

Given a SFCA $\mathcal{A}$ over $\mathbb{F}$ and fixed a basis $\mathfrak{B} = \{b_1, \ldots, b_n\}$ we can consider the following isomorphism of algebras (Is a result of theorems 1 and 3) :

$$\mathcal{A} \overset{\sim}{\longleftrightarrow} M(\mathcal{A}; \mathfrak{B}) := \{M(a; \mathfrak{B}) \mid a \in \mathcal{A}\} \overset{\sim}{\longleftrightarrow} \operatorname{diag}(\mathcal{A}) \tag{17}$$

Definition 6 (Mattson-Solomon transform). Let $\mathcal{A}$ be a n-dimensional SFCA over $\mathbb{F}$ and $\mathfrak{B} = \{b_1, \ldots, b_n\}$ a basis of $\mathcal{A}$. We define the Mattson-Solomon polynomial of an element $a \in \mathcal{A}$ as

$$\mathrm{MS}(a) \doteqdot \sum_{i=1}^{n} \operatorname{diag}(a)_i x^{i-1}$$

where $\operatorname{diag}(a)_i$ is the i-th entry of the diagonalization of $M(a; \mathfrak{B})$.

Let $\mathbb{F}_n[x] \doteqdot \{f(x) \in \mathbb{F}[x] \mid \deg(f(x)) < n\}$ and consider the algebra $\mathcal{M}S = (\mathbb{F}_n[x], +, \star)$ where $+$ is the usual addition on $\mathbb{F}[x]$ and $\star$ is the componentwise multiplication.

Remark 4. In the cyclic case the diagonalizing matrix of the algebra is $X = \mathrm{Vandermonde}(1, \xi, \xi^2, \ldots, \xi^{n-1})$ where $\xi^n = 1$. Thus

$$\mathrm{MS}(a(x)) \doteqdot \sum_{i=1}^{n} a(\xi^{i-1}) x^{i-1}$$

i.e. The Fourier Transform.

Proposition 4. *$\mathcal{A}$ is isomorphic to $\mathcal{M}S$*

Proof. It is a direct consecuence of the discusion above. □

Characterization of the codes

The following result is similar to the well known case of cyclic codes (see for example [10]) and the case of f-circulant codes.

Theorem 6. *Let $\mathcal{A}$ be a SFCA and $\mathcal{C}$ a code over $\mathcal{A}$ generated by $g_1, \ldots, g_s$.*

- *$\mathcal{C}$ is a separable, semisimple, s-dimensional, commutative algebra over $\mathbb{F}$*
- *There exist a matrix X over an extension $\mathbb{K}$ of $\mathbb{F}$ such that*

$$X^{-1} M(c, \mathfrak{B}) X = \sum_{i=1}^{s} \operatorname{diag}(g_i)$$

- *In particular if* $\mathcal{C} = \mathbb{F}[g_1]$ *then* $c \in \mathcal{C}$ *iff* $\mathcal{T}(c) \leq \mathcal{T}(g_1)$.

Remark 5. The properties in the theorem above can be checked easily with the Gröbner basis setting in 2.

Remark 6. Last point in the theorem is just the classical characterization of the cyclic codes where $\mathcal{A} = \mathbb{F}[x]/x^n - 1$, $\mathcal{C} = \langle g(x) \rangle$ where $g | x^n - 1$. Clearly $c \in \mathcal{C}$ iff $c(\alpha_i) = 0$ for all α_i such that $g(\alpha_i) = 0$.

Remark 7. If we choose $\mathfrak{G} = \{g_1, \ldots, g_s\}$ to be a basis of $\mathcal{C}$ and choose $\mathfrak{G}'$ so that $\mathcal{A} = \langle \mathfrak{G} \rangle \bigoplus \langle \mathfrak{G}' \rangle$ and $\mathfrak{B} = \mathfrak{G} \bigcup \mathfrak{G}'$ then

$$M(a, \mathfrak{B}) = \begin{pmatrix} M(a, \mathfrak{G}) & 0 \\ 0 & M(a, \mathfrak{G}') \end{pmatrix}$$

5 What next?

Here we just point some further lines of research.

- **Association schemes.**
  We can also consider non-commutative association schemes. In that case we can consider the (right and left) multiplication tables, i.e. the (right and left) structure constants and rewrite a simmilar Gröbner structure for a non-commutative setting using border basis. The tools on [1] can be useful.

- **Coding theory.**

  § **Product codes**
  Product codes are defined as the Kroneker product of two codes. Clearly, they will be diagonalized by the diagonal matrix whose diagonal entries are the diagonalizing matrices of each code. So their Mattson Solomon transform can be easily determined.

  Is there a translation of theorem 4, page 573 in [10] for codes over SFCA's?

  § **Quasi-cyclic and quasi f circulant codes**
  The construction in [8] based in the Smith normal form and the transform approach in [9] allows us to develop a characterization of quasi f circulant codes.

References

[1] M. A. Borges-Trenard, M. Borges-Quintana, and T. Mora. Computing Gröbner bases by FGLM techniques in a non-commutative setting. *J. Symbolic Comput.*, 30(4):429–449, 2000.

[2] Chillag, D. Regular Representation of Semisimple Algebras, Separable Field Extensions, Group Characters, Generalized Circulants and Generalized Cyclic Codes, Linear Algebra and its Applications, 218, 147–183. 1995

[3] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras* Wiley Classics Library; A Wiley-Interscience Publication. New York: John Wiley Sons., 1962.

[4] Charles W. Curtis and Irving Reiner. *Methods of representation theory with applications to finite groups and orders. Volume 1.* Wiley Classics Library; A Wiley-Interscience Publication. New York: John Wiley Sons., 1990.

[5] Yurij A. Drozd and Vladimir V. Kirichenko. *Finite dimensional algebras.* Berlin: Springer-Verlag., 1994.

[6] Roger A. Horn and Charles R. Johnson. *Matrix analysis.* Cambridge: Cambridge University Press., 1985.

[7] Nathan Jacobson. *Basic algebra I. 2nd ed.* New York: W. H. Freeman and Company., 1985.

[8] K. Lally, P. Fitzpatrick *Algebraic structure of quasicyclic codes.* Discrete Applied Mathematics 111, 157–175 (2001)

[9] S. Ling and P. Sole, *On the algebraic structure of quasi-cyclic codes I: finite fields.* IEEE Trans. Inform. Theory, vol. IT-47, 2751–2759, Nov. 2001

[10] Macwilliams, F.; Sloane, N.J.A. The theory of error-correcting codes. North-Holland, 1977.

[11] Edgar Martínez-Moro. *Computations on character tables of association schemes*, CASC99. Springer Verlag, (1999), 293–307

[12] Edgar Martínez-Moro. *Properties of Commutative Association Schemes derived by FGLM Techniques*, International Journal of Algebra and Computation. 12-6 (2002) 849–865

[13] Edgar Martínez-Moro. *Regular Representations of Finite-dimensional Separable Semisimple Algebras and Gröbner Bases*, Journal of Symbolic Computation 37 (2004) 575–587

[14] Edgar Martínez-Moro. *On semisimple algebra codes: generator theory*, Submitted (2006).

[15] H.F. Mattson, G. Solomon A new treatment of Bose-Chaudhuri codesJour. SIAM. **9**,654 –669, 1961

[16] M. Möller, H.J. Stetter Multivariate polynomial equations with multiples zeros solved by matrix eigenproblemsNumer. Math. **70**,311 –329, 1995