Algebra and Discrete Mathematics
Number 3. **(2007).** pp. 99 – 112

RESEARCH ARTICLE

On semisimple algebra codes: generator theory

Edgar Martínez-Moro

Communicated by Yu. Drozd

Abstract. The class of affine variety codes is defined as the $\mathbb{F}_q$ linear subspaces of $\mathcal{A}$ a $\mathbb{F}_q$-semisimple algebra, where $\mathbb{F}_q$ is the finite field with $q = p^r$ elements and characteristic p. It seems natural to impose to the code some extra structure such as been a subalgebra of $\mathcal{A}$. In this case we will have codes that have a Mattson-Solomon transform treatment as the classical cyclic codes. Moreover, the results on the structure of semisimple finite dimensional algebras allow us to study those codes from the generator point of view.

Introduction

In [8] the authors define the affine variety codes as follows; Consider an ideal $I \subseteq \mathbb{F}_q[X_1, X_2, \ldots, X_n]$ where $\mathbb{F}_q$ is the finite field with $q = p^r$ elements and characteristic p. Let I_q be the ideal generated by

$$I + \langle X_1^q - X_1, X_2^q - X_2, \ldots, X_n^q - X_n \rangle$$

that is, the points in the variety $V(I_q)$ are the $\mathbb{F}_q$-rational points of $V(I)$. Since I_q is a 0-dimensional ideal and radical the coordinate ring

$$R = \mathbb{F}_q[X_1, X_2, \ldots, X_n]/I$$

Partially supported by Spanish MEC MTM2004-00876 and MTM2004-00958. This research was carried out while the author visited the Boole Center for Research in Informatics, University College Cork, Ireland.

2000 Mathematics Subject Classification: *13P10,94B05,94B15.*

Key words and phrases: *Semisimple Algebra, Mattson-Solomon Transform, Discrete Fourier Transform, Gröbner bases.*

is a semisimple $\mathbb{F}_q$-algebra and it is isomorphic to $\mathbb{F}_q^n$ as vector spaces. The isomorphism is usually named Mattson-Solomon transform (or Fourier transform in the cyclic case). Consider the points of $V(I_q)$ in some order $P_1, P_2, \ldots, P_n$, and define the evaluation map $\Phi : R \to \mathbb{F}_q^n$ given by

$$\Phi(f + I_q) = (f(P_1), f(P_2), \ldots, f(P_n)).$$

Let L be a $\mathbb{F}_q^n$-vector subspace of R, then the **affine variety code** $C^{\perp}(I, L) = \Phi(L)^{\perp}$ where the $\perp$ is the orthogonal complement as vector spaces for the usual dot product. These codes are the same as the evaluation codes proposed in [20]. Moreover, in [8] the authors proved that all $\mathbb{F}_q$-linear codes can be defined as affine variety codes and they give a procedure for decoding them based in Gröbner bases techniques.

In this contribution we will impose some extra structure on L as being a subalgebra of R. There are some results on the literature on codes defined as subalgebras of semisimple algebras, see for example [10, 11, 19] that are summarized and extended in [18]. In this contribution we take a "rootless" approach, that is we do not use roots of unity. Since the field $\mathbb{F}_q$ is perfect, the algebra R is also separable, thus we will use the techniques in [17] in order to study the codes, this allows have a simpler view of the structure of the code similar to the polynomial approach to cyclic codes. Moreover,these codes are important since they inherit the symmetries of the algebra, some well known cases are cyclic codes, nega-cyclic codes (i.e. codes over $\mathbb{F}[x]/(x^n + 1)$) or more general codes over $\mathbb{F}[x]/(f(x))$ where $f(x)$ is square-free , codes over $\mathbb{F}A$ where A is an abelian group, etc.

The outline of this contribution is as follows; In the second section we will define the codes and study some basic properties of 0-dimensional separable semisimple algebras. Several remarks and examples are presented in order to show the relationship of this codes with the well-known theory of cyclic codes. In section 3 we will derive some basic bounds such as the BCH bound.

1. Semisimple codes

From now on we will say $\mathbb{F}_q$-algebra for a finite dimensional commutative semisimple algebra $\mathcal{A}$ over $\mathbb{F}_q$ with 1. In particular, since $\mathbb{F}_q$ is a perfect field the algebra is separable, that is the minimal polynomial $m_a(x)$ of each element $a \in \mathcal{A}$ has no multiple roots in the splitting field of $m_a(x)$ over $\mathbb{F}_q$.

Definition 1. *Let $\mathcal{A}$ a $\mathbb{F}_q$-algebra. A semisimple code defined in $\mathcal{A}$ is a subalgebra of $\mathcal{A}$.*

Example 1. *Indeed the first example is a cyclic code as a subalgebra of*

$$\mathcal{A}_1 = \mathbb{F}_q[x]/\langle x^n - 1\rangle$$

where $\gcd(n, q) = 1$.

We will recall a results on the structure of semisimple finite dimensional algebras, for an exhaustive account see [4, 17].

Let $\mathcal{A}$ be a semisimple n-dimensional commutative algebra over a $\mathbb{F}_q$. Given a basis $\mathfrak{B} = \{b_1 = 1, \ldots, b_n\}$ of $\mathcal{A}$, and the multiplication table given by

$$b_i b_j = \sum_{k=1}^{n} m_{i,k}(b_j, \mathfrak{B}) b_k \qquad 1 \leq i, j, k \leq n, \quad m_{i,k}(b_j, \mathfrak{B}) \in \mathbb{F}_q \tag{1}$$

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

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

is called a set of **structure polynomials of the algebra** $\mathcal{A}$. The following result show us a polynomial representation of the algebra (See [17] for a proof).

Proposition 1. *Let* $\mathcal{A}$ *be a semisimple* n*-dimensional commutative algebra over a* $\mathbb{F}_q$ *and* F *a set of structure polynomials of* $\mathcal{A}$

$$\mathcal{A} \cong \mathbb{F}_q[x_1, \ldots, x_n]/\mathcal{I} \tag{3}$$

where $\mathcal{I}$ *is the ideal generated by* F*. Also* F *is a Gröbner basis with respect to a total-degree monomial ordering and the ideal is radical and 0-dimensional.*

Remark 1. *Note that there is no need of computing the Gröbner basis of* $\mathcal{I}$*, it arises from the multiplication table of the algebra* $\mathcal{A}$*. Moreover, the construction depends on the base* $\mathfrak{B}$ *but we can rebuild easily the Gröbner basis when there is a change of the base of the algebra by linear algebra techniques (see [17]), so we can always suppose that the code is taken as a subalgebra that is generated by some of the elements of the base* $\mathcal{B}$*.*

Example 2. *We will use the following "toy example" for understanding the theory during the paper, consider the finite field* $\mathbb{F}_5$ *and the algebra given by*

$$\mathcal{A}_2 = \mathbb{F}_5[x, y, z]/\mathcal{J} \tag{4}$$

where

$$\mathcal{J} = \langle x+y+z+1,\, y^2+y+z+1,\, yz^2+2z^3+yz+z^2-y, \\ z^4+z^3-2yz-y+1\rangle \tag{5}$$

for our convenience the set of polynomials generating $\mathcal{J}$ is a Gröbner basis with respect to the reverse degree lexicographical ordering where $x < y < z$ (note that $\mathcal{J}$ is the ideal generated by $\{(x-3)(x-1)(x-4), y^2-x, z+x+y+1\}$), but this is not the general case, moreover the algebra is usually presented by a multiplication table or rule on the elements of the vector space base of the algebra.
A vector space basis (consisting of monomials) of the quotient ring by the ideal $\mathcal{J}$ is given by

$$\mathfrak{B}_2 = \left\{x_1 = 1, x_2 = z^3, x_3 = z^2, x_4 = yz, x_5 = z, x_6 = y\right\} \tag{6}$$

thus a set of structure polynomials of the algebra $\mathcal{A}_2$, i.e. the multiplication table, is

$$\begin{aligned} F_2 = \{&x_1-1, x_2^2-(2x_2-2x_4+2x_3-x_6+x_5-2),\\ &x_2x_3-(2x_2+2x_4-2x_3+x_6-x_5+1),\\ &x_2x_4-(2x_2+2x_3+x_6+2x_5+2),\\ &x_2x_5-(-x_2+2x_4+x_6-1), x_2x_6-(-2x_2-2x_4+x_3+2x_6+2),\\ &x_3^2-(-x_2+2x_4+x_6-1), x_3x_4-(-2x_2-2x_4+x_3+2x_6+2),\\ &x_3x_5-(x_2), x_3x_6-(-2x_2-x_4-x_3+x_6),\\ &x_4^2-(x_2+x_4-x_6), x_4x_5-(-2x_2-x_4-x_3+x_6),\\ &x_4x_6-(-x_4-x_3-x_5), x_5^2-(x_3)\\ &x_5x_6-(x_4), x_6^2-(-x_5-x_6-1)\} \end{aligned} \tag{7}$$

Note that in this case the elements between () in the previous equation correspond to the normal forms of the products of the base in equation (6) with respect to the Gröbner basis in equation (5) due to the concrete representation we have chosen for the algebra $\mathcal{A}_1$.

Let $V(\mathcal{I}) = (P_1, P_2, \ldots, P_n)$ the points in the variety defined by $\mathcal{I}$, i.e. the roots of the system of equations in F in some extension field $\mathbb{F}$ of $\mathbb{F}_q$. We will denote $P_i = (p_{i1}, \ldots, p_{in})$ as row vectors. We can consider the **Mattson-Solomon** matrix

$$M = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ p_{21} & \cdots & p_{2n} \\ & \ddots & \\ p_{n1} & \cdots & p_{nn} \end{pmatrix} \tag{8}$$

Indeed M is a non-singular matrix and therefore its rowspace is $\mathbb{F}^n$. Moreover, if $a(X) \in \mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}$, the map

$$\Theta : \mathbb{F}[x_1, \ldots, x_n]/\mathcal{I} \longrightarrow \mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}$$

defined by

$$[\Theta(a)](\mathbf{x}) = \sum_{i=1}^{n} a(P_i)x_i \tag{9}$$

is the Mattson-Solomon transform. If $\circ$ is the multiplication of polynomials modulo the ideal $\mathcal{I}$ and $\star$ is the component wise product

$$\left(\sum a_i x_i\right) \star \left(\sum b_i x_i\right) = \left(\sum a_i b_i x_i\right)$$

then $\Theta : (\mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}, +, \circ) \to (\mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}, +, \star)$ is an isomorphism of rings (see for example [4]).
A matrix H given by selecting (not at random, see Section 1.1 below) some of the rows of M is the **parity check matrix of a subalgebra code** of $\mathcal{A}$ (see last item in Remark 3).

Remark 2. *Note that the standard monomials for $\langle F \rangle$ with respect to a total-degree monomial ordering are $\{x_1, x_2, \ldots, x_n\}$, therefore a representative of each element of $\mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}$ can be written as $\sum_{i=1}^{n} a_i x_i$, thus the Mattson-Solomon transform is equivalent to the matrix-vector multiplication $M \cdot \mathbf{a}^T$ where $\mathbf{a} = (a_1, \ldots, a_n)$.*

Example 3. *The previous approach is the same construction as for cyclic codes and the discrete Fourier transform, see [16] where the matrix M is given by the Fourier matrix*

$$M_1 = \left(\xi^{ij}\right)_{1 \le i,j \le n}$$

where ξ is a primitive n-th root of unity.

Example 4. *In the case of Example 2 the Mattson-Solomon matrix is given by*

$$M_2 = \begin{pmatrix} 1 & 3 & 4 & 2 & 2 & 1 \\ 1 & 4 & 1 & 1 & 4 & 4 \\ 1 & -\alpha & 4-2\alpha & 2+\alpha & 1-\alpha & \alpha \\ 1 & +\alpha & 4+2\alpha & 2-\alpha & 1+\alpha & -\alpha \\ 1 & 2 & 4 & 1 & 3 & 2 \\ 1 & 3 & 4 & 1 & 2 & 3 \end{pmatrix} \tag{10}$$

where α is a root of $x^2 + 2$, i.e. $\mathbb{F}_5(\alpha) \cong \mathbb{F}_{5^2}$.

1.1. Allowed rows.

Turning F to an adequate elimination monomial ordering (for example a pure lexicographic monomial ordering where $x_i < x_j$ for all $i \neq j$) we can easily compute the minimal polynomial $m(x_i)$ for each element x_i (see [17]) by eliminating the rest of the variables. Such change of order can be done by linear algebra techniques, since the ideal is 0-dimensional and radical (see [7] or [17] for the semisimple case). The roots are the elements of the column in H corresponding to x_i, so the rows we can choose depends on the multiplicity of the roots in the column and in the extension field of $\mathbb{F}_q$ that we are considering.
More formally, fixed an extension field $\mathbb{F}$ of $\mathbb{F}_q$, and a irreducible factorization of the minimal polynomial $m(x_i) = f_1 \cdot f_2 \cdot \ldots \cdot f_s$ in $\mathbb{F}[x_i]$, if a row corresponding to the value ν in position i is included in H, then there must be a j $1 \leq j \leq s$ such that $f_j(\nu) = 0$ and all the rows corresponding to roots of f_j must be also included in H.

Example 5. *Consider the polynomials in the Gröbner basis F_2 in Example 2. Let $\mathcal{G}_5$ be a Gröbner basis of the ideal generated by F_2 in a pure lexicographic monomial ordering where $x_5 < x_i$, $i \neq 2$, $1 \leq i \leq n$, and*

$$\langle m_5(x_5) \rangle = \mathbb{F}_5[x_5] \cap \mathcal{G}_5$$

then $m_5(x_5) = (x_5+1)(x_5+2)(x_5+3)(x_5^2+3x_5+3)$ in $\mathbb{F}_5[x_2]$. Therefore, if the first row of M_2 is included in H also has to be included the last one (both corresponding to $x_5 - 2$). We have the same situation between the third and fourth row (corresponding to the roots of $x_5^2 + 3x_5 + 3$). Note that in $\mathbb{F}(\alpha)$ this last two rows can be separated.

Note that if we have a **separating element** in $\mathcal{A}$, that is, a column with all it entries different, we can chose any combination of rows (if we allow the code being defined in an extension field of $\mathbb{F}_q$ large enough), for example, this is the case in cyclic codes.

Example 6. *Considering Example 2, x_6 is not a separating element in $\mathbb{F}_5$ since $m_{\mathbb{F}_5}(x_6) = (x_6 + 1)(x_6 + 2)(x_6 + 3)(x_6 + 4)(x_6^2 + 2)$ but it is a separating element in $\mathbb{F}(\alpha)$ since $m_{\mathbb{F}_5(\alpha)}(x_6) = (x_6 + 1)(x_6 + 2)(x_6 + 3)(x_6 + 4)(x_6 + \alpha)(x_6 - \alpha)$.*

1.2. Generator theory.

Up to now we have made use of the Mattson-Solomon matrix for defining our codes. Our purpose is devise a root-free theory (i.e. there is no need of computing M or H). That is generalize in a straightforward way the generator polynomial/ parity check polynomial construction of cyclic

codes where all the codes are generated by a polynomial dividing $x^n - 1$ and checked with $h(x) = x^n - 1/g(x)$.

Fix an extension field $\mathbb{F}$ of $\mathbb{F}_q$. Consider the variety $V(\mathcal{I}')$ where $\mathcal{I}' = I(F')$, the ideal generated by F',

$$F' = F \cup \{g(x_{i_1}), \ldots, g(x_{i_s})\} \tag{11}$$

where F is the Gröbner basis in equation (2) associated to $\mathcal{A}$ and $g(x_{i_j})|m_{\mathbb{F}}(x_{i_j})$ divides the minimal polynomial of the element in $\mathcal{A}$ corresponding to x_{i_j} for some $1 \leq i_j \leq n$. Then the variety $V(\mathcal{I}')$ contains the allowed rows of H for a subalgebra code of $\mathcal{A}$.

Definition 2. *Let $\mathcal{C}$ be subalgebra code over the algebra $\mathcal{A} \cong \mathbb{F}_q[x_1, \ldots, x_n]/\mathcal{I}$ whose parity check matrix is a submatrix from the Mattson-Solomon matrix we define the **generator ideal** $\mathcal{I}_\mathcal{C}$ as the ideal generated by*

$$F_\mathcal{C} = F \cup \{g_i(x_i)\}_{i=1}^n \tag{12}$$

where F is the set of structure equations of the algebra $\mathcal{A}$ and $g_i(x_i)|m_{\mathbb{F}}(x_i)$, and $V(F_\mathcal{C})$ is the set of rows of its parity check matrix.

Remark 3.

- *Note that, as in the classical theory, what we are considering as codes is the preimage by Θ of the subalgebra given by choosing the elements with some fixed zero positions in the Mattson-Solomon codomain.*
- *Eventually, for some indices i_j, $g_{i_j}(x_{i_j}) = m_{\mathbb{F}}(x_{i_j})$, then we will not write them down since $m_{\mathbb{F}}(x_{i_j})$ is already in the ideal generated by F.*
- *We will call **parity check variety** to $V(F_\mathcal{C})$ since the point in the variety are the rows of a parity check matrix of the code.*
- *Note also that strictly speaking the matrix H whose rows are the points in $V(F_\mathcal{C})$ is not a parity check matrix of the code since maybe that its coefficients are not in $\mathbb{F}_q$, anyway we can construct one using the subfield code construction (see for example [12]).*

Moreover, the above construction can be made by linear algebra algorithms, since a lexicographic Gröbner basis $\mathcal{G}$ of $\mathcal{I}_\mathcal{C}$ can be derived directly from F without using Gröbner bases computation (see [17]). This construction of the defining $F_\mathcal{C}$ generalizes in a straightforward way the polynomial construction of cyclic codes and plays the same role as $g(x)$ the generator polynomial of a cyclic code.

Example 7. *Consider the semisimple algebra $\mathcal{A}_2$ in Example 2. We have compute (see [17]) the following minimal polynomials (over $\mathbb{F}_5$) for the elements in the base in equation (6):*

$$\begin{aligned} m(x_2) =&(x_2+1)(x_2+2)(x_2+3)(x_2^2+2)\\ m(x_3) =&(x_3+1)(x_3+4)(x_3^2+2x_3+4)\\ m(x_4) =&(x_4+3)(x_4+4)(x_4^2+x_4+1)\\ m(x_5) =&(x_5+1)(x_5+2)(x_5+3)(x_5^2+3x_5+3)\\ m(x_6) =&(x_6+1)(x_6+2)(x_6+3)(x_6+4)(x_6^2+2) \end{aligned} \tag{13}$$

For example, consider the code $\mathcal{C}$ with generator ideal generated by

$$F_{\mathcal{C}} = F \cup \{(x_6+1)(x_6+2)(x_6+3)(x_6+4), (x_3+1)\}$$

A Gröbner basis with respect to the degree lexicographical ordering for the generator ideal can be computed by linear algebra techniques (see [17])

$$\begin{aligned} \mathcal{I}_{\mathcal{C}} = \langle & x_4 - 2x_5 - 2x_6 - 1, x_3 + 1, x_2 - 2x_4 - x_6 + 2\\ & x_1 - 1, x_6^2 + x_5 + x_6 + 1, x_5x_6 - x_4, x_5^2 + 1\rangle \end{aligned} \tag{14}$$

and the parity check matrix correspond to rows 1,5,6 of matrix M_2 in Example 4. Note also that the election of the generators $g_i(x_i)$ is not unique, for example $F \cup \{(x_5^2+1)\}$ defines the same code, but indeed the generator ideal for the code is unique.

Given a monomial ordering $<$ and an ideal $\mathcal{I} \in \mathbb{F}_q[x_1, \ldots, x_n]$, the **footprint** of $\mathcal{I}$ w.r.t. $<$ is

$$\Delta_<(\mathcal{I}) = \{M \text{ monomial in } F_q[x_1, \ldots, x_n] \mid M \text{ is not leading monomial in } \mathcal{I}\}$$

If $\mathcal{I}$ is a radical ideal $|\Delta_<(\mathcal{I})|$ gives us the size of the variety $V(\mathcal{I})$ in the algebraic closure of $\mathbb{F}_q$. Note also that $\Delta_<(\mathcal{I})$ can be easily derived from a Gröbner basis G of $\mathcal{I}$ (see for example [6]). Thus the dimension of the code $\mathcal{C}$ with parity check variety given by $F_{\mathcal{C}}$ is $k = n - |\Delta_<(\langle F_{\mathcal{C}}\rangle)|$

Remark 4. *Using a lexicographical monomial ordering for F we can detect the minimal number of generators in the base needed to span the whole algebra (not as a linear subspace but as a subalgebra) see [17] , thus the g_i in the previous remark can be chosen polynomials in the variables corresponding to the generating elements.*

Remark 5 (Algebraic structure.)**.** *This codes could be seen as contractions of the adequate multidimensional cyclic codes given as subalgebras of*

$$\mathbb{F}_{q^r}[X_1, X_2, \ldots, X_n]/\langle X_1^m - 1, X_2^m - 1, \ldots, X_n^m - 1\rangle$$

Table 11.1: Cyclic vs. semisimple codes

CYCLIC CODES	SEMISIMPLE CODES
$\mathbb{F}_q[x]/(x^n-1)$	$\mathcal{A} \cong \mathbb{F}_q[x_1,\ldots,x_n]/\mathcal{I}, \quad \mathcal{I} = \langle F \rangle$
$g(x) \vert (x^n-1)$	$F_{\mathcal{C}} = F \cup \{g_i(x_i)\}_{i=1}^n, \quad g_i(x_i) \vert m_{\mathbb{F}_q}(x_i)$
$\deg g(x)$	$\vert\Delta(\langle F_{\mathcal{C}} \rangle)\vert$

for an adequate extension field $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$ and follow the classical theory on products of sets of cyclotomic sets on [18], or derived the analogous structure theorems in [2] for the multidimensional cyclic codes case in terms of trace codes. But in this case the polynomial approach to the semisimple codes in this communication seems much more simpler due to the nice structure of the ideal defining the algebra.

1.3. Encoding and decoding.

The purpose of the paper is to clarify the generator theory and generalize the construction of cyclic codes. Nevertheless we will give some notes and clues to some related works that can be used for encoding and decoding.

Systematic encoding.

A systematic encoding function for our setting can be constructed as follows (see [13] for a similar construction);
Let $\mathcal{G}$ a Gröbner basis of the ideal $\mathcal{I}_{\mathcal{C}}$ generated by $F_{\mathcal{C}}$ in a total-degree monomial ordering ($<$).

1. The information positions are the coefficients of the non-standard monomials for $\mathcal{I}_{\mathcal{C}}$ (i.e. $\Delta_<(\mathcal{I}) \setminus \Delta_<(\mathcal{I}_{\mathcal{C}})$).

2. The parity checks are the coefficients of the monomials in $\Delta_<(\mathcal{I}_{\mathcal{C}})$.

3. The following algorithm gives a systematic encoder for the code $\mathcal{C}$

   - **Input**: w a linear combination of monomials in $\Delta_<(\mathcal{I}) \setminus \Delta_<(\mathcal{I}_{\mathcal{C}})$.
   - Compute $\bar{w} = \mathrm{rem}(w, \mathcal{G})$, the remainder on division.
   - **Output**: $w - \bar{w}$.

The output clearly represents a codeword since $w - \bar{w} \in \mathcal{I}_{\mathcal{C}}$.

Example 8. *Consider the code given by the ideal $\mathcal{I}_\mathcal{C}$ in (14) in Example 7. $\Delta_<(\mathcal{I}) \setminus \Delta_<(\mathcal{I}_\mathcal{C}) = \{x_2, x_3, x_4\}$. Thus if we want to encode $w = 3x_2 + 3x_3 + 2x_4$ we compute*

$$\bar{w} = \operatorname{rem}(3x_2 + 3x_3 + 2x_4, \mathcal{G}) = x_5 - x_6 - 1$$

and the encoded word is $x_1+3x_2+3x_3+2x_4-x_5+x_6$. (Note that $x_1 = 1$).

Remark 6. *Note that from the algorithm above is easy to derive a generator matrix of the code just by encoding the elements in the set $\Delta_<(\mathcal{I}) \setminus \Delta_<(\mathcal{I}_\mathcal{C})$.*

Example 9. *Following Example 8, we have*

$$\operatorname{rem}(x_2, \mathcal{G}) = -x_5, \quad \operatorname{rem}(x_3, \mathcal{G}) = -1, \quad \operatorname{rem}(x_4, \mathcal{G}) = 2x_5 + 2x_6 + 1$$

thus

$$\left(\begin{array}{c|ccc|cc} 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 4 & 0 & 0 & 1 & 3 & 3 \end{array}\right) \tag{15}$$

is a a column-permuted systematic generator matrix.

A note on the syndrome variety.

Given a semisimple code $\mathcal{C}$ defined by a generator ideal $\mathcal{I}_\mathcal{C}$. We have that if $r = \sum_{i=1}^n r_i x_i$ is a received word then the syndromes of r are

$$s_j = \sum_{i=1}^{n} r_i P_{ji} \tag{16}$$

where j ranges in the allowed rows of the Mattson-Solomon matrix of the algebra that correspond to the parity check matrix of the code. If all the syndromes are zero then r belongs to the code.

A brute force approach to the decoding problem would be to find all the solutions for the possible syndromes. Suppose t errors have occur and let $\mathcal{G}$ be a Gröbner basis of $\mathcal{I}_\mathcal{C}$. Consider the following equations:

$$f_j = \sum_{l=1}^{t} y_l x_l - z_j$$

and $\sigma_j = z_j^{q^m} - z_j$, $\lambda_i = y_i^{q-1} - 1$ for adequate indices depending on the extension field considered, since the z_i's represent the syndromes and the y_i's the error values. Consider the set of polynomials

$$\{f_j, \sigma_j, \lambda_i\}_{i,j} \cup \mathcal{G}$$

The variety generated by those polynomials defines the (classical) **Chen-Reed-Helleseth-Truong syndrome variety** of the code (see [5] for further explanations) used for decoding and finding the minimum distance (see [15] and [21]). From this it is clear that we can use Gianni-Kalkbrenner Gröbner shape Theorem (see [3]) in order to get the information about the ideal generated by that set of equations. Unfortunately, from the practical point of view, using elimination in order to solve the system for (x_i, y_i) is nearly impossible when n and t are big enough.
A more clever approach to the decoding problem making use of the concept of a key equation can be found in [14].

2. A van Lint-Wilson bound. BCH codes.

Definition 3. *Let $\mathbb{F}$ any extension field of the ground field of the code and $S \subset \mathbb{F}^n$. A sequence $I_0, I_1, I_2, \ldots$ of subsets of $\mathbb{F}^n$ is an independent sequence with respect to S provided that:*

1. *$I_0 = \emptyset$,*
2. *If $i > 0$ either $I_i = I_j \cup \{\Lambda_1\}$ for some $0 \leq j < i$ such that $I_j \subseteq S$ and $\Lambda_1 \in \mathbb{F}^n \setminus S$ or $I_i = \Lambda_2 \star I_j$ for some $0 \leq j < i$ and $\Lambda_2 \in (\mathbb{F} \setminus \{0\})^n$, where $\star$ is the component-wise product.*

Definition 4. *A subset $I \subseteq \mathbb{F}$ is independent with respect to S provided that I is in an independent sequence with respect to S.*

Proposition 2 (van Lint-Wilson bound)**.** *Let $\mathbb{F}$ a finite field. The number of nonzero coefficients of a linear polynomial $f(\mathbf{x}) \in \mathbb{F}[X_1, \ldots, X_n]$ is not less than the cardinality of any independent set with respect the hyperplane $S = \{P \in \mathbb{F}^n \mid f(P) = 0\}$.*

Proof. Let $f(\mathbf{x}) = c_1 x_{i_1} + c_2 x_{i_2} + \ldots + c_w x_{i_w}$ where $c_j \neq 0$ for $1 \leq j \leq w$ and let I be any independent set w.r.t. S. Let $I_0, I_1, I_2, \ldots$ be an independent sequence with respect to S such that $I_k = I$ for some $k \geq 0$. Consider the projection of I given by

$$\Pi(I) = \{(P_{i_1}, \ldots P_{i_w}) \in \mathbb{F}^w \mid P \in I\}$$

If the vectors in $\Pi(I)$ are linearly independent in $\mathbb{F}^w$ them $w \geq |\Pi(I)| = |I|$.

We complete the proof by showing that $\Pi(I_k)$ is linearly independent by induction on k. Consider $I_0 = \emptyset$, thus $\Pi(I_0)$ is linearly independent. Assume now that $\Pi(I_j)$ is linearly independent for $0 \leq j < k$. Fist suppose that there exist a j with $0 \leq j < k$ such that $I_k = I_j \cup \{\Lambda_1\}$

where $I_j \subseteq S$ and $\Lambda_1 \in \mathbb{F}^n \setminus S$. By the induction hypothesis $\Pi(I_j)$ is linearly independent and also orthogonal to $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ since $f(P) = 0$ for all $P \in S$. Since $\Lambda_1 \notin S$ then $f(\Lambda_1) \neq 0$ and thus its projection is not orthogonal to $\mathbf{c}$. Thus $\Pi(I_k) = \Pi(I_j \cup \{\Lambda_1\})$ is linearly independent. Now suppose the remaining case, there exist a j with $0 \leq j < k$ and $\Lambda_2 \in (\mathbb{F} \setminus \{0\})^n$ such that $I_k = \Lambda_2 \star I_j$. Then $\Pi(I_k) = D\Pi(I_j)$ where D is the non singular diagonal matrix $\mathrm{diag}(\Lambda_2)$, therefore the linear independence of $\Pi(I_k)$ follows from the linear independence of $\Pi(I_j)$. □

Corollary 1 (BCH bound)**.** *Let $\mathcal{C}$ a $[n, k]$ semisimple code over $\mathbb{F}$ and α a primitive element of $\mathbb{F}$ and $\mathcal{I}_\mathcal{C}$ its generator ideal, suppose that there is a $\mathbf{c} \in \mathcal{C}$ and $\mathbf{c}(\mathbf{x})$ its polynomial representation with $\mathbf{c}(\alpha^b, \mathbf{h}_0) = \mathbf{c}(\alpha^{b+1}, \mathbf{h}_1) = \cdots = \mathbf{c}(\alpha^{b+w-1}, \mathbf{h}_{w-1}) = 0$ where the $\mathbf{h}_j$ vectors have no zero components and $\mathbf{c}(\alpha^{b+w}, \mathbf{h}_w) \neq 0$. Then $\mathrm{wt}(c) \geq w + 1$.*

Proof. Let $S = V(\mathcal{I}_\mathcal{C})$. Clearly $(\alpha^{b+i}, \mathbf{h}_i) \in S$ for $0 \leq i \leq w - 1$ and $(\alpha^{b+w}, \mathbf{h}_w) \notin S$. Consider the following sequence, $A_0 = \emptyset$, $A_{2i+1} = A_{2i} \cup \{(\alpha^{b+w}, \mathbf{h}_w)\}$ for $0 \leq i \leq w$ and $A_{2i} = (\alpha^{-1}, \mathbf{t}_i) \star A_{2i-1}$ for $1 \leq i \leq w$ and $\mathbf{t}_i$ are chosen such that $\mathbf{t}_i \star \mathbf{h}_i = \mathbf{h}_{i-1}$.
Therefore $A_{2i} = \{(\alpha^{b+w-1}, \mathbf{h}_{w-1}), \ldots, (\alpha^{b+w-i-1}, \mathbf{h}_{w-i-1})\} \subseteq S$ for $0 \leq i \leq w$ and $A_0, \ldots, A_{2w+1}$ is an independent sequence with respect to S, thus by the previous proposition $\mathrm{wt}(c) \geq w + 1$. □

Remark 7. *Note that there is no inconvenience of choosing any other coordinate for the consecutive roots of the primitive element.*

Corollary 2 (Generalized BCH bound)**.** *Let $\mathcal{C}$ a $[n, k]$ semisimple code over $\mathbb{F}$ and $\mathcal{I}_\mathcal{C}$ its generator ideal generated by*

$$F_\mathcal{C} = F \cup \{g_i(x_i)\}_{i=1}^n$$

and $g_i(x_i)$ divides the minimal polynomial of the element in $\mathcal{A}$ corresponding to x_i. Suppose the minimal polynomial for each x_i has nonzero independent coefficient. Then:

$$\mathrm{d}(\mathcal{C}) \geq \max\{d(x_i)\}$$

where $d(x_i)$ is the maximum of consecutive powers of a primitive element of $\mathbb{F}$ as roots of the minimal polynomial of x_i in $\mathbb{F}[x_1, \ldots, x_n]/\mathcal{I}_\mathcal{C}$ and $\mathrm{d}(\mathcal{C})$ is the minimal distance of the code.

Proof. Follows directly from the remark and corollary above. □

Remark 8. *Hartmann-Tzeng-Roos bound can be generalized in the same way.*

3. Conclusions

In this paper we have shown a generator theory for codes defined as subalgebras of semisimple algebras. This class of codes contain some well known codes as cyclic codes or abelian codes. Usual treatment of this type of codes involves a discrete Fourier transform, whereas our approach is a "rootless" one, that is we do not use roots of unity. Finally we have extend some classical bounds to our codes.

Acknowledgments

The author wants to thank Patrick Fitzpatrick and Massimiliano Sala for their useful discussions and hints during his visit to the Boole Center for Research in Informatics, University College Cork, Ireland. All the computations were carried out with Singular 3.0 [9].

References

[1] Adams,W.; Loustaunau, P. (1994) An introduction to Gröbner bases. Graduate Studies in Mathematics, 3. American Mathematical Society, Providence, RI.

[2] Bierbrauer, J. (2002) The theory of cyclic codes and a generalization to additive codes. Des. Codes Cryptogr. 25, no. 2, 189–206.

[3] Caboara, M.; Mora, T. (2002) The Chen-Reed-Helleseth-Truong decoding algorithm and the Gianni-Kalkbrenner Gröbner shape theorem. Appl. Algebra Engrg. Comm. Comput. 13, no. 3, 209–232.

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

[5] Chen,X. ; Reed, I. S.; Helleseth, T. and Truong, T. K. (1995) Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance. IEEE Transactions on Information Theory, vol. 40, no. 5, 1654-1661.

[6] Cox, Little, O'Shea. (1996) Ideals, Varieties, and Algorithms. Second Edition, 1996 Springer-Verlag

[7] Faugère, J.; Gianni, P.; Lazard, D. and Mora, T. (1995) Efficient computation of zero-dimensional Gröbner bases by change of ordering, J. Symbolic Comput., No. 4, 16, 329–344.

[8] Fitzgerald, J. ; Lax, R.F. (1998) Decoding affine variety codes using Gröbner bases. Designs, Codes and Cryptography. 13, no. 2, 147-158.

[9] Greuel, G.-M.; Pfister, G. and Schönemann, H. (2005) Singular 3.0. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern. `http://www.singular.uni-kl.de`.

[10] Ikai, T; Kosako, H.; Kojima, Y. (1974) Two-dimensional cyclic codes. Electron. Comm. Japan 57 (1974/75), no. 4, 27–35.

[11] Imai, H. (1977) A theory of two-dimensional cyclic codes. Information and Control 34, no. 1, 1–21.

[12] Ling, S.; Xing, C. (2004) Coding theory: A first course. Cambridge University Press.

[13] Little, J.B. (1998) Applications to coding theory. In Applications of computational algebraic geometry. Proceedings of Symposia in Applied Mathematics vol. 53. American Mathematical Society.

[14] Little, J.B. (2005) A key equation and the computation of error values for codes from order domains `http://www.arxiv.org/abs/math.AC/0303299`.

[15] Loustaunau, P.; York, E. V. (1997) On the decoding of cyclic codes using Gröbner bases. Appl. Algebra Engrg. Comm. Comput. 8, no. 6, 469–483.

[16] MacWilliams, F.J. and Sloane, N.J.A. (1985) The theory of error-correcting codes. Parts I, II. (3rd repr.) North-Holland Mathematical Library, Vol. 16. Amsterdam (Elsevier).

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

[18] Poli, A. and Huguet, Ll. (1988) *Codes correcteurs: théorie et applications*, Masson.

[19] Poli,A. (1985) *Important algebraic calculations for n-variable polynomial codes.*, Disc. Math., vol. 56, pp. 255–264.

[20] Saints, K. and Heegard, C. (1995) Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Grobner bases. IEEE Transactions on Information Theory, vol. 41, no. 6, 1733–1751.

[21] Sala, M. (2002) Groebner bases and distance of cyclic codes. Appl. Algebra Engrg. Comm. Comput. 13, no. 2, 137–162.

Contact information

E. Martínez-Moro Dpto. de Matemática Aplicada
Universidad de Valladolid
Campus de los Pajaritos
Soria,Castilla
42004 Spain.
E-Mail: `edgar@maf.uva.es`
URL: `www.math.arq.uva.es/∼edgar/`

Received by the editors: 10.02.2006
and in final form 25.01.2008.