Projective Segre Codes

Rafael H. Villarreal*, joint work with Azucena Tochimani and Maria Vaz Pinto

Departamento de Matemáticas
CINVESTAV-IPN, México

Special Session on Homological and Combinatorial Commutative Algebra

Meeting AMS, EMS, SPM
Porto, Portugal, June 10–13, 2015.

Let a_1, a_2 be positive integers and let $\mathbb{P}^{a_1-1}$, $\mathbb{P}^{a_2-1}$, $\mathbb{P}^{a_1a_2-1}$ be *projective spaces* over a field K.

The *Segre embedding* is given by

$$\begin{array}{rcl} \psi\colon \mathbb{P}^{a_1-1} \times \mathbb{P}^{a_2-1} & \to & \mathbb{P}^{a_1a_2-1} \\ ([\alpha_1, \ldots, \alpha_{a_1}], [\beta_1, \ldots, \beta_{a_2}]) & \to & [\alpha_i\beta_j], \end{array}$$

$[\alpha_i\beta_j] = [\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_{a_2}, \ldots, \alpha_{a_1}\beta_1, \alpha_{a_1}\beta_2, \ldots, \alpha_{a_1}\beta_{a_2}]$.
The map ψ is well-defined and injective.

Given $\mathbb{X}_i \subset \mathbb{P}^{a_i-1}$, $i = 1, 2$, the image of $\mathbb{X}_1 \times \mathbb{X}_2$ under the map ψ, denoted by $\mathbb{X}$, is called the *Segre product* of $\mathbb{X}_1$ and $\mathbb{X}_2$.

Consider the following polynomial rings over a field K with the standard grading:

$$K[\mathbf{x}] = K[x_1, \dots, x_{a_1}] = \oplus_{d=0}^{\infty} K[\mathbf{x}]_d,$$
$$K[\mathbf{y}] = K[y_1, \dots, y_{a_2}] = \oplus_{d=0}^{\infty} K[\mathbf{y}]_d,$$
$$K[\mathbf{t}] = K[t_{1,1}, \dots, t_{a_1,a_2}] = \oplus_{d=0}^{\infty} K[\mathbf{t}]_d.$$

The *vanishing ideal* of $\mathbb{X}_1$ (resp. $\mathbb{X}_2$) is the ideal of $K[\mathbf{x}]$ (resp. $K[\mathbf{y}]$) generated by the homogeneous polynomials that vanish at all points of $\mathbb{X}_1$ (resp. $\mathbb{X}_2$).

The *vanishing ideal* $I(\mathbb{X})$ of $\mathbb{X}$ is a graded ideal of $K[\mathbf{t}]$, where the $t_{i,j}$ variables are ordered as $t_{1,1}, \dots, t_{1,a_2}, \dots, t_{a_1,1}, \dots, t_{a_1,a_2}$.

Notation for Hilbert function and invariants of $K[\mathbf{t}]/I(\mathbb{X})$:

- $H_{\mathbb{X}}(d) =$ Hilbert function of $K[\mathbf{t}]/I(\mathbb{X})$,
- $\operatorname{reg} K[\mathbf{t}]/I(\mathbb{X}) =$ regularity index,
- $\deg K[\mathbf{t}]/I(\mathbb{X}) =$ degree.

The *coordinate ring*

$$K[\mathbf{t}]/I(\mathbb{X})$$

and its algebraic invariants can be expressed in terms of the coordinate rings

$$K[\mathbf{x}]/I(\mathbb{X}_1) \text{ and } K[\mathbf{y}]/I(\mathbb{X}_2).$$

To see this we need to define the Segre product.

Definition

Let $A = \bigoplus_{d \geq 0} A_d$, $B = \bigoplus_{d \geq 0} B_d$ be two standard algebras over a field K. The *Segre product* of A and B, denoted by $A \otimes_S B$, is the graded algebra

$$A \otimes_S B := (A_0 \otimes_K B_0) \oplus (A_1 \otimes_K B_1) \oplus \cdots \subset A \otimes_K B,$$

with the normalized grading $(A \otimes_S B)_d := A_d \otimes_K B_d$ for $d \geq 0$. The tensor product algebra $A \otimes_K B$ is graded by

$$(A \otimes_K B)_p := \sum_{i+j=p} A_i \otimes_K B_j.$$

Example

The Segre product of $K[\mathbf{x}]$ and $K[\mathbf{y}]$ is

$$K[\mathbf{x}] \otimes_{\mathcal{S}} K[\mathbf{y}] \simeq K[\{x_i y_j \mid 1 \leq i \leq a_1,\ 1 \leq j \leq a_2\}],$$

and the tensor product of $K[\mathbf{x}]$ and $K[\mathbf{y}]$ is

$$K[\mathbf{x}] \otimes_K K[\mathbf{y}] \simeq K[\mathbf{x}, \mathbf{y}].$$

The next result is well-known assuming that $\mathbb{X}_1$ and $\mathbb{X}_2$ are projective algebraic sets.

Theorem

If $\mathbb{X}$ is the Segre product of $\mathbb{X}_1$ and $\mathbb{X}_2$, then:

(a) $K[\mathbf{x}]/I(\mathbb{X}_1) \otimes_{\mathcal{S}} K[\mathbf{y}]/I(\mathbb{X}_2) \simeq K[\mathbf{t}]/I(\mathbb{X})$.

(b) $(K[\mathbf{x}]/I(\mathbb{X}_1))_d \otimes_K (K[\mathbf{y}]/I(\mathbb{X}_2))_d \simeq (K[\mathbf{t}]/I(\mathbb{X}))_d$, $d \geq 0$.

(c) $H_{\mathbb{X}_1}(d) H_{\mathbb{X}_2}(d) = H_{\mathbb{X}}(d)$ *for* $d \geq 0$.

(d) $\mathrm{reg}(K[\mathbf{t}]/I(\mathbb{X})) = \max\{\mathrm{reg}(K[\mathbf{x}]/I(\mathbb{X}_i))\}_{i=1}^{2}$.

(e) $\deg(K[\mathbf{t}]/I(\mathbb{X})) = \deg(K[\mathbf{x}]/I(\mathbb{X}_1)) \deg(K[\mathbf{y}]/I(\mathbb{X}_2)) \binom{\rho_1+\rho_2-2}{\rho_1-1}$,
where $\rho_1 = \dim(K[\mathbf{x}]/I(\mathbb{X}_1))$, $\rho_2 = \dim(K[\mathbf{y}]/I(\mathbb{X}_2))$.

Linear Codes

Let $K = \mathbb{F}_q$ be a finite field and let C be a $[s, k]$ *linear code* of *length* s and *dimension* k, that is, C is a linear subspace of K^s with $k = \dim_K(C)$.

Given a subcode D of C, the *support* of D is:

$$\chi(D) := \{i \mid \exists\,(a_1, \ldots, a_s) \in D,\ a_i \neq 0\}.$$

The rth *generalized Hamming weight* of C is:

$$\delta_r(C) := \min\{|\chi(D)| :\ D \text{ is a subcode of } C,\ \dim_K(D) = r\}.$$

If $r = 1$, $\delta_1(C)$ is the *minimum distance* of C.

Direct product codes

Let $C_1 \subset K^{s_1}$ and $C_2 \subset K^{s_2}$ be two linear codes of dimensions k_1 and k_2, respectively.

The *direct product* of C_1 and C_2, denoted by $C_1 \underline{\otimes} C_2$, is the linear code consisting of all $s_1 \times s_2$ matrices in which the rows belong to C_2 and the columns to C_1.

Proposition (Wei and Yang, IEEE Trans. Inform., 1993)

(a) *$C_1 \underline{\otimes} C_2$ has length $s_1 s_2$, dimension $k_1 k_2$, and minimum distance $\delta_1(C_1)\delta_1(C_2)$.*

(b) $\delta_2(C) = \min\{\delta_1(C_1)\delta_2(C_2), \delta_2(C_1)\delta_1(C_2)\}$.

Consider the bilinear map ψ_0 given by

$$\begin{aligned} \psi_0 \colon K^{s_1} \times K^{s_2} &\longrightarrow M_{s_1 \times s_2}(K) \\ ((a_1, \ldots, a_{s_1}), (b_1, \ldots, b_{s_2})) &\longmapsto \begin{bmatrix} a_1 b_1 & a_1 b_2 & \ldots & a_1 b_{s_2} \\ a_2 b_1 & a_2 b_2 & \ldots & a_2 b_{s_2} \\ \vdots & \vdots & & \vdots \\ a_{s_1} b_1 & a_{s_1} b_2 & \ldots & a_{s_1} b_{s_2} \end{bmatrix} \end{aligned}$$

Lemma

There is an isomorphism of K-vector spaces

$$T \colon C_1 \otimes_K C_2 \to C_1 \underline{\otimes} C_2$$

such that $T(a \otimes b) = \psi_0(a, b)$ for $a \in C_1$ and $b \in C_2$.

Projective Reed-Muller-type codes

Let $K = \mathbb{F}_q$ be a finite field,

$X = \{[P_1], \ldots, [P_m]\} \subset \mathbb{P}^{s-1}$ with $m = |X|$,

$S = K[t_1, \ldots, t_s]$ a polynomial ring.

Fix a degree $d \geq 1$. For each i there is $f_i \in S_d$ such that $f_i(P_i) \neq 0$. There is a K-linear map given by

$$\mathrm{ev}_d \colon S_d \to K^m, \qquad f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_m)}{f_m(P_m)} \right).$$

The image of S_d under ev_d, denoted by $C_X(d)$, is called a *projective Reed-Muller-type code* of degree d on X.

The *basic parameters* of the linear code $C_X(d)$ are:

(a) *length*: $|X|$,

(b) *dimension*: $\dim_K C_X(d)$,

(c) *minimum distance*: $\delta_1(C_X(d))$.

The following gives the well-known relation between projective Reed-Muller-type codes and the theory of Hilbert functions:

(a) $\deg(S/I(X)) = |X|$.

(b) $H_X(d) = \dim_K C_X(d)$ for $d \geq 0$.

(c) $\delta_1(C_X(d)) = 1$ for $d \geq \mathrm{reg}(S/I(X))$.

The basic parameters of projective Reed-Muller-type codes have been computed in a number of cases:

- If $X = \mathbb{P}^{s-1}$, $C_X(d)$ this is the *classical projective Reed–Muller code* and formulas for its basic parameters were given by [Sørensen, IEEE Trans. Inform. Theory, 1991].
- If X is a projective torus, $C_X(d)$ is the *generalized projective Reed–Solomon code* and formulas for its basic parameters were given by [Sarmiento, Vaz Pinto, -, Appl. Algebra Engrg. Comm. Comput., 2011].

X is a *projective torus* if X is the image of $(K^*)^s$, under the map $(K^*)^s \to \mathbb{P}^{s-1}$, $x \to [x]$, where $K^* = K \setminus \{0\}$.

In what follows $K = \mathbb{F}_q$ is a finite field

Definition

If $\mathbb{X}$ is the Segre product of $\mathbb{X}_1$ and $\mathbb{X}_2$, we say that the projective Reed-Muller-type code $C_{\mathbb{X}}(d)$ is a *projective Segre code* of degree d.

We come to our main result:

Theorem (Tochimani, Vaz Pinto, -, 2014)

Let $\mathbb{X}$ be the Segre product of $\mathbb{X}_1$ and $\mathbb{X}_2$. If $d \geq 1$, then:

(a) $|\mathbb{X}| = |\mathbb{X}_1||\mathbb{X}_2|$,

(b) $\dim_K(C_{\mathbb{X}}(d)) = \dim_K(C_{\mathbb{X}_1}(d))\dim_K(C_{\mathbb{X}_2}(d))$,

(c) $\delta_1(C_{\mathbb{X}}(d)) = \delta_1(C_{\mathbb{X}_1}(d))\delta_1(C_{\mathbb{X}_2}(d))$,

(d) $C_{\mathbb{X}}(d)$ is the direct product $C_{\mathbb{X}_1}(d) \underline{\otimes} C_{\mathbb{X}_2}(d)$,

(e) $\delta_2(C_{\mathbb{X}}(d)) =$
$\min\{\delta_1(C_{\mathbb{X}_1}(d))\delta_2(C_{\mathbb{X}_2}(d)), \delta_2(C_{\mathbb{X}_1}(d))\delta_1(C_{\mathbb{X}_2}(d))\}$,

(f) $\delta_1(C_{\mathbb{X}}(d)) = 1$ for
$d \geq \max\{\mathrm{reg}(K[\mathbf{x}]/I(\mathbb{X}_1)), \mathrm{reg}(K[\mathbf{y}]/I(\mathbb{X}_2))\}$.

This result tells us that the direct product of projective Reed-Muller-type codes is again a projective Reed-Muller-type code.

Applications

Our main theorem gives generalizations of some results:

- (a_1) If $\mathbb{X}_1 = \mathbb{P}^{a_1-1}$ and $\mathbb{X}_2 = \mathbb{P}^{a_2-1}$, we recover the formula for the minimum distance of $C_{\mathbb{X}}(d)$ given by [González, Rentería, Tapia-Recillas, Finite Fields Appl., 2002)].
- (a_2) If $\mathbb{X}_i$ is a projective torus for $i = 1, 2$, we recover the formula for the minimum distance of $C_{\mathbb{X}}(d)$ given by [González, et. al., Congr. Numer., 2003].

We also recover the following result:

Corollary (González, et. al., Int. J. Contemp. Math. Sci., 2009)

Let $\mathbb{X}$ be the Segre product of two projective torus $\mathbb{X}_1$ and $\mathbb{X}_2$. Then $\delta_2(C_{\mathbb{X}}(d))$ is equal to

$$\min\{\delta_1(C_{\mathbb{X}_1}(d))\delta_2(C_{\mathbb{X}_2}(d)), \delta_2(C_{\mathbb{X}_1}(d))\delta_1(C_{\mathbb{X}_2}(d))\}.$$

Definition

If $\mathbb{X}_i$ is parameterized by monomials $z^{v_1}, \ldots, z^{v_s}$, we say that $C_{\mathbb{X}_i}(d)$ is a *parameterized projective code*.

Corollary

If $C_{\mathbb{X}_i}(d)$ is a parameterized projective code for $i = 1, 2$, then so is the corresponding projective Segre code $C_{\mathbb{X}}(d)$.

The end