THE POINCARÉ POLYNOMIAL OF A LINEAR CODE

CARLOS GALINDO, FERNANDO HERNANDO, RUUD PELLIKAAN AND FRANCISCO MONSERRAT

Abstract. We introduce the Poincaré polynomial of a linear q-ary code and its relation to the corresponding weight enumerator. We prove that the Poincaré polynomial is a complete invariant of the code in the binary and ternary case and it is not when $q \geq 4$. Finally we determine this polynomial for MDS codes and, by means of a recursive formula, for binary Reed-Muller codes.

Appeared in:
Singularities, Algebraic Geometry, Commutative Algebra, and Related Topics
Festschrift for Antonio Campillo on the occasion of his 65th birthday, pp. 525-535, 2018

Introduction

In dimension theory within Commutative Algebra, a very useful tool is the so-called Poincaré series [1]. It is associated to a finitely generated graded A-module $M = \bigoplus_{n\geq 0} M_n$, $A = \bigoplus_{n\geq 0} A_n$ being a Noetherian graded ring with A_0 Artininian, and it is defined as the generating function of the lengths $\ell(M_n)$ of the finite A_0 modules M_n. That is, the Poincaré series is the formal series in $\mathbb{Z}[t]$, $P(M,t) = \sum_{n=0}^{\infty} \ell(M_n)t^n$. This series encodes all the mentioned dimensions and, by the Hilbert theorem, it is, in fact, a rational function.

Using several variables, Poincaré series as generating functions have been extended to other objects with gradings on semigroups or having multi-index filtrations with satisfactory results in singularity theory. In the last fifteen years, Antonio Campillo together with near colleagues has revitalized this study (see, for instance, [4, 5, 6, 7, 10, 12, 8, 9]).

Poincaré series in the above context makes manageable an infinity quantity of data. In this note, we are concerned with error-correcting codes which are finite sets, however the amount of data involved could be very high and so it is also desirable to use tools that allow us to group them according to some interesting property and to give some results to be treated. Recall that error-correcting codes are used when information is received from some source through a noisy communication channel and one tries to correct (or detect) the produced errors. We will only consider linear (error-correcting) codes which are linear spaces of a vector space $\mathbb{F}_q^n$, $\mathbb{F}_q$ being the finite field of q elements. For deciding about the goodness of a linear code C, it is customary to consider its parameters $[n, k, d]$, where k is the dimension of the linear space and d the minimum (Hamming) distance of the code, which is the minimum Hamming weight of their non-vanishing codewords. The generating function of the weight distribution of a code is named its weight enumerator and (given the discrete nature of the codes) it is polynomial in one variable. To determine weight distributions is not easy and the main result to study them is the so-called MacWilliams identity which relates the weight enumerator of a linear code and its dual.

Key words and phrases. Poincaré polynomial; weight enumerator; Tutte polynomial; Plotkin sum.

Supported by the Spanish Ministry of Economy/FEDER: grants MTM2015-65764-C3-2-P and MTM2015-69138-REDT, and the University Jaume I: grant PB1-1B2015-02.

Our aim is to introduce what we call the Poincaré polynomial of a linear code. This polynomial is also related to the weights of the codewords but contains more information than the weight enumerator. It is a polynomial in several variables and gives not only the weight of a codeword but the entries contributing to that weight. We will introduce this polynomial through arrangements of hyperplanes attached to the code; we will prove that the weight enumerator can be obtained from the Poincaré polynomial (Theorem 6) and this polynomial is equivalent to the multivariate Tutte polynomial [18, 20, 21] of the matroid given by the above arrangement (Theorem 10).

An equivalence φ of $\mathbb{F}_q^n$ is an $\mathbb{F}_q$-linear map $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ that is a composition of a permutation matrix and diagonal matrix with non zero entries on the diagonal. Now φ is an equivalence of $\mathbb{F}_q^n$ if and only if φ is linear and leaves the Hamming metric *invariant*, that means that $d(\varphi(\mathbf{x}), \varphi(\mathbf{y})) = d(\mathbf{x}, \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. Let C and D be $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^n$. Then C is called *equivalent* to D if there exists an equivalence φ of $\mathbb{F}_q^n$ such that $\varphi(C) = D$. A map f from the set of all $\mathbb{F}_q$-linear codes to another set is called an *invariant* of $\mathbb{F}_q$-linear code if $f(C) = f(\varphi(C))$ for every code C in $\mathbb{F}_q^n$ and every equivalence φ of codes. The parameters and the weight enumerator of a code are examples of invariants. A *complete invariant* of $\mathbb{F}_q$-linear codes is an invariant f such that for all $\mathbb{F}_q$-linear codes C and D we have that $f(C) = f(D)$ if and only if C and D are equivalent.

We will also show that the Poincaré polynomial is a complete invariant of the code in the binary and ternary case (Corollary 14 and it is not when $q \geq 4$ (Remark 12. We complete this note by showing how the Poincaré polynomial of an MDS code is (Proposition 11), and giving in Corollary 18 recursive formulae for computing the Poincaré polynomial of the binary Reed-Muller codes.

1. The Poincaré polynomial

Denote by $\mathbb{F}_q$ the finite field with q elements. For a fixed positive integer k, consider the linear space $\mathbb{F}_q^k$. An arrangement of hyperplanes in $\mathbb{F}_q^k$, $(H_1, H_2, \ldots, H_n)$ is an n-tuple where each H_i, $1 \leq i \leq n$, is the set of solutions in $\mathbb{F}_q^k$ satisfying a linear equation with k variables.

Definition 1. An arrangement of hyperplanes in $\mathbb{F}_q^k$, $(H_1, H_2, \ldots, H_n)$, is called *simple* (respectively, *central*) whenever all the H_i are mutually different (respectively, are linear subspaces of $\mathbb{F}_q^k$). In addition, the arrangement is named *essential* when it is central and $H_1 \cap H_2 \cap \cdots \cap H_n = \{\mathbf{0}\}$.

Central arrangements can be considered in the projective space, they are essential when $H_1 \cap H_2 \cap \cdots \cap H_n$ is the empty set.

A linear code $C \subseteq \mathbb{F}_q^n$ is *degenerate* when there is an index j such that $x_j = 0$ for all $x \in C$. Arrangements of hyperplanes and linear codes are intimately related to projective systems in the projective space. Indeed, n points $\mathcal{P}$ in the projective space $\mathbb{P}^{k-1}(\mathbb{F}_q)$ which do not belong (all of them) to the same hyperplane are named a *projective system* [22]. The $k \times n$ matrix of coordinates of the system has rank k, which is what happens with the generator matrix G of non-degenerate linear $[n, k, d]$ codes over $\mathbb{F}_q$. Specifically,

Proposition 2. *There exists a bijective map between equivalence classes of essential arrangements of n hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ and equivalence classes of non-degenerate $[n, k, d]$ codes over $\mathbb{F}_q$.*

Since projective systems and arrangements of hyperplanes are dual objects, we observe that the bijection mentioned in Proposition 2 comes from and extends to equivalence

classes of projective systems of n points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. For a complete explanation of the above result we add the two following definitions. The first one says that two *projective systems* $\mathcal{P} \subseteq \mathbb{P}$ and $\mathcal{P}' \subseteq \mathbb{P}'$ over projective spaces $\mathbb{P}$ and $\mathbb{P}'$ are *equivalent* if there is a projective isomorphism between $\mathbb{P}$ and $\mathbb{P}'$ that takes $\mathcal{P}$ to $\mathcal{P}'$. And the second one: two linear codes C and C' in $\mathbb{F}_q^n$ are equivalent if $C' = B(C)$, where B belongs to the subgroup $\mathcal{B}$ in the group of linear automorphisms of $\mathbb{F}_q^n$ generated by permutation of coordinates and multiplication of coordinates by elements in $\mathbb{F}_q^*$ $(= \mathbb{F}_q \setminus \{0\})$. The group $\mathcal{B}$ is represented by monomial matrices, which are square matrices where each row and column contain exactly one non-zero element.

Consider now a non-degenerate $[n, k, d]$ linear code C over $\mathbb{F}_q$ and assume that $G = (g_{ij})_{1\leq i\leq k;\, 1\leq j\leq n}$ is a generator matrix. Let H_j be the hyperplane in $\mathbb{F}_q^k$ defined by the equation $g_{1j}X_1+g_{2j}X_2+\cdots+g_{kj}X_k = 0$ and denote by $\mathcal{A}_G$ the arrangement of hyperplanes $(H_1, H_2, \ldots, H_n)$. Taking into account that a codeword $\mathbf{c} \in C$ satisfies $\mathbf{c} = \mathbf{x}G$ for some $\mathbf{x} \in \mathbb{F}_q^k$, it holds that the jth coordinate of $\mathbf{c}$, satisfies $c_j = \sum_{i=1}^k g_{ij}x_i$ and so $c_j = 0$ if and only if $\mathbf{x}$ lies on the hyplerplane H_j. As a consequence, if we denote by $\mathrm{wt}(\mathbf{c})$ the Hamming weight of the codeword $\mathbf{c} \in C$, then the following result holds:

Proposition 3. [22] *With the above notation, let $\mathbf{c} = \mathbf{x}G$ be a codeword of a non-degenerate linear code C over $\mathbb{F}_q$, then the number of hyperplanes of $\mathcal{A}_G$ going through $\mathbf{x}$ is equal to $n - \mathrm{wt}(\mathbf{c})$.*

Next we introduce the object we are interested in.

Definition 4. Let $C \subseteq \mathbb{F}_q^n$ be a non-degenerate linear code of dimension k with generator matrix G. Let $\mathcal{A}_G = (H_1, H_2, \ldots, H_n)$ be the corresponding arrangement of hyperplanes, and for each $\mathbf{x} \in \mathbb{F}_q^k$, define the n-tuple $\boldsymbol{\epsilon}(\mathbf{x}) = (\epsilon_1(\mathbf{x}), \epsilon_2(\mathbf{x}), \ldots, \epsilon_n(\mathbf{x})) \in \{0, 1\}^n$ by $\epsilon_j(\mathbf{x}) = 1$ if $\mathbf{x} \in H_j$ and 0 otherwise.

Then, the *Poincaré polynomial* of the linear code C is defined as

$$P_C(t_1, t_2, \ldots, t_n) = \sum_{\mathbf{x}\in\mathbb{F}_q^k} \underline{t}^{\boldsymbol{\epsilon}(\mathbf{x})} \in \mathbb{Z}[t_1, t_2, \ldots, t_n],$$

where $\underline{t}^{\boldsymbol{\epsilon}(\mathbf{x})} = t_1^{\epsilon_1(\mathbf{x})} t_2^{\epsilon_2(\mathbf{x})} \cdots t_n^{\epsilon_n(\mathbf{x})}$.

For each subset $J \subseteq \{1, 2, \ldots, n\}$, consider the monomial in $\mathbb{Z}[t_1, t_2, \ldots, t_n]$, $\underline{t}^J = \prod_{j\in J} t_j$, and define $a(J)$ to be the cardinality of the set of vectors $\mathbf{x} \in \mathbb{F}_q^k$ such that the set of zero coordinates of $\mathbf{x}$ is equal to J, or equivalently, lie in $\cap_{j\in J} H_j$ but do not lie in $\cap_{j\in J'} H_j$ for some $J' \not\supseteq J$. Then, there exists an alternative presentation of the Poincaré polynomial as the following straightforward result states.

Proposition 5. *Let $C \subseteq \mathbb{F}_q^n$ be a non-degenerate linear code. Then, with the above notation, it holds that*

$$P_C(t_1, t_2, \ldots, t_n) = \sum_{J\subseteq\{1,2,\ldots,n\}} a(J)\underline{t}^J.$$

As mentioned in the introduction, the weight distribution of a linear code $C \subseteq \mathbb{F}_q^n$ is an important non-complete invariant which provides important information for the structure and practical use of C. Its generating function comes with two equivalent versions. On the one hand, the *weight enumerator of C* which is defined by $W_C(T) = \sum_{i=0}^n \omega_i T^i \in \mathbb{Z}[T]$, where $\omega_i := \mathrm{card}\{\mathbf{c} \in C \mid \mathrm{wt}(\mathbf{c}) = i\}$ and, on the other hand the *homogeneous weight enumerator of C* which is defined as the homogeneous polynomial $W_C(X, Y) =$

$\sum_{i=0}^{n} \omega_i X^{n-i}Y^i \in \mathbb{Z}[X,Y]$. Now, we prove that the Poincaré polynomial of a code contains at least as much information as the weight enumerator.

Theorem 6. *Let $C \subseteq \mathbb{F}_q^n$ be a non-degenerate linear code. Then, with the above notations, it holds that the homogeneous weight enumerator of C is the homogenization with respect to the variable Y of the polynomial $P_C(X, X, \ldots, X)$. In addition, it holds that*

$$P_C(T, T, \ldots, T) = T^n W_C(T^{-1}).$$

Proof. It follows from the equality $P_C(X, X, \ldots, X) = \sum_{i=0}^{n} \omega_i X^{n-i}$. Its homogenization with respect to Y will be $\sum_{i=0}^{n} \omega_i X^{n-i}Y^i$, that is $W_C(X,Y)$. Now $T^n \left(\sum_{i=0}^{n} \omega_i T^{i-n}\right) = \sum_{i=0}^{n} \omega_i T^i = W_C(T)$, which concludes the proof. □

The arrangement $\mathcal{A}_G$ defined by a code C can be regarded as a matroid. Recall that a matroid is a pair $\mathcal{M} := (\mathcal{H}, \mathcal{I})$, where $\mathcal{H}$ is a finite set named ground set and $(\emptyset \in)\ \mathcal{I}$ a family of subsets of $\mathcal{H}$, called the independent sets, that must satisfy $J \subseteq I \in \mathcal{I}$ implies $J \in \mathcal{I}$. In addition $(\mathcal{H}, \mathcal{I})$ has to satisfy that if $I, J \in \mathcal{I}$ and $\mathrm{card}(I) > \mathrm{card}(J)$, then there exists $i \in I \setminus J$ such that $J \cup \{i\} \in \mathcal{I}$.

Definition 7. Let $\mathcal{M}$ be a matroid with ground set $\mathcal{H}$. Assume that n is the cardinality of $\mathcal{H}$. Set $r_{\mathcal{M}}$ its rank function. The *multivariate Tutte polynomial* is defined by

$$Z_{\mathcal{M}}(T, t_1, \ldots, t_n) = \sum_{J \subseteq \mathcal{H}} T^{-r_{\mathcal{M}}(J)} \underline{t}^J \in \mathbb{Z}[T^{-1}, t_1, \ldots, t_n].$$

The multivariate Tutte polynomial encodes the full structure of the matroid, contains as a special case the more known two variable Tutte polynomial and also the so-called chromatic polynomial. The Poincaré polynomial of a code and the multivariate Tutte polynomial of the matroid given by the arrangement attached to the code determine each other. For this result we need some results from [18, 20] first.

Let C be a linear code with generator matrix G. For a subset J of $\{1, 2, \ldots, n\}$ define

$$C(J) = \{\mathbf{c} \in C \mid c_j = 0 \text{ for all } j \in J\} \quad \text{and} \quad l(J) = \dim C(J).$$

Let $\mathrm{card}(J) = t$ and let G_J be the $k \times t$ submatrix of G consisting of the columns of G indexed by J. Let $r(J)$ be the rank of G_J. Then the map r is equal to $r_{\mathcal{M}}$, the rank of the associated matroid $\mathcal{M}$ of the arrangement of the code. Furthermore the dimension $l(J)$ is equal to $k - r(J)$ by [18] and [20, Lemma 3.2.12]. We have the following result from [20, Proposition 3.2.18].

Proposition 8. *Let C be a linear code of length n and minimum distance d. If $d \leq w \leq n$, then the number of codewords in C of weight w is given by*

$$\omega_w = \sum_{t=n-w}^{n-d} (-1)^{n+w+t} \binom{t}{n-w} \sum_{\mathrm{card}(J)=t} (q^{l(J)} - 1).$$

Furthermore $\omega_0 = 1$ and $\omega_w = 0$ for all $0 < w < d$.

Let $J \subseteq \{1, 2, \ldots, n\}$ consist of the m integers $j_1, j_2, \ldots, j_m$ with $1 \leq i_1 < i_2 < \cdots < i_m \leq n$. Let $\mathbf{x} \in \mathbb{F}_q^n$. Define

$$\mathbf{x}_J = (x_{j_1}, x_{j_2}, \ldots, x_{j_m}) \in \mathbb{F}_q^m$$

the restriction of $\mathbf{x}$ to the coordinates indexed by J. Let $\overline{J}$ be the relative complement of J in $\{1, 2, \ldots, n\}$. The *shortened* code C^J is obtained from $C(J)$ by deleting the entries that are at positions indexed by J:

$$C^J = \{\mathbf{c}_{\overline{J}} \mid \mathbf{c} \in C \text{ and } \mathbf{c}_J = 0\}.$$

Notice that $C(J)$ is an $\mathbb{F}_q$-linear vector space that is isomorphic with $\cap_{j\in J}H_j$ under the map $\mathbf{x}\mapsto \mathbf{x}G$. By this map we see that $a(J)$ is equal to the number of codewords of the shortened code C^J of maximal weight $n-\mathrm{card}(J)$. The formalism above gives a way to obtain this number.

Proposition 9. *Let C be a linear code of length n, dimension k and minimum distance d. Let $J\subseteq\{1,2,\ldots,n\}$ and $\mathrm{card}(J)=t$. Then $a(J)=1$ if $t=n$ and $a(J)=0$ if $n-d<t<n$. For $0\leq t\leq n-d$ we have that*

$$a(J)=\sum_{s=0}^{n-t-d}(-1)^s\sum_{I\subseteq\bar{J},\ \mathrm{card}(I)=s}(q^{k-r(J\cup I)}-1).$$

Proof. The shortened code C^J is isomorphic with $C(J)$, has dimension $l(J)=k-r(J)$ by [20, Lemma 3.2.12] and minimum distance $d(J)\geq d$. We view the codewords of C^J with entries indexed by $\bar{J}$, the complement of J in $\{1,2,\ldots,n\}$. If $I\subseteq\bar{J}$, then $C^J(I)$ is isomorphic with $C(J\cup I)$. Hence $\dim C^J(I)=k-r(J\cup I)$ by [20, Lemma 3.2.12]. So we better use the notation $k-r(J\cup I)$ instead of $l(I)$ for the dimension of $\dim C^J(I)$, since in the latter notation the dependency on J is not clear. Now $a(J)$ is equal to the number of codewords of the shortened code C^J of maximal weight $n-t$ where $t=\mathrm{card}(J)$ as remarked before. Hence $a(J)$ is given by the formula in Proposition 8 applied to C^J.
Notice that if $s>n-t-d(J)$ we have that in the summation $\sum_{s=0}^{n-t-d}$ the summand $q^{k-r(J\cup I)}-1$ is zero, since $\mathrm{card}(J\cup I)=s+t>n-d(J)$ and a codeword with $s+t$ zero entries is the all zeros word, so $C^J(I)=\{0\}$. □

Theorem 10. *Let $C\subseteq\mathbb{F}_q^n$ be a non-degenerate linear code with generator matrix G. Set $\mathcal{M}$ the matroid defined by the arrangement of hyperplanes $\mathcal{A}_G$. Then the Poincaré polynomial $P_C(t_1,\ldots,t_n)$ and the multivariate Tutte polynomial $Z_{\mathcal{M}}(T,t_1,\ldots,t_n)$ are equivalent.*

Proof. The multivariate Tutte polynomial of C determines the Poincaré polynomial of C since the latter is determined by the $a(J)$ by Proposition 5, and the $a(J)$ can be computed by means of the rank function $r_{\mathcal{M}}$ by Proposition 9, and the value $r_{\mathcal{M}}(J)$ can be read off form the coefficient $T^{-r_{\mathcal{M}}(J)}$ of $\underline{t}^J$ in $Z_{\mathcal{M}}(T,t_1,\ldots,t_n)$.
Conversely, $a(J)$ is the coefficient of $\underline{t}^J$ in $P_C(t_1,\ldots,t_n)$. Now $a(J)$ is equal to the number of codewords $\mathbf{c}$ in C such that the set of zero coordinates of $\mathbf{c}$ is equal to J. Hence $\sum_{J\subseteq J'}a(J')$ is equal to the number of codewords $\mathbf{c}$ in C such that the zero coordinates of $\mathbf{c}$ are in J, which is equal to $\mathrm{card}\,(C(J))=l(J)$. Finally $r_{\mathcal{M}}(J)=k-l(J)$ by [20, Lemma 3.2.12]. Hence the Poincaré polynomial of C determines the multivariate Tutte polynomial of C. □

Since it is known that the multivariate Tutte polynomial attached to a linear code is not a complete invariant, we deduce the same result for the Poincaré polynomial of a linear code.

As a consequence of the above result we can state the following one.

Proposition 11. *Let C be an MDS linear code with parameters $[n,k,n-k+1]$ over the field $\mathbb{F}_q$. Then the Poincaré polynomial of C is given by*

$$P_C(t_1,t_2,\ldots,t_n)=t_1t_2\cdots t_n+\sum_{t=0}^{k-1}\sum_{\mathrm{card}(J)=t}\sum_{s=0}^{k-1-t}(-1)^s\binom{n-t}{s}(q^{k-t-s}-1)\underline{t}^J.$$

Proof. The code C is MDS. Hence $d(C^\perp)=k+1$. So the numbers $l(J)$ and therefore $r(J)$ depend only on the size of J. That is $r(J)=\mathrm{card}(J)$ if $\mathrm{card}(J)\leq k$ and $r(J)=k$ if

$\mathrm{card}(J) > k$ by [20, Lemma 3.2.15].
Let $J \subseteq \{1, 2, \ldots, n\}$ and $\mathrm{card}(J) = t$. Then $a(J) = 1$ if $t = n$ and $a(J) = 0$ if $n - d < t < n$. If $0 \leq t \leq n - d$ then $I \subseteq \bar{J}$ and $\mathrm{card}(I) = s$, so $r(J \cup I) = \mathrm{card}(J \cup I) = t + s$ if $t + s \leq k$ and k otherwise. With Proposition 9 we get

$$a(J) = \sum_{s=0}^{k-1-t} (-1)^s \binom{n-t}{s} (q^{k-t-s} - 1).$$

The formula follows now from Proposition 5. □

Remark 12. Let $C(a)$ be the $\mathbb{F}_q$-linear code of length 10 and dimension 2 generated by $(1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$ and $(0, 1, 1, 1, 1, 1, a, a, a, a)$ where $a \in \mathbb{F}_q$ and $a \notin \{0, 1\}$. Then $\mathcal{P}(a)$, the corresponding projective system on the projective line consists of the 10-tuple of points P_i with $P_1 = (1 : 0)$, $P_2 = P_3 = (0 : 1)$, $P_4 = P_5 = P_6 = (1 : 1)$ and $P_j = (1 : a)$ for $7 \leq j \leq 10$. That is to say the four points $(1 : 0)$, $(0 : 1)$, $(1 : 1)$ and $(1 : a)$ have multiplicity 1, 2, 3 and 4, respectively. All such codes have equivalent matroids and the same multivariate Poincaré polynomial by Theorem 10, but they are not all equivalent. Two projective systems on the projective line are equivalent if and only if the corresponding points are mapped to each other by a fractional transformation. Moreover if three distinct points of the system remain fixed under such a transformation, then the remaining points remain also fixed by [11] and Propositions 5.1.33 and 5.1.34 of [20]. Now suppose that the codes $C(a)$ and $C(b)$ are equivalent with $a, b \in \mathbb{F}_q$ and $a, b \notin \{0, 1\}$, then the projective systems $\mathcal{P}(a)$ and $\mathcal{P}(b)$ are equivalent. Now the points $(1 : 0)$, $(0 : 1)$, $(1 : 1)$ remain fixed under the fractional transformation, since their multiplicities are distinct and should remain the same. Therefore $(1 : a)$ remains also fixed under the transformation. If $q \geq 4$ then there are at least two choices for a giving two inequivalent codes with the same matroid. Hence the Poincaré polynomial is not a complete invariant of $\mathbb{F}_q$-linear codes if $q \geq 4$. The matroid of an $\mathbb{F}_q$-linear code determines the equivalence class of the code if and only if $q = 2$ or $q = 3$. See [3, 19]. That implies by Theorem 10 that the Poincaré polynomial is a complete invariant of the code of $\mathbb{F}_q$-linear codes if and only if $q = 2$ or $q = 3$. In the next section we treat the Poincaré polynomial of binary codes in more detail.

2. The Poincaré polynomial in the binary case

We devote this section to provide some results about the Poincaré polynomial of binary linear codes. However our first result is true for codes over any finite field.

Proposition 13. *Let $C \subseteq \mathbb{F}_q^n$ be a non-degenerate linear code. Then, with the above notation*

$$P_C(t_1, t_2, \ldots, t_n) = \sum_{\mathbf{c} \in C} \underline{t}^{\mathbf{1} - \mathbf{c}^{q-1}},$$

where $\mathbf{1} = (1, 1, \ldots, 1) \in \mathbb{F}_q^n$ and $\mathbf{c}^{q-1} = (c_1^{q-1}, c_2^{q-1}, \ldots, c_n^{q-1})$ whenever $\mathbf{c} = (c_1, c_2, \ldots, c_n)$.

Proof. The codewords in C are exactly the vectors $\mathbf{x}G$, where $\mathbf{x}$ runs along all vectors in $\mathbb{F}_q^k$ and G is a generator matrix of C. Then the result follows by noting that $\boldsymbol{\epsilon}(\mathbf{x}) = \mathbf{1} - (\mathbf{x}G)^{q-1}$ because $C \subseteq \mathbb{F}_q^n$. □

From now on, our codes will be included in $\mathbb{F}_2^n$. First we state an immediate and interesting consequence of Proposition 13. It says that the Poincaré polynomial of a binary code is a complete invariant of the code.

Corollary 14. *Let $C \subseteq \mathbb{F}_2^n$ be a non-degenerate binary linear code, then*

$$P_C(t_1, t_2, \ldots, t_n) = \sum_{\mathbf{c} \in C} \underline{t}^{\mathbf{1}-\mathbf{c}}.$$

Next we explain how the Poincaré polynomial can be obtained for the so-called $(u, u+v)$-construction of binary linear codes. From that result, we will derive a recursive formula for computing the Poincaré polynomial of binary Reed-Muller codes. In our development, we will use the following polynomial, close to the Poincaré one, which is attached to a binary linear code $C \subseteq \mathbb{F}_2^n$:

$$\hat{P}_C(t_1, t_2, \ldots, t_n) = \sum_{\mathbf{c} \in C} \underline{t}^{\mathbf{c}}. \tag{1}$$

The $(u, u+v)$-construction is a particular case of matrix-product code [2] and sometimes it is called the Plotkin sum. Matrix-product codes constitute a natural way to obtain large codes from others previously known (denominated constituent codes) [14]. They admit decoding procedures depending on the decoding methods of the corresponding constituent ones [16, 13], and when the constituent codes are cyclic, their corresponding matrix-product codes are quasi-cyclic codes [15]. Let us show the definition of $(u, u+v)$-construction.

Definition 15. Let C_1 and C_2 be two binary linear codes with parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$, respectively. The $(C_1, C_1 + C_2)$ code ($(u, u+v)$-construction of C_1 and C_2) is defined to be the following binary linear code

$$(C_1, C_1 + C_2) = \{(\mathbf{c}_1, \mathbf{c}_1 + \mathbf{c}_2) \mid \mathbf{c}_1 \in C_1, \mathbf{c}_2 \in C_2\}.$$

It has parameters $[2n, k_1 + k_2, \min\{2d_1, d_2\}]$.

For the codes on length $2n$ we are going to study, we will distinguish the variables for the Poincaré polynomial setting $t_j = t_{1j}$ and $t_{n+j} = t_{2j}$ for $1 \leq j \leq n$. So we will consider the Poincaré polynomial as an element in the ring

$$\mathbb{Z}[t_{11}, t_{12}, \ldots, t_{1n}, t_{21}, t_{21}, \ldots, t_{2n}].$$

As above, for $i = 1, 2$ the product $\prod_{j=1}^n t_{ij}^{c_{ij}}$ is expressed as $\underline{t_i}^{\mathbf{c}_i}$. With this notation, the Poincaré polynomial of a binary $(u, u+v)$ code can be obtained as follows.

Theorem 16. *Let C_1 and C_2 be two binary non-degenerate linear codes both of length n and dimensions k_1 and k_2, respectively. Then.*

$$P_{(C_1, C_1+C_2)}(t_{11}, \ldots, t_{1n}, t_{21}, \ldots, t_{2n}) = \\ P_{(C_1, C_1)}(t_{11}, \ldots, t_{1n}, t_{21}, \ldots, t_{2n}) \hat{P}_{C_2}(t_{21}, \ldots, t_{2n}).$$

Proof. Denote by G_1 (respectively, G_2) the generator matrix of C_1 (respectively, C_2). Then, using Corollary 14, the following chain of equalities holds.

$$\begin{aligned} P_{(C_1,C_1+C_2)}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^{k_1},\,\mathbf{y}\in\mathbb{F}_2^{k_2}} \underline{t_1}^{\mathbf{1}-\mathbf{x}G_1}\underline{t_2}^{\mathbf{1}-\mathbf{x}G_1-\mathbf{y}G_2} \\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^{k_1},\,\mathbf{y}\in\mathbb{F}_2^{k_2}} \underline{t_1}^{\mathbf{1}-\mathbf{x}G_1}\underline{t_2}^{\mathbf{1}-\mathbf{x}G_1}\underline{t_2}^{-\mathbf{y}G_2} \\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^{k_1}} \underline{t_1}^{\mathbf{1}-\mathbf{x}G_1}\underline{t_2}^{\mathbf{1}-\mathbf{x}G_1} \sum_{\mathbf{y}\in\mathbb{F}_2^{k_2}} \underline{t_2}^{-\mathbf{y}G_2} \\ &= P_{(C_1,C_1)}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n}) \sum_{\mathbf{y}\in\mathbb{F}_2^{k_2}} \underline{t_2}^{-\mathbf{y}G_2}. \end{aligned}$$

Since we are in the binary field, we have $-\mathbf{y}G_2 = \mathbf{y}G_2$ and the right hand side of the last equality equals

$$P_{(C_1,C_1)}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2,n}) \sum_{\mathbf{y}\in\mathbb{F}_2^{k_2}} \underline{t_2}^{\mathbf{y}G_2}.$$

According to (1), we get $P_{(C_1,C_1)}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n})\hat{P}_{C_2}(t_{21},\dots,t_{2n})$, which concludes the proof. □

Remark 17. Reasoning as in the proof of Theorem 16, one obtains the following equality of polynomials

$$\begin{aligned} \hat{P}_{(C_1,C_1+C_2)}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n}) = \\ \hat{P}_{(C_1,C_1)}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n})\hat{P}_{C_2}(t_{21},\dots,t_{2n}). \end{aligned}$$

As an application of Theorem 16, we show recursive formulae for obtaining the Poincaré polynomial of a binary Reed-Muller code. Generally speaking and for two fixed nonnegative integers r and m, the *Reed-Muller code* $\mathrm{RM}_q[r,m]$ is defined to be as the linear code obtained as follows:

$$\mathrm{RM}_q[r,m] = \left\{ p(\mathbf{a}) \mid p \in \mathbb{F}_q[X_1,X_2,\dots,X_m],\ \mathbf{a}\in\mathbb{F}_q^m \ \text{ and } \ \deg(p) \le r \right\}.$$

The mentioned recursive formulae apply to binary Reed-Muller codes and are stated in the following result.

Corollary 18. *Let m and r be positive integers such that $0 < r < m$. Then, setting $n = 2^{m-1}$, the following two recursive formulae concerning Poincaré polynomials and polynomials as in (1) hold.*

$$\begin{aligned} P_{\mathrm{RM}_2[r,m]}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n}) = \\ P_{(\mathrm{RM}_2[r,m-1],\mathrm{RM}_2[r,m-1])}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n})\hat{P}_{\mathrm{RM}_2[r-1,m-1]}(t_{21},\dots,t_{2n}). \end{aligned}$$

$$\begin{aligned} \hat{P}_{\mathrm{RM}_2[r,m]}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n}) = \\ \hat{P}_{(\mathrm{RM}_2[r,m-1],\mathrm{RM}_2[r,m-1])}(t_{11},\dots,t_{1n},t_{21},\dots,t_{2n})\hat{P}_{\mathrm{RM}_2[r-1,m-1]}(t_{21},\dots,t_{2n}). \end{aligned}$$

Proof. It follows from Theorem 16, Remark 17 and the fact that the code $\mathrm{RM}_2[r,m]$ is obtained from the $(u,u+v)$-construction of $\mathrm{RM}_2[r,m-1]$ and $\mathrm{RM}_2[r-1,m-1]$ [17]. □

References

[1] Atiyah, M.F., Macdonald, I.G. *Introduction to commutative algebra.* Addison-Wesley, 1969.

[2] Blackmore, T., Norton, G. H. Matrix-product codes over $\mathbb{F}_q$, *Appl. Algebra Eng. Comm. Comp.* **12** (2001) 477-500.

[3] Brylawski, T. H., Lucas, D., Uniquely representable combinatorial geometries, in *Teorie Combinatorie* Proc. 1973 Internat. Colloq. pp. 83-104, Accademia Nazionale del Lincei, Rome, 1976.

[4] Campillo, A., Delgado, F., Gusein-Zade S. Poincaré series of a rational surface singularity. *Inventiones Math.* **155** 45-53 (2004) 45-53.

[5] Campillo, A., Delgado, F., Gusein-Zade S. Poincaré series of curves on rational surface singularities. *Comm. Math. Helvetici* **80** (2005) 95-102.

[6] Campillo, A., Delgado, F., Gusein-Zade S. Multiindex filtrations and motivic Poincaré series. *Monatshefte. Math.* **150** (2007) 193-209.

[7] Campillo, A., Delgado, F., Gusein-Zade S., Hernando, F. Poincaré series of collections of plane valuations. *Int. J. Math* **21** (2010) 1461-1473.

[8] Campillo, A., Delgado, F., Gusein-Zade S. Equivariant Poincaré series of filtrations. *Rev. Mat. Complutense* **26** (2013)

[9] Campillo, A., Delgado, F., Gusein-Zade S. An equivariant Poincaré series of filtrations and monodromy of zeta functions. *Rev. Mat. Complutense* **28** (2015) 449-467.

[10] Delgado, F., Moyano-Fernández, J.J. On the relation between the generalized Poincaré series and the Stöhr zeta function. *Proc. Amer. Math. Soc.* **137** (2009) 51-59.

[11] Dür, A., The automorphism groups of Reed-Solomon codes. *Journ. Comb. Th.*, Series A **44** (1) (1987) 69-82.

[12] Galindo, C. Monserrat, F. The Poincaré series of multiplier ideals of a simple complete ideal in a local ring of a smooth surface. *Adv. Math.* **225** (2010) 1046-1068.

[13] Hernando, F., Høholdt, T., Ruano, D. List Decoding of matrix-product codes from nested codes: an application to quasi-cyclic codes, *Adv. Math. Commun* **6** (2012) 259-272.

[14] Hernando, F., Lally, K., Ruano, D. Construction and decoding of matrix-product codes from nested codes, *Appl. Algebra Eng. Comm. Comp.* **20** (2009) 497-507.

[15] Hernando, F., Ruano, D. New linear codes from matrix-product codes with polynomial units, *Adv. Math. Commun.* **4** (2010) 363-367

[16] Hernando, F., Ruano, D. Decoding of matrix-product codes, *J. Algebra Appl.* **12** (2013) 1250185.

[17] Roman, S. *Coding and information theory.* Springer, 1992.

[18] Jurrius, R., Pellikaan, R. Codes, arrangements and matroids, *Series on Coding Theory and Cryptology.* Algebraic Geometry Modeling in Information Theory. World Scientific vol. **8** (2013) 219-325.

[19] Kahn, J., On the uniqueness of matroid representations over GF(4), *Bull. London Math. Soc.* **20** (1988) 5-10

[20] Pellikaan, R., Wu, X.-W., Bulygin, S., Jurrius, R. *Codes, cryptology and curves with computer algebra.* Cambridge University Press, 2017.

[21] Sokal, A.D., The multivariate Tutte polynomial (alias Potts model) for graphs and matroids. Surveys in combinatorics, London Math. Soc. Lecture Note Ser. **327** 173-226 (2005). Cambridge Univ. Press, Cambridge.

[22] Tsfasman M.A., Vlădut S.G. *Algebraic-geometric codes.* Kluwer Academic Publishers, 1991.

Current address: `Carlos Galindo and Fernando Hernando:` Instituto Universitario de Matemáticas y Aplicaciones de Castellón and Departamento de Matemáticas, Universitat Jaume I, Campus de Riu Sec. 12071 Castelló, Spain., `Ruud Pellikaan:` Discrete Mathematics, Techn. Univ. Eindhoven, P.O. Box 513, 5600 MB Eindhoven, The Netherlands., `Francisco Monserrat:` Instituto Universitario de Matemática Pura y Aplicada (IUMPA). Universidad Politécnica de Valencia. Camino de Vera sn, 46022 Valencia, Spain.

E-mail address: `galindo@uji.es; carrillf@uji.es; g.r.pellikaan@tue.nl; framonde@mat.upv.es`