Power sum polynomials in a discrete tomography perspective

Silvia M.C. Pagani, Silvia Pianta
Università Cattolica del Sacro Cuore
via Musei 41, 25121 Brescia, Italy

Abstract

For a point of the projective space $\text{PG}(n,q)$, its Rédei factor is the linear polynomial in $n + 1$ variables, whose coefficients are the point coordinates. The power sum polynomial of a subset $S$ of $\text{PG}(n,q)$ is the sum of the $(q - 1)$-th powers of the Rédei factors of the points of $S$. The fact that many subsets may share the same power sum polynomial offers a natural connection to discrete tomography. In this paper we deal with the two-dimensional case and show that the notion of ghost, whose employment enables to find all solutions of the tomographic problem, can be rephrased in the finite geometry context, where subsets with null power sum polynomial are called ghosts as well. In the latter case, one can add ghosts still preserving the power sum polynomial by means of the multiset sum (modulo the field characteristic). We prove some general results on ghosts in $\text{PG}(2,q)$ and compute their number in case $q$ is a prime.

Keywords: discrete tomography; ghost; multiset sum; power sum polynomial; projective plane.

1 Introduction

The aim of the present paper is to investigate the structure and the size of those point sets of $\text{PG}(2,q)$ associated to a given homogeneous polynomial of degree $q - 1$, introduced by P. Sziklai in [8] and named power sum polynomial. It is a hard task in general to determine all sets sharing the same power sum polynomial. The ill-posedness of the aforementioned problem enables to construct a link to discrete tomography. There, linear algebra offers a straightforward way of dealing with all images agreeing with the same set of projections (see [5]). The key role is played by ghosts, which constitute the kernel of the linear system in which the problem may be translated.

Motivated by the description of the set of solutions of a tomographic problem, we investigate the recovery of the subsets of $\text{PG}(2,q)$ related to the same power sum polynomial in the following way. We look for an operation on the subsets of $\text{PG}(2,q)$ such that those with associated null polynomial, which we call ghosts as well, constitute the kernel of a suitable function mapping a subset to the corresponding power sum polynomial. A good choice for the operation turns out to be the multiset sum modulo $p$ (the field characteristic). Then, we investigate the algebraic and geometric properties of the set of ghosts and find out the size of the subset of ghosts when $q = p$, namely, for prime fields.
We remark that the “polynomial technique” for subsets of a projective space is a well investigated research field in the framework of finite geometries. It consists in the study of the interplay between subsets of a projective space and polynomials over finite fields (see for instance [1, 2]). It is essentially listed in three steps: rephrasing the theorem to be proven into a relationship on points, reformulating the (new) theorem in terms of polynomials over finite fields, and perform the calculations. This technique was introduced in the 70’s by L. Rédei [7] and inspired a series of results on blocking sets, directions and codes from the 90’s onward, such as [3, 9, 10]. The advantage of choosing the power sum polynomial, w.r.t. the more studied Rédei polynomial, is the fact that the first one has a lower degree when the subset has more than \( q-1 \) points.

The paper is organized as follows. Section 2 establishes the framework and gives the main definitions. In Section 3 the tomographic problem is recalled, together with a focus on the similarities with the treated problem. Section 4 gives some general results for ghosts in the projective plane, while in Section 5 we set \( q = p \) and show the size of the set of ghosts in that case. Section 6 provides possible further work and concludes the paper.

2 The power sum polynomial

Let \( \mathbb{F}_q \) denote the Galois field of order \( q = p^h \), \( p \) prime, \( h \geq 1 \), whilst PG\((n,q)\) will refer to the projective space of dimension \( n \) over \( \mathbb{F}_q \). Let \( X = (X_1, \ldots, X_{n+1}) \) be the vector of the variables.

**Definition 1.** Let \( P = (p_1, \ldots, p_{n+1}) \) be a point of PG\((n,q)\). The Rédei factor corresponding to \( P \) is the linear polynomial
\[
P \cdot X = p_1X_1 + \ldots + p_{n+1}X_{n+1}.
\]

The zeros of a Rédei factor \( P \cdot X \) are the Plücker coordinates of the hyperplanes through \( P \).

The well-known Rédei polynomial of a point set \( S \) is defined as the product of the Rédei factors corresponding to the points of \( S \). We are interested in a different polynomial.

**Definition 2.** Let \( S = \{P_1, i = 1, \ldots, |S|\} \subseteq \text{PG}(n,q) \) be a point set. The power sum polynomial of \( S \) is defined as
\[
G_S(X) := \sum_{i=1}^{|S|} (P_i \cdot X)^{q-1}.
\]

The power sum polynomial is therefore a homogeneous polynomial of degree \( q - 1 \). Denote by \( \mathbb{F}_q^{\times}[X] \) the set of homogeneous polynomials of degree \( q - 1 \) in the variables \( X \) with coefficients in \( \mathbb{F}_q \). It is a vector space over \( \mathbb{F}_q \) with dimension \( \binom{n+q-1}{n} \). For \( n = 2 \), we will write
\[
G_S(X,Y,Z) = \sum_{k=1}^{|S|} (a_kX + b_kY + c_kZ)^{q-1} = \sum_{k=1}^{|S|} \sum_{i=0}^{q-1} \sum_{j=0}^{q-1-i} \binom{q-1}{i,j} (a_kX)^{q-1-i-j} (b_kY)^i (c_kZ)^j,
\]
where \[ \binom{q-1}{i,j} = \frac{(q-1)!}{i!j!(q-1-i-j)!} \] for \( i + j \leq q - 1 \).

The power sum polynomial of the union of disjoint subsets of \( \text{PG}(n,q) \) is clearly the sum of the corresponding power sum polynomials. If a hyperplane \((x_1,\ldots,x_{n+1})\) intersects \(S\) in \(m\) points, then, from the well-known fact that

\[ \forall \alpha \in \mathbb{F}_q : \alpha^{q-1} = \begin{cases} 0 & \text{if } \alpha = 0, \\ 1 & \text{otherwise}, \end{cases} \]

it results that \(G^S(x_1,\ldots,x_{n+1}) = |S| - m\).

As noted in [8], while there is an one-to-one correspondence between Rédei polynomials and point sets, the same power sum polynomial may refer to different point sets.

**Example 3.** Consider the Fano plane \(\text{PG}(2,2)\) and the subset \(S_1 = \{(0,0,1)\}\). The corresponding power sum polynomial is \(G^{S_1}(X,Y,Z) = Z\), which is shared with other subsets of \(\text{PG}(2,2)\), such as \(S_2 = \{(1,0,1),(1,0,0)\}\) and \(S_3 = \{(1,0,0),(0,1,0),(1,1,1)\}\).

We address the following problem: Given a homogeneous polynomial \(G\) of degree \(q - 1\), find all sets \(S \subseteq \text{PG}(2,q)\) such that \(G^S = G\). The choice of considering the two-dimensional case is justified in the next section.

### 3 Discrete tomography

The problem stated at the end of the previous section belongs to the large class of the inverse problems, where an object has to be retrieved from the measurements of its features, broadly intended. In the same class one can find the tomographic problem, whose measurements are the projections of the unknown object along a set of given directions. Tomography originates from the work of J. Radon [6], who proved that, under some regularity hypotheses, a density function defined over \(\mathbb{R}^2\) can be reconstructed from its projections taken along angles in the whole range \([0,\pi)\). From [6] on, the tomographic problem has mainly addressed the two-dimensional case (in diagnostics imaging, for instance, the 3D scan of the body is obtained by stacking 2D slices), as we will do in the present paper.

The function to be recovered is also called an image.

When a finite set of directions is employed and the image is assumed to be defined on a finite subset of the lattice \(\mathbb{Z}^2\), one deals with discrete tomography. Directions are lattice directions, i.e., with rational slopes, and projections are obtained by summing up the values of the points which are intersections between lines with given direction and the domain (see Fig. 1). Usually, the codomain of the image is (a subset of) \(\mathbb{Z}\).

In general, neither existence nor uniqueness of a solution applies to a discrete tomographic problem, which is ill-posed as most of the inverse problems. In fact, on the one side the available data may be inconsistent due to noise, so that no image exists with prescribed projections. On the other side, when dealing with consistent measurement (i.e., at least one solution exists) many images which agree with the projections could be allowed (see for instance [4]). The lack of uniqueness is caused by the presence of images whose projections along the set of considered directions are zero, and therefore are, in a sense, invisible to
measurements. Such images are known as ghosts and constitute the kernel of a suitable linear system, obtained by ordering the projections in some way.

Linear algebra and [5] show how to treat ghosts in order to move among the solutions of a tomographic problem. In fact, every solution of a same problem may be obtained as the sum between a peculiar solution and a suitable ghost (see Fig. 2 for an example). We investigate their counterpart in the power sum polynomial problem, which will be called ghosts as well, in particular in the two-dimensional case.

![Figure 1: A four by two integer-valued image and the projections along a direction.](image)

3.1 Connections and differences

Our goal is to determine all point sets of PG(2, q) sharing the same power sum polynomial. Arguing in analogy with the tomographic framework, the role of the grid (i.e., the domain) and that of an image are played by PG(2, q) and a point set S, respectively. The counterpart of tomographic ghosts is defined as follows.

**Definition 4.** Let $S \subseteq \mathrm{PG}(2, q)$. We say that S is a ghost if $G^S(X, Y, Z) \equiv 0$.

Note that, in the tomographic case, the set of directions has to be specified, while the definition of the power sum polynomial does not depend on other features. We study the structure of ghosts and look for an operation which maps a pair, consisting of a generic point set and a ghost, to another point set with the same power sum polynomial as the previous generic one. The investigation of ghosts therefore completes the search of subsets $S$ such that $G^S = G$ for a given polynomial $G$.

4 Ghosts and multiset sum in PG(2, q)

As stated in the previous section, we have to study the structure of ghosts. We first prove some general results about classes of ghosts.

![Figure 2: Adding a ghost (w.r.t. the coordinate directions in this case) to an image produces a new image, whose horizontal and vertical projections equal those of the starting image.](image)
In order to prove that a point set \( S \subseteq \text{PG}(2,q) \) has the zero polynomial as the corresponding one, we have to find when \( G^S \) vanishes identically. We look at the intersections of \( S \) with lines, which are the hyperplanes in the plane. In fact, if \(|S \cap \ell| = m\) for a line \( \ell \), then \( G^S(\ell) = |S| - m \), where, by an abuse of notation, we write that the polynomial is computed in \( \ell \) instead of the Plücker coordinates of \( \ell \).

Therefore, as \( \deg G^S < q \), we seek those point sets whose intersections with all lines of \( \text{PG}(2,q) \) have size congruent to that of \( S \) modulo the field characteristic \( p \). According to [8, Theorem 13.5], such point sets \( S \) are exactly those intersecting each line in a fixed (mod \( p \)) number of points. So, our ghosts are the generalized Vandermonde sets defined in [8].

**Theorem 5.** Let \( S \subseteq \text{PG}(2,q) \) be a ghost. Then \( \text{PG}(2,q) \setminus S \) is a ghost.

**Proof.** Since \( S \) has constant intersection size with lines, the same holds true for its complement \( \text{PG}(2,q) \setminus S \). \( \square \)

As a consequence, both the empty set and the whole projective plane are ghosts.

**Theorem 6.** A partial pencil \( P \) of \( \lambda p + 1 \) lines, \( \lambda = 0,\ldots,p^{h-1} \), is a ghost. Consequently, a set of \( q - \lambda p \) lines through a point \( P \) minus \( P \) is a ghost.

**Proof.** Every line \( \ell \) meets \( P \) in either one, \( \lambda p + 1 \) or \( q + 1 \) points. In all cases \( m = 1 \mod p \) and

\[
G^P(\ell) = (\lambda p + 1)q + 1 - m = 0 \mod p.
\]

Therefore, every line is a ghost, as well as any affine plane contained in \( \text{PG}(2,q) \).

It would be desirable to define a binary operation in order to endow the subsets of \( \text{PG}(2,q) \) with a group structure, so that the set of ghosts is stable under such an operation. Unfortunately, the usual set-theoretical union is not a good choice. Consider for instance the two lines \( \ell_1, \ell_2 \) of \( \text{PG}(2,2) \), whose points have coordinates satisfying \( X = 0 \) and \( Y = 0 \), respectively. Lines are ghosts of \( \text{PG}(2,2) \); their union consists of the five points \((0,1,0), (0,0,1), (0,1,1), (1,0,0), (1,1,0)\) and the corresponding power sum polynomial is

\[
G^{\ell_1 \cup \ell_2} = Y + Z + (Y + Z) + X + (X + Y) = Y,
\]

so the union of two ghosts is not a ghost in general. To deal with a deeper algebraic structure, we need to consider a different kind of operation.

### 4.1 Multiset sum

The structure of all solutions of a same tomographic problem can be described by linear algebra as the sum between a peculiar solution and the vector subspace of ghosts (see [5]). Concerning power sum polynomials, the usual set-theoretical union is not enough and has to be replaced with the multiset sum.

Let \( A \) be a multiset, namely, a set whose elements can appear with multiplicity greater than one. Denote by \( m_A(x) \) the multiplicity of the element \( x \)
in $A$, which is zero if $x \notin A$. The multiset sum of two multisets $A$ and $B$ is a multiset $C$ such that, for any element $x$,

$$m_C(x) = m_A(x) + m_B(x).$$

Denote the set of subsets $S$ of $\text{PG}(2, q)$, where each point $P$ is counted $m_S(P)$ mod $p$ times, by $p^{\text{PG}(2, q)}$. Of course $p^{\text{PG}(2, q)}$ has $p^{q^2+q+1}$ elements. Moreover, consider the binary operation $\uplus_p$, which is the multiset sum modulo $p$.

**Lemma 7.** $(p^{\text{PG}(2, q)}, \uplus_p)$ is an abelian $p$-group.

**Proof.** The operation $\uplus_p$ is clearly internal to $p^{\text{PG}(2, q)}$, associative and commutative. The identity element is the empty set and the inverse of a subset $S$, whose element $P_i$ is counted $\lambda_i$ times ($i = 1, \ldots, |S|$), is the subset where $P_i$ is counted $p - \lambda_i$ times.

Also, $p^{\text{PG}(2, q)}$ is a $p$-group since every non-identity element has period $p$. ϕ is a homomorphism between abelian groups. In particular, if $A \subseteq B$, then $G_{B \setminus A} = G_B - G_A$.

The kernel of $\varphi$ is the set of ghosts $G$, which is indeed a subgroup of $p^{\text{PG}(2, q)}$. Moreover

$$p^{\text{PG}(2, q)} / \ker \varphi \cong \text{im} \varphi.$$

We now extend the results of Theorems 5 and 6 to multisets. For a subset $A$ of a multiset $B$, we define the complement of $A$ in $B$ as the multiset where each element $b \in B$ is counted $m_B(b) - m_A(b)$ times.

**Theorem 8.** Let $S$ be a ghost. Then the complement of $S$ is a ghost. Moreover, lines and (multiset) sums of lines are ghosts of $\text{PG}(2, q)$.

**Proof.** It results $G^{\text{PG}(2, q) \setminus S} = G^{\text{PG}(2, q)} - G^S = 0 - 0 = 0$. The statement about lines follows from Theorem 6 and the properties of $\uplus_p$. 

## 5 The case $q = p$

From now on we focus on the case $q = p^h = p$ (i.e., $h = 1$), namely, we refer to prime fields. In order to get information about the size of the subgroup of ghosts, we argue on the size of the image of $\varphi$. 


5.1 Surjectivity of $\varphi$

We now prove that, for $q = p$ prime, the dimension of $\text{im} \varphi$ is $\binom{p+1}{2}$, namely, the function $\varphi$ is onto.

If $p = 2$, it is trivial to prove that the images of points $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ constitute a basis of $F_2[X,Y,Z]$. For $p$ odd, we will prove that the set consisting of the images of the $\binom{p+1}{2}$ points

$\{(1,0,0), (1,0,1), (1,0,2), \ldots, (1,0,p-1), (1,1,0), (1,1,1), \ldots, (1,1,p-2), \ldots, (1,p-2,0), (1,p-2,1), (1,p-1,0)\}$

is linearly independent. This can be done by showing that the matrix having as rows the components (w.r.t. the canonical basis of $F_p[X,Y,Z]$) of the images of the above points is non-singular. Each entry of the matrix is the coefficient of a certain monomial in the development of $(X + bY + cZ)^{p-1}$, where $(1, b, c)$ is one of the above points. Since from the column corresponding to the monomial $X^{p-1}Y^{j}Z^i$ we can extract the coefficient $\binom{p-1}{i,j}$ and this does not interfere with the fact that the determinant is either zero or non-zero, we will omit the coefficients and simply write the value of $b^j c^i$. By reordering rows and columns in a suitable way we get the matrix in Table 1, which is a block lower triangular matrix. Its determinant is given by the product of the determinants of its blocks.

The four blocks are: the one by one upper leftmost block $(1)$, two equal blocks

$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 2 & 2^2 & 2^3 & \ldots & 1 \\ \vdots & & & & \\ p-1 & (p-1)^2 & (p-1)^3 & \ldots & 1 \end{pmatrix}$

and the remaining block of order $\binom{p-2}{p-1}$.

The first three blocks are non-singular (in particular, the second and the third blocks are Vandermonde matrices), so the matrix has non-zero determinant if and only if the fourth block has.
The columns of the fourth block are indexed as $bc, b^2c, bc^2, \ldots, bc^{p-2}$, so we can extract a factor $bc$ from every row to get, after reordering rows and columns suitably, the matrix in Table 2.

| $(1, 1, 1)$ | $1$ | $b$ | $b^2$ | $\ldots$ | $b^{p-3}$ | $c$ | $bc$ | $\ldots$ | $b^{p-4}c$ | $c^2$ | $\ldots$ | $c^{p-3}$ |
|-------------|----|----|----|---|---|----|----|---|---|---|---|---|
| $(1, 2, 1)$ | $1$ | $2$ | $2^2$ | $\ldots$ | $2^{p-3}$ | $1$ | $2$ | $\ldots$ | $2^{p-4}$ | $1$ | $\ldots$ | $1$ |
| $(1, 3, 1)$ | $1$ | $3$ | $3^2$ | $\ldots$ | $3^{p-3}$ | $1$ | $3$ | $\ldots$ | $3^{p-4}$ | $1$ | $\ldots$ | $1$ |
| $(1, p-2, 1)$ | $1$ | $p-2$ | $(p-2)^2$ | $\ldots$ | $(p-2)^{p-3}$ | $1$ | $p-2$ | $\ldots$ | $(p-2)^{p-4}$ | $1$ | $\ldots$ | $1$ |
| $(1, 1, 2)$ | $1$ | $1$ | $1$ | $\ldots$ | $1$ | $2$ | $2$ | $\ldots$ | $2$ | $2^2$ | $\ldots$ | $2^{p-3}$ |
| $(1, p-3, 2)$ | $1$ | $p-3$ | $(p-3)^2$ | $\ldots$ | $(p-3)^{p-3}$ | $2$ | $(p-3) \cdot 2$ | $\ldots$ | $(p-3)^{p-4} \cdot 2$ | $2^2$ | $\ldots$ | $2^{p-3}$ |
| $(1, 1, 3)$ | $1$ | $1$ | $1$ | $\ldots$ | $1$ | $3$ | $3$ | $\ldots$ | $3$ | $3^2$ | $\ldots$ | $3^{p-3}$ |
| $(1, 1, p-2)$ | $1$ | $1$ | $1$ | $\ldots$ | $1$ | $p-2$ | $p-2$ | $p-2$ | $\ldots$ | $(p-2)^2$ | $\ldots$ | $(p-2)^{p-3}$ |

Table 2: The $\frac{(p-2)(p-1)}{2}$ lower leftmost block.

In order to prove that the determinant of the matrix in Table 2 is non-zero, we apply some basic operations to its rows in order to obtain a block upper triangular matrix, whose blocks are Vandermonde matrices and which is singular if and only if the starting matrix is. The procedure consists of $p-2$ steps; in each of them we consider some rows as pivotal and substitute to a non-pivotal row a linear combination of its and the corresponding pivotal row, in order to have zeroes as entries in the columns corresponding to a certain power of $c$.

Denote by $(1, b, c)^{(n)}$ the row corresponding to the image of the point $(1, b, c)$ at the $n$-th step of the procedure. It is defined recursively as follows:

\[
(1, b, c)^{(0)} : \text{ the row corresponding to } \varphi(1, b, c),
\]

\[
(1, b, c)^{(1)} := (1, b, c)^{(0)} - (1, b, 1)^{(0)}, \quad c \geq 2,
\]

\[
(1, b, c)^{(n)} := \frac{(1, b, c)^{(n-1)} - (1, b, n)^{(n-1)}}{c - (n-1)} - (1, b, n)^{(n-1)}, \quad n \geq 2, c \geq n + 1,
\]

where the subtraction is intended to be element-wise. The third entry is at least $n + 1$ since at Step $n$ the pivotal rows are $(1, b, n)^{(n-1)}$, $b = 1, \ldots, p - 1 - n$, so only rows such that $c \geq n + 1$ will be modified.

After each step, the matrix becomes block upper triangular consisting of two blocks: the upper leftmost block is a Vandermonde matrix and the other block has to be treated at the next step. Rows in the matrix in Table 2 are ordered such that the first $p-2$ rows $(1, b, 1), b = 1, \ldots, p - 2)$ are the pivotal ones in the first step, the following $p-3$ ones $(1, b, 2), b = 1, \ldots, p - 3)$ will be the pivotal rows in the second step after the operations, and so on.

At Step $n$, the row $(1, b, c)^{(n)}$ has the entry corresponding to the column $b^\lambda c^\mu$ equal to:

- for $n = 1$: $b^\lambda (c^\mu - 1)$.
• for \( n = 2n', \ n' \geq 1 \):

\[
\sum_{i_1=0}^{\mu-2} (2^{\mu-1} - 1) \sum_{i_2=0}^{i_1-2} (4^{i_1-1} - 3^{i_1-1}) \sum_{i_3=0}^{i_2-2} \ldots \\
\cdot \sum_{i_{n'=1}}^{i_{n'-1}} (c - n) \left(n^{i_{n'-1} - 1} - (n - 1)^{i_{n'-1} - 1} \right) c^{i_{n'}} ;
\]

• for \( n = 2n' + 1, \ n' \geq 1 \):

\[
\sum_{i_1=0}^{\mu-2} (2^{\mu-1} - 1) \sum_{i_2=0}^{i_1-2} (4^{i_1-1} - 3^{i_1-1}) \sum_{i_3=0}^{i_2-2} \ldots \\
\cdot \sum_{i_{n'=1}}^{i_{n'-1}} ((2n')^{i_{n'-1} - 1} - (2n' - 1)^{i_{n'-1} - 1}) (c^{i_{n'}} - n^{i_{n'}}) .
\]

The above formulas may be proven by induction on \( n \). Note that, for \( \mu < n \), there are empty summations and therefore the entry is zero. Moreover, all elements of row \((1, b, c)^{(n)}\) are divisible by \( c - n \) even over the integers.

In particular, the pivotal rows at the next step, say \( n + 1 \), have a Vandermonde submatrix in the columns corresponding to the power \( b^\lambda c^n \), \( \lambda = 0, \ldots, p - 2 - n \) (it is obtained by substituting \( \mu = n \) and \( c = n + 1 \) in the above formulas; note that, for \( \mu = n \), all summations reduce to a single term).

At the final step \( p - 2 \), the resulting matrix is block triangular and each block is a Vandermonde matrix with no repeated rows, so non-singular. We can conclude that the images of points in \([\mathbf{1}]\) are linearly independent and then \( \text{im} \varphi \) has dimension \( \left(\begin{array}{c} p+1 \\ 2 \end{array}\right) \).

In the next example we show how the procedure works.

**Example 9.** Set \( p = 7 \) and consider the \( \frac{7 	imes 6}{2} = 15 \) points

\[
(1, 1, 1), (1, 1, 2), (1, 1, 3), (1, 1, 4), (1, 1, 5), (1, 2, 1), (1, 2, 2), (1, 2, 3), (1, 2, 4), \\
(1, 3, 1), (1, 3, 2), (1, 3, 3), (1, 4, 1), (1, 4, 2), (1, 5, 1),
\]

which are those, among the \( \binom{7+1}{2} = 28 \) points whose images constitute a basis for \( \text{im} \varphi \), having no zero coordinate. This means that the above points are those whose images constitute the block on which the procedure is applied.
The initial matrix is 

\[
\begin{array}{cccccccccccc}
(1,1,1) & 1 & b & b^2 & b^3 & b^4 & c & bc & b^2c & b^3c & b^4c & c^2 & bc^2 & b^2c^2 & c^3 & bc^3 & c^4 \\
(1,2,1) & 1 & 2 & b^2 & b^3 & b^4 & 1 & 2 & b^2 & b^3 & 1 & 2 & b^2 & 1 & 2 & 1 \\
(1,3,1) & 1 & 3 & 2^2 & 3^2 & 3^4 & 1 & 3 & 2^3 & 3^3 & 1 & 3 & 2^3 & 1 & 3 & 1 \\
(1,4,1) & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 4^3 & 1 & 4 & 4^2 & 1 & 4 & 1 \\
(1,5,1) & 1 & 5 & 5^2 & 5^3 & 5^4 & 1 & 5 & 5^2 & 5^3 & 1 & 5 & 5^2 & 1 & 5 & 1 \\
(1,1,2) & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 1 & 2 & 1 \\
(1,2,2) & 1 & 2 & b^2 & 2^3 & 2^4 & 1 & 2 & b^2 & 2^3 & 2^4 & 1 & 2 & b^2 & 1 & 2 \\
(1,3,2) & 1 & 3 & 3^2 & 3^3 & 3^4 & 1 & 3 & 3^3 & 3^2 & 3^4 & 1 & 3 & 3^3 & 1 & 3 \\
(1,4,2) & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 1 & 4 \\
(1,1,3) & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
(1,2,3) & 1 & 2 & b^2 & 2^3 & 2^4 & 1 & 2 & b^2 & 2^3 & 2^4 & 1 & 2 & b^2 & 1 & 2 \\
(1,3,3) & 1 & 3 & 2^2 & 2^3 & 2^4 & 1 & 3 & 2^2 & 2^3 & 2^4 & 1 & 3 & 2^2 & 1 & 3 \\
(1,4,3) & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 1 & 4 \\
(1,1,4) & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
(1,2,4) & 1 & 2 & 2^2 & 2^3 & 2^4 & 1 & 2 & 2^2 & 2^3 & 2^4 & 1 & 2 & 2^2 & 1 & 2 \\
(1,3,4) & 1 & 3 & 2^2 & 2^3 & 2^4 & 1 & 3 & 2^2 & 2^3 & 2^4 & 1 & 3 & 2^2 & 1 & 3 \\
(1,4,4) & 1 & 4 & 2^2 & 2^3 & 2^4 & 1 & 4 & 2^2 & 2^3 & 2^4 & 1 & 4 & 2^2 & 1 & 4 \\
(1,1,5) & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

The upper leftmost 5 by 5 block is a Vandermonde matrix and the corresponding rows will be the pivotal ones at Step 1. The other rows will be manipulated so that the first five entries are zero. Therefore, matrix at Step 1 is 

\[
\begin{array}{cccccccccccc}
(1,1,1) & 1 & b & b^2 & b^3 & b^4 & c & bc & b^2c & b^3c & b^4c & c^2 & bc^2 & b^2c^2 & c^3 & bc^3 & c^4 \\
(1,2,1) & 1 & 2 & b^2 & b^3 & b^4 & 1 & 2 & b^2 & b^3 & 1 & 2 & b^2 & 1 & 2 & 1 \\
(1,3,1) & 1 & 3 & 2^2 & 3^2 & 3^4 & 1 & 3 & 2^3 & 3^3 & 1 & 3 & 2^3 & 1 & 3 & 1 \\
(1,4,1) & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 4^3 & 1 & 4 & 4^2 & 1 & 4 & 1 \\
(1,1,2) & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 2 & 2 & 1 & 2 & 1 & 2 & 1 \\
(1,2,2) & 1 & 2 & b^2 & 2^3 & 2^4 & 1 & 2 & b^2 & 2^3 & 2^4 & 1 & 2 & b^2 & 1 & 2 \\
(1,3,2) & 1 & 3 & 3^2 & 3^3 & 3^4 & 1 & 3 & 3^3 & 3^2 & 3^4 & 1 & 3 & 3^3 & 1 & 3 \\
(1,4,2) & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 1 & 4 \\
(1,1,3) & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
(1,2,3) & 1 & 2 & b^2 & 2^3 & 2^4 & 1 & 2 & b^2 & 2^3 & 2^4 & 1 & 2 & b^2 & 1 & 2 \\
(1,3,3) & 1 & 3 & 2^2 & 2^3 & 2^4 & 1 & 3 & 2^2 & 2^3 & 2^4 & 1 & 3 & 2^2 & 1 & 3 \\
(1,4,3) & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 4^3 & 4^4 & 1 & 4 & 4^2 & 1 & 4 \\
(1,1,4) & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
(1,2,4) & 1 & 2 & 2^2 & 2^3 & 2^4 & 1 & 2 & 2^2 & 2^3 & 2^4 & 1 & 2 & 2^2 & 1 & 2 \\
(1,3,4) & 1 & 3 & 2^2 & 2^3 & 2^4 & 1 & 3 & 2^2 & 2^3 & 2^4 & 1 & 3 & 2^2 & 1 & 3 \\
(1,4,4) & 1 & 4 & 2^2 & 2^3 & 2^4 & 1 & 4 & 2^2 & 2^3 & 2^4 & 1 & 4 & 2^2 & 1 & 4 \\
(1,1,5) & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

where the asterisk means any value. In Step 2 we focus on the 10 by 10 lower rightmost block. Rows corresponding to \((1, b, 2)^{(1)}\), \(b = 1, 2, 3, 4\), form a Vandermonde matrix in the first four columns and they will be the pivotal ones.
The (sub-)matrix at Step 2 is

\[
\begin{array}{cccccccc}
1 & 1 & 1 & 1 & * & \ldots \\
1 & 2 & 2^2 & 2^3 & * & \ldots \\
1 & 3 & 3^2 & 3^3 & * & \ldots \\
1 & 4 & 4^2 & 4^3 & * & \ldots \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 6 & 6 & 25 \\
0 & 0 & 0 & 0 & 1 & 2 & 2^2 & 6 & 2 \cdot 6 & 25 \\
0 & 0 & 0 & 0 & 1 & 3 & 3^2 & 6 & 3 \cdot 6 & 25 \\
0 & 0 & 0 & 0 & 2 & 2 & 2 & 14 & 14 & 70 \\
0 & 0 & 0 & 0 & 3 & 3 & 3 & 24 & 24 & 141 \\
\end{array}
\]

At Step 3 we consider the 6 by 6 lower rightmost submatrix, whose pivotal rows will be \((1, b, 3)\), \(b = 1, 2, 3\), and the remaining rows are modified as follows:

\[
\begin{array}{cccccccc}
c^2 & bc^2 & b^2c^2 & c^3 & bc^3 & c^4 \\
1 & 1 & 1 & * & \ldots \\
1 & 2 & 2^2 & * & \ldots \\
1 & 3 & 3^2 & * & \ldots \\
0 & 0 & 0 & 1 & 1 & 10 \\
0 & 0 & 0 & 1 & 2 & 10 \\
0 & 0 & 0 & 2 & 2 & 22 \\
\end{array}
\]

The matrix at Step 4 is the following one:

\[
\begin{array}{cccc}
c^3 & bc^3 & c^4 \\
1 & 1 & * \\
1 & 2 & * \\
0 & 0 & 1 \\
\end{array}
\]

At Step 5 = 7 – 2 the one by one matrix (1) is left. Therefore, the initial matrix has been transformed into a block triangular matrix, whose blocks are Vandermonde matrices with no rows repeated, and so non-singular. This means that also the initial matrix is non-singular. Combined with the fact that even the other three blocks of the matrix, whose rows are the images of the 28 points as in [1], are non-singular, it results that \(\text{im} \varphi\) has dimension 28.

The knowledge of \(\dim \text{im} \varphi\) enables us to compute the size of the ghost subgroup \(\mathcal{G}\).

**Theorem 10.** \(|\mathcal{G}| = p^{\left(\begin{array}{c} p+1 \\ 2 \end{array}\right)} + 1\).

**Proof.** \(\text{im} \varphi\) has \(p^{\left(\begin{array}{c} p+1 \\ 2 \end{array}\right)}\) elements. So, there are

\[
\frac{p^{p^2+p+1}}{p^{\left(\begin{array}{c} p+1 \\ 2 \end{array}\right)}} = p^{\left(\begin{array}{c} p+1 \\ 2 \end{array}\right)} + 1
\]

ghosts in \(\text{PG}(2, p)\).
6 Conclusions

In this paper we have addressed the problem of classifying the subsets of \( \text{PG}(2, q) \) associated to a same power sum polynomial. By exploiting some similarities with the classical tomographic problem, we have shown that two sets with a same power sum polynomial differ, in the multiset sum sense, by a set whose power sum polynomial is the null one. In analogy to tomography, such a set has been called ghost. We have then counted the number of ghosts of \( \text{PG}(2, p) \) by arguing on the image of the function \( \varphi \), which maps a (multi)set of \( \text{PG}(2, p) \) to the corresponding power sum polynomial.

The present paper may be considered as a starting point in the study of the connection between (multi)sets of points in \( \text{PG}(2, q) \) and their corresponding power sum polynomials within the framework of the polynomial technique for finite geometries. Therefore several future developments may be taken into account.

An immediate related research could be the study of the behavior of the power sum polynomials under the intersection of two sets.

Secondly, we aim to study the size of \( \text{im} \varphi \) even when \( h \) is greater than one. This would give the exact number of ghosts in every projective plane.

Moreover, the subgroup of ghosts deserves a deeper investigation. In particular, we would like to find, if possible, a set of generators for the ghosts.

Further, our investigation has dealt with the planar case, due to its connections with the tomographic problem. Another development is the extension to higher dimensions, to treat the problem in full generality.

References

[1] A. Blokhuis. *Polynomials in finite geometries and combinatorics*, pages 35–52. London Mathematical Society Lecture Note Series. Cambridge University Press, 1993.

[2] F. Buekenhout, editor. *Handbook of Incidence Geometry*. North Holland, 1995.

[3] J. De Beule. Direction problems in affine spaces. *Galois Geometries and Applications*, pages 79–94, 2014.

[4] P.C. Fishburn, J.C. Lagarias, J.A. Reeds, and L.A. Shepp. Sets uniquely determined by projections on axes. II. Discrete case. *Discrete Math.*, 91(2):149–159, 1991.

[5] L. Hajdu and R. Tijdeman. Algebraic aspects of discrete tomography. *J. Reine Angew. Math.*, 534:119–128, 2001.

[6] J. Radon. Über die Bestimmung von Funktionen durch ihre Integralwerte längs gewisser Mannigfaltigkeiten. *Ber. Verh. Sächs. Akad. Wiss. Leipzig Math.-Phys. Kl.*, (69):262–277, 1917.

[7] L. Rédei. *Lacunary polynomials over finite fields*. North Holland, Amsterdam, 1973.
[8] P. Sziklai. Polynomials in finite geometry. Manuscript. Available online at http://web.cs.elte.hu/~sziklai/polynom/poly08feb.pdf.

[9] T. Szönyi, A. Gács, and Zs. Weiner. On the spectrum of minimal blocking sets in PG(2, q). J. Geom., 76(1-2):256–281, 2003.

[10] T. Szönyi and Zs. Weiner. Stability of k mod p multisets and small weight codewords of the code generated by the lines of PG(2, q). J. Combin. Theory Ser. A, 157:321–333, 2018.