Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-022-01051-1

Some hypersurfaces over finite fields, minimal codes and secret sharing schemes

Angela Aguglia[1] · Michela Ceria[1] · Luca Giuzzi[2]

Received: 26 August 2021 / Revised: 19 April 2022 / Accepted: 21 April 2022

Abstract

Linear error-correcting codes can be used for constructing secret sharing schemes; however, finding in general the access structures of these secret sharing schemes and, in particular, determining efficient access structures is difficult. Here we investigate the properties of certain algebraic hypersurfaces over finite fields, whose intersection numbers with any hyperplane only takes a few values; these varieties give rise to q-divisible linear codes with at most 5 weights. Furthermore, for q odd, these codes turn out to be minimal and we characterize the access structures of the secret sharing schemes based on their dual codes. Indeed, the secret sharing schemes thus obtained are democratic, that is each participant belongs to the same number of minimal access sets and can easily be described.

Keywords Algebraic variety · Hermitian variety · Linear code · Secret sharing scheme

MSC Classification 94B05 · 51A05 · 51E21

Communicated by C. Blundo.

Angela Aguglia, Michela Ceria and Luca Giuzzi contributed equally to this work.

The authors wish to thank M. Bonini and M. Borello for having pointed out several very recent references on the relationship between minimal linear codes and projective systems, as well as for having corrected a misattribution present on the first version of the preprint.

✉ Angela Aguglia
angela.aguglia@poliba.it

Michela Ceria
michela.ceria@poliba.it

Luca Giuzzi
luca.giuzzi@unibs.it

[1] Dipartimento di Meccanica, Matematica e Management,
Politecnico di Bari, Via Orabona 4, 70125 Bari, Italy

[2] DICATAM, University of Brescia, Via Branze 53, 25123 Brescia, Italy

Published online: 21 May 2022

1 Introduction

A *secret sharing scheme* (henceforth SSS for short) is a cryptographic technique for the management of the access to a secret s by a collective partnership. The partners, also called *participants*, (to the scheme) hold shares of information and access is allowed only to certain qualified groups of them, who can be given authorization by combining together their shares. For any given SSS, a set of participants who can reconstruct the secret value s from its shares is said to be an *access set*. Also, an access set is *minimal* if none of its proper subsets is in turn an access set itself. The family of all the minimal access sets for a SSS is called the *access structure* of the SSS. In [10], Massey devised a SSS based on linear codes and pointed out the relationship between the minimal codewords of the dual code and the access structure. We refer to his work and [7] for details on the construction and performance of these schemes. This provides a motivation for determining the set of all minimal codewords of an arbitrary linear code over a finite field. This problem turns out to be, in general, hard; however some useful criteria might be obtained in the case of projective codes. Recently, several authors have considered this problem; see e.g. [7, 9, 14] and the references therein.

In the present paper, we study certain algebraic hypersurfaces in the finite projective space $\mathrm{PG}(r, q^2)$ over $\mathrm{GF}(q^2)$ of dimension $r \geq 3$, whose intersection numbers with any hyperplane only take a few values. These hypersurfaces arise in the construction of quasi-Hermitian varieties and are, as such, also of independent interest; see [1]. Then we determine the five weights of the corresponding q^2-ary projective codes proving that, except for $r = 3$ and q odd, these codes are all *q-divisible*, that is their weights are divisible by q; see [13]. Finally, for q odd, we show that these projective codes are minimal and hence the related SSS's have an efficient access structures as they are democratic SSS's, namely, each participant is involved in the same number of minimal access sets. We also discuss how these access structures are related to the involved geometry.

The paper is organized into 6 sections. Section 2 introduces the necessary background on quasi-Hermitian varieties and minimal codes. In Sect. 3, we exhibit an infinite family of q^2-ary minimal codes arising from quasi-Hermitian varieties. In Sect. 4, we study the intersections of certain algebraic hypersurfaces of degree $2q$ over $\mathrm{GF}(q^2)$ with the extremal subspaces of $\mathrm{PG}(r, q^2)$ and, as a byproduct, in Sect. 5 we provide an infinite family of q-divisible minimal codes. In 6 we consider the access structures arising from projective codes and apply our results to the construction of infinite families of SSS's, which can be described algebraically.

Our main results are contained in Theorems 6, 7 and 13.

2 Preliminaries

An $[n, r+1]_q$ *projective system* is a collection $\mathcal{V}$ of n not necessarily distinct points in the projective space $\mathrm{PG}(r, q)$ over the finite field $\mathrm{GF}(q)$ of order q, with q a prime power. Fix a reference frame in $\mathrm{PG}(r, q)$, with homogeneous coordinates $(X_0, X_1, \ldots, X_r)$, and construct a matrix G by taking as columns the coordinates of the points of $\mathcal{V}$, suitably normalized. The code $\mathcal{C}(\mathcal{V})$ having G as generator matrix is called *the code determined from* $\mathcal{V}$.

It is straightforward to see that, even if $\mathcal{C}(\mathcal{V})$ is not uniquely determined by $\mathcal{V}$, all the codes that might be obtained in this way are in fact equivalent; so we shall often speak of *the* projective code determined by $\mathcal{V}$.

The spectrum of the intersections of $\mathcal{V}$ with the hyperplanes of $\mathrm{PG}(r,q)$ is related with the list of the weights of the associated code; the *k-higher weights* of $\mathcal{C}(\mathcal{V})$ are given by

$$d_k(\mathcal{C}) = n - \max\{\mid \mathcal{V}\cap\pi \mid : \pi \text{ is a projective subspace of codimension k in } \mathrm{PG}(r,q)\};$$

note that the first higher weight $d_1(\mathcal{C}(\mathcal{V}))$ is actually the minimum distance of the code $\mathcal{C}(\mathcal{V})$. We refer to [12] for further details on this geometric approach to codes.

Error correcting codes can be used in order to devise *access schemes* or SSS's. In his seminal work [10], Massey proposed the use of minimal codewords in a *dual code*, in order to specify the access structure of a SSS.

Definition 1 Let $\mathcal{C}$ be a code of length n. For any codeword $c \in \mathcal{C}$ and $1 \leq i \leq n$ the *support* of c is the set $\mathrm{supp}(c) := \{i : c_i \neq 0\}$ of the positions of its non-zero components. Given $c, c' \in \mathcal{C}$ we write that $c' \preccurlyeq c$ if $\mathrm{supp}(c') \subseteq \mathrm{supp}(c)$. We say that c is a *minimal word* of $\mathcal{C}$ if $c' \preccurlyeq c$ implies that there is $\alpha \in \mathrm{GF}(q)$ such that $c' = \alpha c$.

Remark 1 According to our definition, a minimal codeword is just a word of $\mathcal{C}$ which is not covered by any other linearly independent codewords. From the point of view of the geometric description of the code, this is most convenient and this is consistent with the terminology of [9]. We point out that in [10] for a codeword to be minimal it is also required that the leftmost non-zero component of the word must be 1 (such codewords are called *minimal AS-codewords* in [9]). Accordingly, if $\mathcal{C}$ is a linear code, the minimal AS-codewords are exactly those minimal codewords of $\mathcal{C}$ which lie in the affine space $\mathrm{PG}(\mathcal{C}) \setminus \Sigma_\infty$, where Σ_∞ is the hyperplane at infinity of equation $X_0 = 0$.

It is well known that a linear code is spanned by its minimal words and that all its minimum weight codewords are minimal (according to our definition), but little can be said about the remaining words in general.

Definition 2 A linear code is a *minimal code* if all of its codewords are minimal.

Ashikhmin and Barg in [3] provided a sufficient condition so that an $[n,k]$-linear code $\mathcal{C}$ over $\mathrm{GF}(q)$ is minimal, namely

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}, \tag{1}$$

where $w_{\min}$ and $w_{\max}$ are respectively the minimum and maximum weight of non-zero codewords of $\mathcal{C}$.

Nice examples of linear codes can be obtained by considering some algebraic varieties of $\mathrm{PG}(r,q)$. In general, pointsets with few intersection numbers with respect to the hyperplanes provide codes with interesting structure.

Here we shall take into account *quasi-Hermitian varieties* in $\mathrm{PG}(r,q^2)$, that is, point sets having the same size and the same intersection numbers with respect to hyperplanes as a non-singular Hermitian variety $\mathcal{H}(r,q^2)$ of $\mathrm{PG}(r,q^2)$. More in detail, the size of a quasi-Hermitian variety $\mathcal{V}$ is

$$\mid \mathcal{H}(r,q^2) \mid = \frac{(q^{r+1}+(-1)^r)(q^r-(-1)^r)}{(q^2-1)},$$

whereas the intersection numbers of $\mathcal{V}$ with respect to hyperplanes are

$$\mid \mathcal{H}(r-1,q^2) \mid = \frac{(q^r+(-1)^{r-1})(q^{r-1}-(-1)^{r-1})}{q^2-1},$$

and

$$| \Pi_0\mathcal{H}(r-2,q^2) |= \frac{(q^r+(-1)^{r-1})(q^{r-1}-(-1)^{r-1})}{q^2-1} + (-1)^{r-1}q^{r-1},$$

where Π_i is an i-dimensional space of $\mathrm{PG}(r,q^2)$ and $\Pi_0\mathcal{H}(r-2,q^2)$ is a cone, the join of the vertex Π_0 to a non-singular Hermitian variety $\mathcal{H}(r-2,q^2)$ of a projective subspace Π_{r-2} which does not contain Π_0. A non-singular Hermitian variety of $\mathrm{PG}(r,q^2)$ is, by definition, a quasi-Hermitian variety: the *classical quasi-Hermitian variety*.

3 Projective minimal codes

In recent years [4–6, 11] constructions of minimal codes arising from projective systems have been considered. In particular, in [11] it has been proved that minimal projective codes are equivalent to projective systems which are *cutting* 1-blocking sets (see [5] for the definition).

Recall that a cutting 1-blocking set (or, in brief a *cutting* blocking set) $\mathcal{H}$ is a subset of $\mathrm{PG}(r,q)$ such that for any hyperplane Σ we have $\langle\Sigma\cap\mathcal{H}\rangle=\Sigma$.

Let $\mathcal{H}$ be a set of points of $\mathrm{PG}(r,q)$, and $\mathcal{C}(\mathcal{H})$ be one of its associated projective codes. It is straightforward to see that the words of a projective code determined by $\mathcal{H}\subseteq\mathrm{PG}(V)$, where $\langle\mathcal{H}\rangle=\mathrm{PG}(V)$ and V is the vector space underlying $\mathrm{PG}(r,q)$, correspond exactly to the evaluations of the elements of the dual V^* of V on the given projective system. The following result was proved in [2] and independently in [11].

Theorem 1 *Let $\mathcal{H}$ be a set of N points of $\mathrm{PG}(r,q)$ such that $\langle\mathcal{H}\rangle=\mathrm{PG}(r,q)$. For each $i\in\{1\ldots N\}$ let $P_i\in\mathrm{GF}(q)^{r+1}$ be a fixed representative of a point $[P_i]\in\mathcal{H}$ and denote by $\mathcal{C}(\mathcal{H})$ the projective linear code having generator matrix whose columns are the vectors P_i. Then $\mathcal{C}(\mathcal{H})$ is a minimal code if and only if for any hyperplane Σ of $\mathrm{PG}(r,q)$*

$$\langle\Sigma\cap\mathcal{H}\rangle=\Sigma. \tag{2}$$

A general problem is to determine when the set of points of an algebraic variety $\mathcal{H}$ in $\mathrm{PG}(r,q)$ is a cutting blocking set. It is easy to see that elliptic quadrics in $\mathrm{PG}(3,q)$, as well as degenerate hypersurfaces, in general, are not. In [6] the authors proved that if $\mathcal{H}$ is a non-singular Hermitian variety in a given canonical form or a quadric in projective dimension $r\geq 4$, then $\mathcal{H}$ is a cutting blocking set and thus $\mathcal{C}(\mathcal{H})$ is minimal. We can easily extend the same result to any quasi-Hermitian variety of $\mathrm{PG}(r,q^2)$. If $\mathcal{H}$ is a quasi-Hermitian variety of $\mathrm{PG}(r,q^2)$ then $\mathcal{C}(\mathcal{H})$ has 2 weights. It is straightforward to see that Condition (1) does not hold but Theorem 1 can be applied as follows.

Theorem 2 *Let $\mathcal{H}$ be a quasi-Hermitian variety in $\mathrm{PG}(r,q^2)$. Then, $\mathcal{C}(\mathcal{H})$ is a minimal code.*

Proof Since a quasi-Hermitian variety is a projective variety whose intersections with hyperplanes have the same cardinalities as the intersection of a Hermitian variety, we first see that $\mathcal{H}$ cannot be contained in any hyperplane of $\mathrm{PG}(r,q^2)$. Also, suppose that there is a hyperplane φ such that $\dim(\langle\mathcal{H}\cap\varphi\rangle)<r-1$. This means that $\mathcal{H}\cap\varphi\subseteq\Sigma$ with Σ a projective space of dimension at most $r-2$. Thus, we would have

$$| \mathcal{H}\cap\varphi |\leq \frac{q^{2r-2}-1}{q^2-1},$$

which is not possible. The thesis now follows from Theorem 1. □

Remark 2 If we want to study codes arising from higher degree functions defined over some algebraic varieties $\mathcal{H}$, a convenient setting is to use Veronese embeddings and represent these codes (in turn) as projective codes. In particular, to investigate quadratic sections of $\mathcal{H}$, we just apply the quadratic Veronese embedding

$$\nu_r^2 : \begin{cases} \mathrm{PG}(r,q) \to \mathrm{PG}(\frac{r^2+3r}{2}, q) \\ [(x_0,\dots,x_r)] \to [(x_0^2, x_0x_1, \dots, x_0x_r, x_1^2, \dots, x_r^2)] \end{cases}$$

and then consider Theorem 1.
We denote this new code, arising from the projective system of $\nu_r^2(\mathcal{H})$ as $\mathcal{C}^2$. Observe however, that in general it is not true that $\langle \nu_r^2(\mathcal{H})\rangle = \mathrm{PG}(\frac{r^2+3r}{2}, q)$.

4 Hypersurfaces with few intersection numbers

In $\mathrm{PG}(r,q^2)$ with homogeneous coordinates $(X_0, X_1, \dots, X_r)$, consider the affine space $\mathrm{AG}(r,q^2)$ whose infinite hyperplane Σ_∞ has equation $X_0 = 0$. Then $\mathrm{AG}(r,q^2)$ has affine coordinates $(x_1, x_2, \dots, x_r)$ where $x_i = X_i/X_0$ for $i \in \{1,\dots,r\}$. Consider the algebraic variety $\mathcal{B}$ of affine equation

$$x_r^q - x_r + \alpha^q(x_1^{2q} + \cdots + x_{r-1}^{2q}) - \alpha(x_1^2 + \cdots + x_{r-1}^2) = (\beta^q - \beta)(x_1^{q+1} + \cdots + x_{r-1}^{q+1}), \tag{3}$$

where $\alpha \in GF(q^2)^*$, $\beta \in GF(q^2) \setminus GF(q)$ and the following conditions are satisfied: for odd q,

(1) r is odd and $4\alpha^{q+1} + (\beta^q - \beta)^2 \neq 0$, or
(2) r is even and $4\alpha^{q+1} + (\beta^q - \beta)^2$ is a non–square in $\mathrm{GF}(q)$;

for even $q > 2$,

(i) r is odd, or
(ii) r is even and $\mathrm{Tr}\,(\alpha^{q+1}/(\beta^q + \beta)^2) = 0$.

In [1] the authors proved that gluing together the set of affine points of $\mathcal{B}$ with the degenerate Hermitian variety

$$\mathcal{F} = \{(0, X_1, \dots, X_r) \colon X_1^{q+1} + \cdots + X_{r-1}^{q+1} = 0\}$$

gives a quasi-Hermitian variety $\mathcal{H} = (\mathcal{B} \cap AG(r,q^2)) \cup \mathcal{F}$. In this section we study the intersection numbers of $\mathcal{B}$ with hyperplanes by a "surgery" argument, that is

- First we consider the intersection of a hyperplane Σ with the quasi-Hermitian variety $\mathcal{H}$;
- Then we remove from this intersection its points at infinity which are contained in $\mathcal{F}$ and add the possible intersections of Σ with $\mathcal{B}_\infty := \mathcal{B} \cap \Sigma_\infty$.

More concisely, our arguments are based on these facts

1. $\Sigma \cap \mathcal{B} = ((\Sigma \cap \mathcal{H}) \setminus \mathcal{H}_\infty) \cup (\Sigma \cap \mathcal{B}_\infty)$;
2. the cardinalities of $\Sigma \cap \mathcal{H}$ are known;
3. $\mid \mathcal{B} \cap AG(r,q^2) \mid = \mid \mathcal{H} \setminus \mathcal{H}_\infty \mid = q^{2r-1}$.

In particular $\mid \Sigma \cap \mathcal{B} \mid = \mid \Sigma \cap \mathcal{H} \mid - \mid \Sigma \cap \mathcal{H}_\infty \mid + \mid \Sigma \cap \mathcal{B}_\infty \mid$. Observe that for $r = 2$ $\mathcal{F} = \{P_\infty\}$ and $\mathcal{B} = \mathcal{H}$ is a Buekenhout-Metz unital of $\mathrm{PG}(2,q^2)$, see [8].

4.1 Case $r \geq 3$ and q odd

We compute the intersection numbers of $\mathcal{B}$ with respect to any hyperplane Σ of $\mathrm{PG}(r, q^2)$, with q odd. The intersection between the algebraic variety $\mathcal{B}$ and Σ_∞ is the degenerate quadric $\mathcal{B}_\infty$ of Σ_∞ with equation

$$x_1^2 + \cdots + x_{r-1}^2 = 0.$$

In this section $\mathcal{P}_i$ will denote a parabolic quadric of an i-dimensional projective space Π_i for i even, whereas $\mathcal{I}_i$ and $\mathcal{E}_i$ will denote a hyperbolic and an elliptic quadric of Π_i, with i odd. We set $\mathcal{I}_{-1} = \emptyset$ and $\mathcal{H}(-1, q^2) = \mathcal{H}(0, q^2) = \emptyset$.

Assume that $r \geq 3$ is odd. In this case $\mathcal{B}_\infty$ is a cone with vertex the point $P_\infty(0, 0, \ldots, 0, 1)$ and basis a hyperbolic quadric $\mathcal{I}_{r-2}$ of an $(r-2)$-dimensional projective space contained in Σ_∞, hence $\mid \mathcal{B}_\infty \mid = q^2[(q^{2(r-2)} - 1)/(q^2 - 1) + q^{r-3}] + 1$ and $\mid \mathcal{B} \mid = q^{2r-1} + q^2[(q^{2(r-2)} - 1)/(q^2 - 1) + q^{r-3}] + 1$.

Let Σ be a hyperplane passing through the point P_∞. Then Σ meets $\mathcal{B}_\infty$ in a cone with vertex the point P_∞ and basis either a parabolic quadric $\mathcal{P}_{r-3}$ or a cone $\Pi_0\mathcal{I}_{r-4}$. Now, suppose that the hyperplane Σ does not contain P_∞. We observe that Σ meets $\mathcal{B}_\infty$ in a hyperbolic quadric $\mathcal{I}_{r-2}$ of an $(r-2)$-dimensional projective space contained in Σ_∞. Thus, the possible values of $\mid \Sigma \cap \mathcal{B} \mid$, for any hyperplane Σ of $\mathrm{PG}(r, q^2)$, are:

(C1) $\mid \mathcal{B}_\infty \mid$;
(C2) $\mid \mathcal{H}(r-1, q^2) \mid - \mid P_\infty\mathcal{H}(r-3, q^2) \mid + \mid P_\infty\mathcal{P}_{r-3} \mid$;
(C3) $\mid \mathcal{H}(r-1, q^2) \mid - \mid P_\infty\mathcal{H}(r-3, q^2) \mid + q^2 \mid \Pi_0\mathcal{I}_{r-4} \mid + 1$;
(C4) $\mid \Pi_0\mathcal{H}(r-2, q^2) \mid - \mid P_\infty(\Pi_0\mathcal{H}(r-4, q^2)) \mid + q^2 \mid \Pi_0\mathcal{I}_{r-4} \mid + 1$;
(C5) $\mid \Pi_0\mathcal{H}(r-2, q^2) \mid - \mid P_\infty(\Pi_0\mathcal{H}(r-4, q^2)) \mid + \mid P_\infty\mathcal{P}_{r-3} \mid$;
(C6) $\mid \mathcal{H}(r-1, q^2) \mid - \mid \mathcal{H}(r-2, q^2) \mid + \mid \mathcal{I}_{r-2} \mid$;
(C7) $\mid \Pi_0\mathcal{H}(r-2, q^2) \mid - \mid \mathcal{H}(r-2, q^2) \mid + \mid \mathcal{I}_{r-2} \mid$.

In increasing order we get the following intersection numbers n_i with $i = 1, \ldots, 5$:

1. (C1) gives $n_1 = q^2 \frac{(q^{2(r-2)}-1)}{q^2-1} + q^{r-1} + 1$;
2. (C6) gives $n_2 = q^{2r-3} - q^{r-2} + q^{r-3} + \frac{q^{2(r-2)}-1}{q^2-1}$;
3. (C2) and (C5) yield $n_3 = q^{2r-3} + \frac{q^{2(r-2)}-q^2}{q^2-1} + 1$;
4. (C7) provides $n_4 = q^{2r-3} + q^{r-1} - q^{r-2} + q^{r-3} + \frac{q^{2(r-2)}-1}{q^2-1}$;
5. (C3) and (C4) provide $n_5 = q^{2r-3} + q^{r-1} + \frac{q^{2(r-2)}-q^2}{q^2-1} + 1$.

Now suppose that $r \geq 4$ is even. In this case $\mathcal{B}_\infty$ is a cone with vertex the point $P_\infty(0, 0, \ldots, 0, 1)$ and basis a parabolic quadric $\mathcal{P}_{r-2}$ in an $r-2$-dimensional projective space contained in Σ_∞ and it contains $q^2[(q^{2(r-2)} - 1)/(q^2 - 1)] + 1$ points over $\mathrm{GF}(q^2)$. As $\mathcal{B} \cap AG(r, q^2)$ contains q^{2r-1} affine points, we get

$$\mid \mathcal{B} \mid = q^{2r-1} + q^2[(q^{2(r-2)} - 1)/(q^2 - 1)] + 1.$$

We observe that a generic hyperplane of Σ which does not pass through P_∞ meets $\mathcal{B}_\infty$ in a parabolic quadric $\mathcal{P}_{r-2}$ of an $r-2$-dimensional projective space in Σ_∞. On the other hand, if Σ contains P_∞ then it meets $\mathcal{B}_\infty$ in a cone with vertex P_∞ and basis either a cone $\Pi_0'\mathcal{P}_{r-4}$, or a hyperbolic quadric $\mathcal{I}_{r-3}$, or an elliptic quadric $\mathcal{E}_{r-3}$. Thus, the possible values of $\mid \Sigma \cap \mathcal{B} \mid$, for any hyperplane Σ of $\mathrm{PG}(r, q^2)$, are:

(C1) $\mid \mathcal{B}_\infty \mid$;
(C2) $\mid \mathcal{H}(r-1,q^2) \mid - \mid P_\infty \mathcal{H}(r-3,q^2) \mid + q^2 \mid \Pi_0' \mathcal{P}_{r-4} \mid + 1$;
(C3) $\mid \mathcal{H}(r-1,q^2) \mid - \mid P_\infty \mathcal{H}(r-3,q^2) \mid + q^2 \mid \mathcal{E}_{r-3} \mid + 1$;
(C4) $\mid \mathcal{H}(r-1,q^2) \mid - \mid P_\infty \mathcal{H}(r-3,q^2) \mid + q^2 \mid \mathcal{I}_{r-3} \mid + 1$;
(C5) $\mid \Pi_0 \mathcal{H}(r-2,q^2) \mid - \mid P_\infty(\Pi_0 \mathcal{H}(r-4,q^2)) \mid + q^2 \mid \Pi_0' \mathcal{P}_{r-4} \mid + 1$;
(C6) $\mid \Pi_0 \mathcal{H}(r-2,q^2) \mid - \mid P_\infty(\Pi_0 \mathcal{H}(r-4,q^2)) \mid + q^2 \mid \mathcal{E}_{r-3} \mid + 1$;
(C7) $\mid \Pi_0 \mathcal{H}(r-2,q^2) \mid - \mid P_\infty(\Pi_0 \mathcal{H}(r-4,q^2)) \mid + q^2 \mid \mathcal{I}_{r-3} \mid + 1$;
(C8) $\mid \mathcal{H}(r-1,q^2) \mid - \mid \mathcal{H}(r-2,q^2) \mid + \mid \mathcal{P}_{r-2} \mid$;
(C9) $\mid \Pi_0 \mathcal{H}(r-2,q^2) \mid - \mid \mathcal{H}(r-2,q^2) \mid + \mid \mathcal{P}_{r-2} \mid$.

In increasing order, we obtain as the possible intersection numbers of $\mathcal{B}$ with respect to the hyperplanes the following

(C1) gives $n_1 = q^2 \frac{(q^{2(r-2)}-1)}{q^2-1} + 1$;
(C9) gives $n_2 = q^{2r-3} - q^{r-1} + q^{r-2} + \frac{q^{2(r-2)}-1}{q^2-1}$;
(C3) and (C6) yield $n_3 = q^{2r-3} + \frac{q^{2(r-2)}-q^2}{q^2-1} - q^{r-2} + 1$;
(C2) and (C5) provide $n_4 = q^{2r-3} + \frac{(q^{2(r-2)}-q^2)}{q^2-1} + 1$;
(C4) (C7) and (C8) provide $n_5 = q^{2r-3} + \frac{q^{2(r-2)}-q^2}{q^2-1} + q^{r-2} + 1$.

We summarize our results in the following theorem.

Theorem 3 *Suppose q to be an odd prime power. Then the hypersurface $\mathcal{B}$ of $\mathrm{PG}(r,q^2)$, $r \geq 3$, with equation (3) contains $q^{2r-1} + q^{r-1} + (q^{2(r-1)} - q^2)/(q^2-1) + 1$ points if r is odd or $q^{2r-1} + (q^{2(r-1)} - q^2)/(q^2-1) + 1$ points if r is even. Furthermore its possible intersection sizes with hyperplanes are:*

- *for r odd:*

$$n_1 = q^2 \frac{(q^{2(r-2)}-1)}{q^2-1} + q^{r-1} + 1, \qquad n_2 = q^{2r-3} - q^{r-2} + q^{r-3} + \frac{q^{2(r-2)}-1}{q^2-1},$$
$$n_3 = q^{2r-3} + \frac{q^{2(r-2)}-q^2}{q^2-1} + 1,$$
$$n_4 = q^{2r-3} + q^{r-1} - q^{r-2} + q^{r-3} + \frac{q^{2(r-2)}-1}{q^2-1},$$
$$n_5 = q^{2r-3} + q^{r-1} + \frac{q^{2(r-2)}-q^2}{q^2-1} + 1;$$

- *for r even:*

$$n_1 = q^2 \frac{(q^{2(r-2)}-1)}{q^2-1} + 1, \qquad n_2 = q^{2r-3} - q^{r-1} + q^{r-2} + \frac{q^{2(r-2)}-1}{q^2-1},$$
$$n_3 = q^{2r-3} + \frac{q^{2(r-2)}-q^2}{q^2-1} - q^{r-2} + 1, \qquad n_4 = q^{2r-3} + \frac{(q^{2(r-2)}-q^2)}{q^2-1} + 1,$$
$$n_5 = q^{2r-3} + \frac{q^{2(r-2)}-q^2}{q^2-1} + q^{r-2} + 1.$$

4.2 Case $r \geq 3$ and q even

In this case, the intersection between the algebraic variety $\mathcal{B}$ and Σ_∞ is the degenerate quadric $\mathcal{B}_\infty$ which consists of the single hyperplane of Σ_∞: $x_1 + \cdots + x_{r-1} = 0$. Therefore the size of $\mathcal{B}$ is:

$$q^{2r-1} + q^{2(r-2)} + \cdots + q^2 + 1,$$

and the possible intersection numbers of $\mathcal{B}$ with respect to hyperplanes of $\mathrm{PG}(r, q^2)$ are

(C1) $\mid \mathcal{B}_\infty \mid$;
(C2) $\mid \mathcal{H}(r-1, q^2) \mid - \mid P_\infty \mathcal{H}(r-3, q^2) \mid + \mid \Pi_{r-2} \mid$;
(C3) $\mid \mathcal{H}(r-1, q^2) \mid - \mid P_\infty \mathcal{H}(r-3, q^2) \mid + \mid \Pi_{r-3} \mid$;
(C4) $\mid \Pi_0 \mathcal{H}(r-2, q^2) \mid - \mid P_\infty (\Pi_0 \mathcal{H}(r-4, q^2) \mid + \mid \Pi_{r-2} \mid$;
(C5) $\mid \Pi_0 \mathcal{H}(r-2, q^2) \mid - \mid P_\infty (\Pi_0 \mathcal{H}(r-4, q^2) \mid + \mid \Pi_{r-3} \mid$;
(C6) $\mid \mathcal{H}(r-1, q^2) \mid - \mid \mathcal{H}(r-2, q^2) \mid + \mid \Pi_{r-3} \mid$;
(C7) $\mid \Pi_0 \mathcal{H}(r-2, q^2) \mid - \mid \mathcal{H}(r-2, q^2) \mid + \mid \Pi_{r-3} \mid$.

So, for r odd we obtain the following weights:

- (C1) gives $n_1 = \frac{q^{2(r-1)}-1}{q^2-1}$;
- (C6) gives $n_2 = q^{2r-3} - q^{r-2} + \frac{q^{2(r-2)}-1}{q^2-1}$;
- (C3) and (C5) provide $n_3 = q^{2r-3} + \frac{q^{2(r-2)}-1}{q^2-1}$;
- (C7) yields $n_4 = q^{2r-3} + q^{r-1} - q^{r-2} + \frac{q^{2(r-2)}-1}{q^2-1}$;
- (C2) and (C4) provide $n_5 = q^{2r-3} + \frac{q^{2(r-1)}-1}{q^2-1}$.

For r even we obtain

- (C1) gives $n_1 = \frac{q^{2(r-1)}-1}{q^2-1}$;
- (C7) gives $n_2 = q^{2r-3} - q^{r-1} + q^{r-2} + \frac{q^{2(r-2)}-1}{q^2-1}$;
- (C3) and (C5) provide $n_3 = q^{2r-3} + \frac{q^{2(r-2)}-1}{q^2-1}$;
- (C6) yields $n_4 = q^{2r-3} + q^{r-2} + \frac{q^{2(r-2)}-1}{q^2-1}$;
- (C2) and (C4) provide $n_5 = q^{2r-3} + \frac{q^{2(r-1)}-1}{q^2-1}$.

Theorem 4 *Suppose q to be even and $r \geq 3$. Then the hypersurface $\mathcal{B}$ of Equation (3) has $q^{2r-1} + q^{2(r-2)} + \cdots + q^2 + 1$ points in $\mathrm{PG}(r, q^2)$ and the following intersection sizes with respect to hyperplanes:*

- *for r odd:*

$$n_1 = \frac{q^{2(r-1)} - 1}{q^2 - 1}, \qquad n_2 = q^{2r-3} - q^{r-2} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_3 = q^{2r-3} + \frac{q^{2(r-2)} - 1}{q^2 - 1}, \qquad n_4 = q^{2r-3} + q^{r-1} - q^{r-2} + \frac{q^{2(r-2)} - 1}{q^2 - 1},$$

$$n_5 = q^{2r-3} + \frac{q^{2(r-1)} - 1}{q^2 - 1};$$

- *for r even:*

$$n_1 = \frac{q^{2(r-1)}-1}{q^2-1}, \qquad n_2 = q^{2r-3} - q^{r-1} + q^{r-2} + \frac{q^{2(r-2)}-1}{q^2-1},$$

$$n_3 = q^{2r-3} + \frac{q^{2(r-2)}-1}{q^2-1}, \qquad n_4 = q^{2r-3} + q^{r-2} + \frac{q^{2(r-2)}-1}{q^2-1},$$

$$n_5 = q^{2r-3} + \frac{q^{2(r-1)}-1}{q^2-1}.$$

4.3 Line sections of $\mathcal{B}$ in PG(r, q^2)

Our aim is to provide the spectrum of all possible intersection numbers between $\mathcal{B}$ and a line of PG(r, q^2). We are going to prove the following theorem.

Theorem 5 *Let ℓ be a line of* PG(r, q^2)*. Then, the possible sizes for $\ell \cap \mathcal{B}$ are as follows*

$$0, 1, 2, q-1, q, q+1, q+2, 2q-1, 2q, q^2+1$$

Proof Let us assume q to be odd and consider a line ℓ of PG(r, q^2). If ℓ is contained in Σ_∞ then the possible sizes of $\ell \cap \mathcal{B}$ are 0, 1,2 or q^2+1. Now suppose that $\ell \nsubseteq \Sigma_\infty$ and $|\ \ell \cap \mathcal{B}\ | \geq 1$. From [1], it can be directly seen that the collineation group of $\mathcal{B}$ acts transitively on its affine points. Thus, we can assume that ℓ passes through the origin of the fixed reference system. We have to study the following system

$$\left\{ \begin{aligned} & x_r^q - x_r + \alpha^q(x_1^{2q} + \cdots + x_{r-1}^{2q}) - \alpha(x_1^2 + \cdots + x_{r-1}^2) \\ & \quad = (\beta^q - \beta)(x_1^{q+1} + \cdots + x_{r-1}^{q+1}), \\ & x_1 = m_1 t \\ & x_2 = m_2 t \\ & \vdots \\ & x_r = m_r t \end{aligned} \right. \tag{4}$$

where t ranges over GF(q^2). First we consider the case in which $m_r \neq 0$ and hence we can assume $m_r = 1$. In order to study System (4), choose a primitive element γ of GF(q^2) and let $\varepsilon = \gamma^{(q+1)/2}$. We now regard GF$(q^2)$ as a vector space over GF(q) with a fixed basis $\{1, \varepsilon\}$ and write the elements in GF(q^2) as linear combinations with respect to this basis, that is, $x_i = x_i^{(0)} + x_i^{(1)}\varepsilon$. Then, $\varepsilon^q = -\varepsilon$ and ε^2 is a primitive element of GF(q). With this choice of ε, setting

$$u = m_1^{(0)} m_1^{(1)} + \cdots + m_{r-1}^{(0)} m_{r-1}^{(1)},$$

$$v = \left(m_1^{(0)}\right)^2 + \cdots + \left(m_{r-1}^{(0)}\right)^2 \quad \text{and} \quad z = \left(m_1^{(1)}\right)^2 + \cdots + \left(m_{r-1}^{(1)}\right)^2.$$

Equation (4) gives

$$\begin{aligned} & [2\alpha_0 u + \alpha_1(\varepsilon^2 z + v) + \beta_1(\varepsilon^2 z - v)]t_0^2 + \varepsilon^2[2\alpha_0 u + \alpha_1(v + \varepsilon^2 z) + \beta_1(v - \varepsilon^2 z)]t_1^2 \\ & \quad + 2[\alpha_0(\varepsilon^2 z + v) + 2\alpha_1 \varepsilon^2 u]t_0 t_1 + t_1 = 0 \end{aligned} \tag{5}$$

The solutions (t_0, t_1) of (5) can be viewed as the affine points of the (possibly degenerate) conic Γ of $\mathrm{PG}(2, q)$ associated to the symmetric 3×3 matrix

$$A = \begin{pmatrix} 2\alpha_0 u + \alpha_1(\varepsilon^2 z + v) + \beta_1(\varepsilon^2 z - v) & \alpha_0(\varepsilon^2 z + v) + 2\alpha_1\varepsilon^2 u & 0 \\ \alpha_0(\varepsilon^2 z + v) + 2\alpha_1\varepsilon^2 u & \varepsilon^2[2\alpha_0 u + \alpha_1(v + \varepsilon^2 z) + \beta_1(v - \varepsilon^2 z)] & 1/2 \\ 0 & 1/2 & 0 \end{pmatrix}.$$

The number of affine points of Γ equals the number of points in $\mathrm{AG}(3, q^2)$ which lie in $\mathcal{B} \cap \ell$. Observe that $\mathrm{rank}(A) \geq 2$. Let us first suppose $\det(A) \neq 0$. In this case Γ is a non-degenerate conic in $\mathrm{PG}(2, q)$ and hence has either $q - 1$ or q or $q + 1$ affine points. If $\mathrm{rank}(A) = 2$ then Γ is the union of two distinct lines either defined over $\mathrm{GF}(q)$ or defined over $\mathrm{GF}(q^2)$ and conjugate to each other. This means that the number of affine points of Γ is either $2q - 1$ or $2q$ or 1. Thus if $\ell \cap \mathcal{B}_\infty = \emptyset$ then $| \ell \cap \mathcal{B} | \in \{1, q - 1, q, q + 1, 2q - 1, 2q\}$

Now suppose that ℓ meets $\mathcal{B}_\infty$. The point at infinity of ℓ is $R = (0, m_1, m_2 \ldots, m_r)$ and R is also a point of $\mathcal{B}_\infty$ if and only if

$$m_1^2 + \cdots + m_{r-1}^2 = 0,$$

that is, $\sum_{i=1}^{r-1}(m_i^{(0)} + \varepsilon m_i^{(1)})^2 = 0$. This can be rewritten as

$$\sum_{i=1}^{r-1}(m_i^{(0)})^2 + \varepsilon^2(m_i^{(1)})^2 + 2\varepsilon \sum_{i=1}^{r-1} m_i^{(0)} m_i^{(1)} = 0,$$

and hence we get

$$\begin{cases} \sum_{i=1}^{r-1}(m_i^{(0)})^2 + \varepsilon^2(m_i^{(1)})^2 = 0 \\ \sum_{i=1}^{r-1} m_i^{(0)} m_i^{(1)} = 0. \end{cases}$$

Thus if $R \in \mathcal{B}_\infty$ then $v + \varepsilon^2 z = 0$ and $u = 0$. In this case A becomes

$$A = \begin{pmatrix} \beta_1(\varepsilon^2 z - v) & 0 & 0 \\ 0 & \varepsilon^2\beta_1(v - \varepsilon^2 z) & 1/2 \\ 0 & 1/2 & 0 \end{pmatrix}.$$

If $\det(A) \neq 0$ then Γ is an ellipse as ε^2 is a non–square of $\mathrm{GF}(q)$. In the case in which $\mathrm{rank}(A) = 2$, then we get $u = v = z = 0$ and Γ consists of q affine points. Thus, $| \ell \cap \mathcal{B} | \in \{q + 1, q + 2\}$.

Now suppose that $m_r = 0$. In this case the number of points in $\mathrm{AG}(3, q^2)$ which lie in $\mathcal{B} \cap \ell$ equals the number of affine points of the degenerate conic Γ with associated matrix

$$A = \begin{pmatrix} 2\alpha_0 u + \alpha_1(\varepsilon^2 z + v) + \beta_1(\varepsilon^2 z - v) & \alpha_0(\varepsilon^2 z + v) + 2\alpha_1\varepsilon^2 u & 0 \\ \alpha_0(\varepsilon^2 z + v) + 2\alpha_1\varepsilon^2 u & \varepsilon^2[2\alpha_0 u + \alpha_1(v + \varepsilon^2 z) + \beta_1(v - \varepsilon^2 z)] & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

If $\mathrm{rank}(A) = 2$ then Γ has either 1 or $2q - 1$ or $2q$ points. Otherwise, $\mathrm{rank}(A) = 1$ and Γ consists of q points, or the matrix A is the null matrix, namely Γ is the entire affine plane and $\ell \subset \mathcal{B}$. Furthermore, in the case in which $| \ell \cap \mathcal{B}_\infty | = 1$, it is easy to see that $\Gamma \cap \mathrm{AG}(2, q^2)$ consists of a single point over $\mathrm{GF}(q)$ or it is the entire plane. Hence $| \ell \cap \mathcal{B} | \in \{1, 2, q, 2q-1, 2q, q^2+1\}$ and our theorem follows for q odd.

Let us consider the case of q even. As $q > 2$, we can fix a basis for $\mathrm{GF}(q^2)$ over $\mathrm{GF}(q)$ as $\{1, \epsilon\}$, with $\epsilon \in \mathrm{GF}(q^2) \setminus \mathrm{GF}(q)$ such that $\epsilon^2 + \epsilon + \nu = 0$, for some $\nu \in \mathrm{GF}(q) \setminus \{1\}$, with $\mathrm{Tr}_q(\nu) = 1$. Then $\epsilon^{2q} + \epsilon^q + \nu = 0$ and hence $(\epsilon^q + \epsilon)^2 + (\epsilon^q + \epsilon) = 0$, leading to $\epsilon^q + \epsilon + 1 = 0$. With this choice of ε, setting as before $u = m_1^{(0)} m_1^{(1)} + \cdots + m_{r-1}^{(0)} m_{r-1}^{(1)}$, $v = (m_1^{(0)})^2 + \cdots + (m_{r-1}^{(0)})^2$ and $z = (m_1^{(1)})^2 + \cdots + (m_{r-1}^{(1)})^2$, (4) gives

$$\begin{aligned} &[\beta_1(u + v + \nu z) + \alpha_1(v + z + \nu z) + \alpha_0 z]\, t_0^2 \\ &\quad + [(\beta_1 \nu(u + v + \nu z) + \alpha_1 \nu(v + z + \nu z) + (\alpha_1 + \alpha_0)(v + z)]\, t_1^2 \\ &\quad + \beta_1(u + v + \nu z) t_0 t_1 + t_1 = 0. \end{aligned} \tag{6}$$

which can be viewed again as the equation of a conic Γ of $\mathrm{AG}(2, q^2)$.

It is straightforward to see that $| \Gamma \cap \mathrm{AG}(2, q^2) | \in \{1, q-1, q, q+1, 2q-1, 2q, q^2\}$. Arguing as in the q odd case, the proof is completed.

□

5 Codes with 5 weights

We are going to determine the parameters of the projective code generated from the hypersurface $\mathcal{B}$ of Equation (3) and in particular its weight enumerator for $r = 3$ and q odd.

Theorem 6 *Let q be an odd prime power. Then, the points of $\mathcal{B}$ in $\mathrm{PG}(r, q^2)$, $r > 3$ determine a q-divisible minimal projective code $\mathcal{C}(\mathcal{B})$ of length $N = q^{2r-1} + q^{r-1} + (q^{2(r-1)} - q^2)/(q^2 - 1) + 1$ for r odd, or $N = q^{2r-1} + (q^{2(r-1)} - q^2)/(q^2 - 1) + 1$ for r even, dimension $r + 1$ and non-zero weights:*

- *for r odd:*

$$\begin{aligned} &w_5 = q^{2r-1} - q^{2r-3} + q^{2(r-2)}, \qquad w_4 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-2} - q^{r-3}, \\ &w_3 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-1}, \\ &w_2 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-1} + q^{r-2} - q^{r-3}, \qquad w_1 = q^{2r-1}; \end{aligned}$$

- *for r even:*

$$\begin{aligned} &w_5 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} - q^{r-2}, \qquad w_4 = q^{2r-1} - q^{2r-3} + q^{2(r-2)}, \\ &w_3 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-2}, \\ &w_2 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-1} - q^{r-2}, \qquad w_1 = q^{2r-1}. \end{aligned}$$

Proof Since $w_i = N - n_i$ where the n_i's are the intersection numbers of $\mathcal{B}$ with respect to the hyperplanes of $\mathrm{PG}(r, q^2)$, from Theorem (3) we have just to prove that $\mathcal{C}(\mathcal{B})$ is a minimal code. We restrict ourselves to the case r odd. Under this hypothesis the maximal weight of $\mathcal{C}(\mathcal{B})$ is $w_1 = q^{2r-1}$ whereas the minimal one is $w_5 = q^{2r-1} - q^{2r-3} + q^{2(r-2)}$. We observe that $\frac{w_5}{w_1} > \frac{q^2-1}{q^2}$, that is, Condition (1) is satisfied and hence $C(\mathcal{B})$ is a minimal code. □

From Theorem (4) we obtain the following.

Theorem 7 *Let q be an even prime power. Then, the points of $\mathcal{B}$ in $PG(r, q^2)$, $r \geq 3$ determine a q-divisible projective code $\mathcal{C}(\mathcal{B})$ of length $N = q^{2r-1} + q^{2(r-2)} + q^{2(r-3)} + \cdots + q^2 + 1$, dimension $r + 1$ and non-zero weights:*

- *for r odd:*

$$\begin{aligned}&w_5 = q^{2r-1} - q^{2r-3}, \quad w_4 = q^{2r-1} - q^{2r-3} + q^{2r-4} - q^{r-1} + q^{r-2},\\ &w_3 = q^{2r-1} - q^{2r-3} + q^{2(r-2)},\\ &w_2 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-2}, \quad w_1 = q^{2r-1};\end{aligned}$$

- *for r even:*

$$\begin{aligned}&w_5 = q^{2r-1} - q^{2r-3}, \quad w_4 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} - q^{r-2},\\ &w_3 = q^{2r-1} - q^{2r-3} + q^{2(r-2)},\\ &w_2 = q^{2r-1} - q^{2r-3} + q^{2(r-2)} + q^{r-1} - q^{r-2}, \quad w_1 = q^{2r-1}.\end{aligned}$$

Remark 3 For q even, the code $\mathcal{C}(\mathcal{B})$ is not a minimal code, as the support of the words of weight w_5 is contained in the support of words of weight w_1. This is consistent with Theorem 1, as $\langle\mathcal{B}_\infty\rangle = \mathcal{B}_\infty \neq \Sigma_\infty$ in this case. So, the $q^2 - 1$ words of weight $w_1 = q^{2r-1}$ are exactly those which are not minimal.

Let A_j denote the number of codewords of $\mathcal{C}(\mathcal{B})$ of weight j.

Proposition 8 *The points of $\mathcal{B}$ in* PG$(3, q^2)$*, with q an odd prime power, determine a minimal projective code $\mathcal{C}(\mathcal{B})$ of length $N = q^5 + 2q^2 + 1$, non-zero weights:*

$$\begin{aligned}&w_1 = q^5, \quad w_2 = q^5 - q^3 + 2q^2 + q - 1, \quad w_3 = q^5 - q^3 + 2q^2,\\ &w_4 = q^5 - q^3 + q^2 + q - 1, \quad w_5 = q^5 - q^3 + q^2,\end{aligned}$$

and weight enumerator $w(x) := \sum_i A_i x^i$, where

$$A_0 = 1,\ A_{w_1} = q^2 - 1,\ A_{w_2} = (q^6 - q^5 + q^3)(q^2 - 1),\ A_{w_3} = (q^4 - q^2)(q^2 - 1),$$

$$A_{w_4} = (q^5 - q^3)(q^2 - 1),\ A_{w_5} = 2q^2(q^2 - 1)$$

and all of the remaining A_i's are 0.

Proof As $w_i = N - n_i$, where n_i's are the intersection numbers of $\mathcal{B}$ with respect to the planes, the first part of our theorem follows from Theorem (3) for $r = 3$ and from the fact that $w_5/w_1 > (q^2 - 1)/q^2$. We are going to compute the weight enumerator of the code. We observe that Σ_∞ is the only hyperplane meeting $\mathcal{B}$ in $2q^2 + 1$ points and this means $A_{w_1} = q^2 - 1$. Also, through the point $P_\infty = (0, 0, 0, 1)$ there pass $2q^2$ planes meeting $\Sigma_\infty \cap \mathcal{B}$ in one line and $q^4 - q^2$ planes meeting $\Sigma_\infty \cap \mathcal{B}$ just at the point P_∞. Hence, $A_{w_5} = 2q^2(q^2 - 1)$ and $A_{w_3} = (q^4 - q^2)(q^2 - 1)$.

Finally, we recall that $\mathcal{H} = (\mathcal{B} \cap AG(3, q^2)) \cup \mathcal{F}$ is a quasi-Hermitian variety of PG$(3, q^2)$. Let us call a plane intersecting $\mathcal{H}$ in i points an (i)-*plane* of $\mathcal{H}$. Using the following properties of $\mathcal{H}$:

- The number of $(q^3 + q^2 + 1)$-planes is $q^5 + q^2 + 1$,
- The number of $(q^3 + 1)$-planes is $q^6 - q^5 + q^4$,
- P_∞ lies on $q^4 - q^3$ $(q^3 + 1)$-planes and on $q^3 + q^2 + 1$ $(q^3 + q^2 + 1)$-planes of $\mathcal{H}$,

we get $A_{w_4} = (q^5 - q^3)(q^2 - 1)$ and $A_{w_2} = (q^6 - q^5 + q^3)(q^2 - 1)$. □

Remark 4 Theorems 5 and 6 yield that the higher weights $d_1(\mathcal{C}(\mathcal{B}))$ and $d_{r-1}(\mathcal{C}(\mathcal{B}))$ are as follows:

- for q odd:
  - if r is odd: $d_1(\mathcal{C}(\mathcal{B})) = q^{2r-1} - q^{2r-3} + q^{2(r-2)}$, $d_{r-1}(\mathcal{C}(\mathcal{B})) = q^{2r-1} + q^2 \frac{(q^{2(r-2)}-1)}{q^2-1} + q^{r-1} - q^2$;
  - if r is even: $d_1(\mathcal{C}(\mathcal{B})) = q^{2r-1} - q^{2r-3} + q^{2(r-2)} - q^{r-2}$, $d_{r-1}(\mathcal{C}(\mathcal{B})) = q^{2r-1} + q^2 \frac{(q^{2(r-2)}-1)}{q^2-1} - q^2$;
- for q even and any r: $d_1(\mathcal{C}(\mathcal{B})) = q^{2r-1} - q^{2r-3}$, $d_{r-1}(\mathcal{C}(\mathcal{B})) = q^{2r-1} + q^{2(r-2)} + \cdots + q^4$.

We leave to a future work to determine the higher weights $d_k(\mathcal{C}(\mathcal{B}))$ for all $1 < k < r-1$.

6 Secret sharing schemes from hypersurfaces

In this section we recall a method for constructing SSS's based on linear codes and then we present a class of SSS's using the hypersurfaces introduced in Sect. 4.

Let C be an $[n, k, d]_q$-linear code. In the SSS $\mathfrak{S}(C)$ based on C, the secret is an element of $\mathrm{GF}(q)$, and $n-1$ parties $P_1, P_2, \dots, P_{n-1}$ as well as a trusted third party are involved. To compute the shares with respect to a secret s, the trusted third party randomly chooses a vector $\mathbf{u} = (u_0, \dots, u_{k-1}) \in \mathrm{GF}(q)^k$ such that $s = \mathbf{u}g_0$ and $G = (g_0, g_1, \dots g_{n-1})$ is a generator matrix of C. There are altogether q^{k-1} such vectors $\mathbf{u} \in \mathrm{GF}(\mathbf{q})^{\mathbf{k}}$. The third party then treats $\mathbf{u}$ as an information vector and computes the corresponding codeword $t = (t_0, t_1, \dots, t_{n-1}) = \mathbf{u}G$. He then gives t_i to party P_i as share for each $i \geq 1$. Note that $t_0 = \mathbf{u}g_0 = s$. It is easily seen that a set of shares $\{t_{i_1}, t_{i_2}, \dots, t_{i_m}\}$ determines the secret if and only if g_0 is a linear combination of $g_{i_1}, \dots, g_{i_m}$. The following properties hold.

Proposition 9 [10] *Let G be a generator matrix of an $[n, k; q]$-code C. In the SSS based on C, a set of shares $\{t_{i_1}, t_{i_2}, \dots, t_{i_m}\}$ determines the secret if and only if there exists a codeword*

$$\mathbf{c} = (1, 0, \dots, 0, c_{i_1}, 0, \dots, 0, c_{i_m}, 0, \dots, 0)$$

in the dual code $C^\perp$ where $c_{i_j} \neq 0$ for at least one j, $1 \leq i_1 < \cdots < i_m \leq n-1$ and $1 \leq m \leq n-1$. If there is a codeword like $\mathbf{c}$ in $C^\perp$, then the vector

$$g_0 = \sum_{j=1,\dots,m} x_j g_{i_j}$$

where $x_j \in \mathrm{GF}(q)$ for $1 \leq j \leq m$. Then the secret s is recovered by computing

$$s = \sum_{j=1,\dots,m} x_j t_{i_j}.$$

If a set of participants can recover the secret by combining their shares, then any group of participants containing this set can also recover the secret.

Definition 3 A set of participants is called a *minimal access set* if they can recover the secret by combining their shares and none of its proper subsets can do so. Here, a proper subset has fewer members than this set. The *access structure* $\mathfrak{A}(\mathcal{C})$ of the SSS $\mathfrak{S}(\mathcal{C})$ is the set of its minimal access sets.

Proposition 10 [10] *Let C be an $[n, k; q]$-code, and let $G = (g_0, g_1, \ldots, g_{n-1})$ be its generator matrix. If each nonzero codeword of C is a minimal word, then in the SSS based on $C^\perp$, there are altogether q^{k-1} minimal access sets. In addition, we have the following:*

1. *If g_i is a multiple of g_0, $1 \le i \le n-1$, then participant P_i must be in every minimal access set. Such a participant is called a* dictatorial *participant.*
2. *If g_i is not a multiple of g_0, $1 \le i \le n-1$, then participant P_i must be in $(q-1)q^{k-2}$ out of q^{k-1} minimal access sets.*

We refer the reader to [10] for the actual construction of the SSS.

In this section we shall consider the access structures of SSS's arising from codes constructed from hypersurfaces. These access structures turn out to reflect the geometry of the hypersurface and they also afford a compact description in terms of their automorphism groups.

Proposition 11 *Let C and C' be two equivalent $[n, k, d]$-codes over* $\mathrm{GF}(q)$ *with generator matrices G and G' with $G' = RGPD$ where R is a $k \times k$ invertible matrix, P is an $n \times n$ permutation matrix and D is an invertible $n \times n$ diagonal matrix. Suppose that the permutation $\sigma : \{0, \ldots, n-1\} \to \{0, \ldots, n-1\}$, induced by P, fixes 0. Then there is a bijection between the shares of the SSS's $\mathfrak{S}(C)$ and $\mathfrak{S}(C')$ as well as between the corresponding access structures $\mathfrak{A}(C)$ and $\mathfrak{A}(C')$.*

In light of the above proposition, given an hypersurface $\mathcal{V}$ of $\mathrm{PG}(V)$ and a fixed point $P_0 \in \mathcal{V}$, we can construct many equivalent $[n, k, d]$-linear codes with a generator matrix having P_0 as its first column.

So, we propose the following notation. Let $\mathcal{V}$ be an hypersurface, and let P_1 be a chosen point of $\mathcal{V}$; let $C = \mathcal{C}(\mathcal{V}; P_0)$ be a projective code arising from $\mathcal{V}$, with a generator matrix having P_0 as its first column. We denote the SSS's based on C by the symbol $\mathfrak{S}(\mathcal{V}; P_0)$ and the SSS's based on $C^\perp$ by $\mathfrak{S}(\mathcal{V}^\perp; P_0)$.

Remark 5 Suppose $\mathcal{V} \subseteq \mathrm{PG}(V)$. The elements of the access structure $\mathfrak{A}(\mathcal{V}^\perp; P_0)$ correspond to the support of the subsets $(\mathcal{V} \setminus \{P_0\}) \setminus \Pi$ of $\mathcal{V}$ as Π varies among the hyperplanes of $\mathrm{PG}(V)$ not containing the point P_0. In particular, we can describe $\mathfrak{A}(\mathcal{V}^\perp; P_0)$ directly, without explicit mention of the projective code $C^\perp$ induced by $\mathcal{V}$.

Definition 4 We say that two access structures $\mathfrak{A}$ and $\mathfrak{A}'$ associated to SSS's $\mathfrak{S}$ and $\mathfrak{S}'$ with set of participants X and X', respectively, are *equivalent* if there is a bijection $\theta : X \to X'$ such that $\mathfrak{A}' = \{S^\theta : S \in \mathfrak{A}\}$.

Definition 5 Let $\mathfrak{S}$ be a SSS with corresponding access structure $\mathfrak{A}$ and set of participants X. We say that $\gamma \in \mathrm{Sym}(X)$ is an *automorphism* of $\mathfrak{A}$ if, for any $T \in \mathfrak{A}$, we have $T^\gamma := \{\gamma(t) : t \in T\} \in \mathfrak{A}$. Given a subgroup Γ of $\mathrm{Sym}(X)$ and some elements $S_1, \ldots, S_t \in \mathfrak{A}$, we say that $\mathfrak{A}$ is a Γ-*development* of the *starters* $S_1, \ldots, S_t$ if

$$\mathfrak{A} = \{S_i^\gamma : \gamma \in \Gamma, i \in 1, \ldots, t\}.$$

Proposition 12 *Let $\mathcal{V} = \{P_0, \ldots, P_{n-1}\}$ be an algebraic variety of* $\mathrm{PG}(V)$. *Denote by $\mathfrak{A}(\mathcal{V}^\perp; P_0)$ the access structure of the SSS $\mathfrak{S}(\mathcal{V}; P_0)$. Let γ be a collineation of* $\mathrm{PG}(V)$ *fixing P_0 and such that $\gamma(\mathcal{V}) = \mathcal{V}$. Then $\hat{\gamma} \in \mathrm{Sym}(1, \ldots, n-1)$, where*

$$\hat{\gamma}(i) = j \Leftrightarrow \gamma(P_i) = P_j$$

acts as an automorphism of $\mathfrak{A}(\mathcal{V}^\perp; P_0)$.

Proof The elements of $\mathfrak{A}(\mathcal{V}^{\perp}; P_0)$ correspond to the support of the complement of the intersection of $\mathcal{V}$ with the hyperplanes Σ of $\mathrm{PG}(V)$ for which $P_0 \notin \Sigma$. Since γ preserves $\mathcal{V}$ and fixes P_0, it also acts on the hyperplanes of $\mathrm{PG}(V)$ not through P_0; as such $\hat{\gamma}$ acts on the access structures as a permutation group. □

Remark 6 Let $\mathcal{V}$ be a projective hypersurface in $\mathrm{PG}(V)$ and suppose that $\mathcal{V}$ admits a transitive group of automorphisms. Then, for any $P, Q \in \mathcal{V}$ we have that $\mathfrak{A}(\mathcal{V}^{\perp}; P)$ is equivalent to $\mathfrak{A}(\mathcal{V}^{\perp}; Q)$.

We now apply these notions to quasi-Hermitian varieties. Let $\mathcal{B}$ be the hypersurface of Equation (3) and let P_0 be a fixed point of $\mathcal{B}$. Denote by $C = \mathcal{C}(\mathcal{B})$ an associated projective q^2-ary $[N, r+1, d_1]$-code.

Using Proposition 10, we shall first prove that for q odd, the SSS $\mathfrak{S}(\mathcal{B}^{\perp}; P_0)$ based on the dual code of $\mathcal{C}(\mathcal{B})$ is *democratic*, that is, each participant is involved in the same number of minimal access sets, no matter the choice of the point P_0.

Theorem 13 *Let $r \geq 3$ and q be an odd prime power. In the SSS $\mathfrak{S}(\mathcal{B}^{\perp}; P_0) := \mathfrak{S}(C^{\perp})$ based on the dual code $C^{\perp} := \mathcal{C}(\mathcal{B})^{\perp}$, there are altogether q^{2r} minimal access sets and $m = N - 1$ participants where*

- $m = q^{2r-1} + q^{r-1} + \frac{(q^{2(r-1)} - q^2)}{q^2-1}$, *for r odd;*
- $m = q^{2r-1} + \frac{(q^{2(r-1)} - q^2)}{q^2-1}$, *for r even.*

Furthermore, each participant P_i, $\forall i = 1 \ldots m$, is involved in exactly $(q^2-1)q^{2(r-1)}$ out of q^{2r} minimal access sets.

Proof Let G be a generator matrix of $\mathcal{C}(B)$ and let g_i denote the i-column of G. We observe that $\forall i \neq j$ g_i is not a multiple of g_j. Thus, the result follows from Theorem 6 and Propositions 8 and 10. □

Remark 7 We observe that if $\mathcal{H}$ is a quasi-Hermitian variety of $\mathrm{PG}(r, q^2)$, where $r \geq 2$ and q any prime power, then the projective code $\mathcal{C}(\mathcal{H})$ is a two-weight code. From Theorem 2 we also know that $\mathcal{C}(\mathcal{H})$ is minimal. In particular, Property 2 of Proposition 10 applies and the SSS based on the dual of $\mathcal{C}(\mathcal{H})$ turns out to be democratic. For q odd, the SSS associated to the aforementioned code has the same number of minimal access sets as the SSS based on $\mathcal{C}(\mathcal{B})^{\perp}$ but it has a different number of participants, that is $\frac{(q^{r+1}+(-1)^r)(q^r-(-1)^r)}{(q^2-1)} - 1$ for $r > 2$.

We now present a detailed example of access structure with a rich automorphism group by considering the case of Hermitian varieties.

Example 1 Let us consider the Hermitian surface $\mathcal{H}$ of $\mathrm{PG}(3, q^2)$. Then, the projective code $\mathcal{C}(\mathcal{H})$ has parameters $[(q^3+1)(q^2+1), 4, q^5]$ and its weight distribution is given by $A_0 = 1$, $A_{q^5} = (q^4-1)(q^3+1)$ and $A_{q^5+q^2} = q^8 - q^7 - q^4 + q^3 + 1$. Also the automorphism group $\mathrm{PGU}(4, q)$ of $\mathcal{H}$ is transitive on $\mathcal{H}$. So, no matter what point P is chosen in $\mathcal{H}$, all access structures $\mathfrak{A}(\mathcal{H}^{\perp}; P)$ are equivalent. Since $\mathcal{C}(\mathcal{H}^{\perp})$ is a $[(q^3+1)(q^2+1), (q^3+1)(q^2+1)-4, 3]$ code, in the SSS $\mathfrak{S}(\mathcal{H}^{\perp}; P)$ there are q^6 minimal access sets and each participant is involved in $q^6 - q^4$ of them. As seen before, each minimal access set $A \in \mathfrak{A}$ corresponds to a plane π_A not through a fixed point P_1 of $\mathcal{H}$ and, consequently, it has size $\mid \mathcal{H} \setminus \pi_A \mid -1$. In particular, since $\mathcal{H}$ is a two-intersection set with respect to the (hyper)planes, the possible sizes of the minimal access sets are $q^5 - 1$ and $q^5 + q^2 - 1$. Observing that there is exactly one plane through P_1 meeting $\mathcal{H}$ in $q^3 + q^2 + 1$ points, while the remaining $q^4 + q^2$ planes meet $\mathcal{H}$ in $q^3 + 1$ points, it is straightforward to determine how many access structures of each type there are from the weight enumerator of $\mathcal{C}(\mathcal{H})$.

We now describe in further detail the structures for $q = 2$. In this case the size of $\mathfrak{A}$ is 64 and we can easily see that 32 of its minimal access sets have size 31 and the remaining 32 are of size 35. The stabilizer Γ of a point P_1 in $\mathrm{PGU}(4, 2)$ has size 576. It has 5 orbits, say Ω_i (with $i = 1, \dots, 5$), on the hyperplanes of $\mathrm{PG}(3, 4)$ of size respectively 1, 8, 12, 32, and 32, respectively. The union of the first 3 orbits is the set of the hyperplanes through the fixed point P_1; the orbits Ω_4 and Ω_5 correspond to the families of hyperplanes with intersection, respectively, 9 and 13 with $\mathcal{H}$. In turn these correspond to the access structures of size 35 and 31.

Denote by $\{P_1, \dots, P_{45}\}$ the points of $\mathcal{H}$. It can be seen that Γ acts on the P_i's as the permutation group generated by

$$\begin{aligned}
\gamma_1 &:= (2, 44, 38, 3, 42, 40)(4, 10, 28, 7, 13, 30)(5, 22, 15, 8, 24, 12)(6, 34, 20, 9, 32, 18)\\
&\quad (11, 19, 29, 14, 23, 33)(16, 25, 21)(26, 31, 27)(37, 41, 45)(39, 43)\\
\gamma_2 &:= (10, 12, 11)(13, 15, 14)(16, 36, 26)(17, 45, 31)(18, 43, 32)(19, 44, 30)\\
&\quad (20, 39, 34)(21, 37, 35)(22, 38, 33)(23, 42, 28)(24, 40, 29)(25, 41, 27),\\
\gamma_3 &:= (4, 12)(5, 10)(6, 11)(7, 15)(8, 13)(9, 14)(16, 26)(17, 35)(18, 33)(19, 34)\\
&\quad (20, 29)(21, 27)(22, 28)(23, 32)(24, 30)(25, 31).
\end{aligned}$$

By the previous remarks Γ acts in a natural way on the minimal access sets of $\mathfrak{A}$. In particular, $\mathfrak{A}$ is the Γ-development of the following two starters:

$$\begin{aligned}
&S_1 := \{2, 3, 4, 5, 6, 7, 8, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 26,\\
&30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 43, 44, 45\},\\
&S_2 := \{2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 17, 18, 19, 20, 21, 22, 23, 24,\\
&25, 26, 27, 28, 29, 33, 34, 35, 36, 40, 41, 42, 43, 44, 45\}.
\end{aligned}$$

Remark 8 We point out that all access structure arising from Hermitian varieties are the Γ-development of 2 elements under the action of a group Γ which is isomorphic to the stabilizer of an isotropic point in $\mathrm{PGU}(r + 1, q)$.

Acknowledgements This research was carried out within the activities of the GNSAGA - Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni of the Italian INdAM.

References

1. Aguglia A., Cossidente A., Korchmáros G.: On quasi-hermitian varieties. J. Comb. Des. **20**, 433–447 (2012).

2. Alfarano G.N., Borello M., Neri A.: A geometric characterization of minimal codes and their asymptotic performance. Adv. Math. Commun. (To appear).
3. Ashikhmin A., Barg A.: Minimal vectors in linear codes. IEEE Trans. Inf. Theory **44**, 2010–2017 (1998).
4. Bartoli D., Bonini M., Güneş B.: An inductive construction of minimal code. Cryptogr. Commun. **13**, 439–449 (2021).
5. Bonini M., Borello M.: Minimal linear codes arising from blocking sets. J. Algebr. Comb. **53**, 327–341 (2021).
6. Bonini M., Lia S., Timpanella M.: Minimal linear codes from hermitian varieties and quadrics. Appl. Algebra Eng. Commun. Comput., pp. 1–10 (2021).
7. Ding C., Yuan J.: Covering and Secret Sharing with Linear Codes, pp. 11–25. Discret Mathematics and Theoretical Computer Science, Lecture Notes in Computer Science. Springer, Berlin (2003).
8. Ebert G.L.: Hermitian arcs. Rend. Circ. Mat. Palermo **2**(Suppl. 51), 87–105 (1998).
9. Li Z., Xue T., Lai H.: Secret sharing schemes from binary linear codes. Inf. Sci. **180**, 4412–4419 (2010).
10. Massey J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian Workshop on Information Theory, August 22–27, 276–279 (1993).
11. Tang C., Qiu Y., Liao Y., Zhou Z.: Full characterization of minimal linear codes as cutting blocking sets. IEEE Trans. Inf. Theory **67**, 3690–3700 (2021).
12. Tsfasman M.A., Vlăduţ S.G., Nogin D.: Algebraic geometric codes: basic notions. Mathematical Surveys and Monographs American Mathematical Society, Providence **139** (2007).
13. Ward H.N.: Divisible codes-a survey. Serdica Math. J. **27**, 263–278 (2001).
14. Yuan J., Ding C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**, 206–212 (2006).