On the dual code of points and generators on the Hermitian variety $\mathcal{H}(2n+1, q^2)$

M. De Boeck[*] and P. Vandendriessche[*]

January 5, 2016

Abstract

We study the dual linear code of points and generators on a non-singular Hermitian variety $\mathcal{H}(2n+1, q^2)$. We improve the earlier results for $n = 2$, we solve the minimum distance problem for general n, we classify the n smallest types of code words and we characterize all small weight code words as being a linear combination of these n types.

1 Preliminaries

Over the last decades, several types of linear codes arising from finite geometries have been studied. The general concept is as follows: one considers the point set $\mathcal{P}$ of a geometric space or variety $\mathcal{S}$, together with a collection $\mathcal{B}$ of k-dimensional subspaces on $\mathcal{S}$.

Definition 1.1. The incidence matrix $A \in \{0, 1\}^{\mathcal{B} \times \mathcal{P}}$ is the unique matrix such that $H_{b,p} = 1$ if $p \in b$ and $H_{b,p} = 0$ otherwise.

Since 0 and 1 are elements of every field, one can use this matrix to construct subspaces of $\mathbb{F}_p^{\mathcal{P}}$, p prime. There are two common ways to do this:

- by considering the $\mathbb{F}_p$-row span of A, which is usually called *the code generated by the k-spaces of $\mathcal{S}$* and denoted by $C_k(\mathcal{S})$, and

- by considering the $\mathbb{F}_p$-null space of A, which is usually called *the dual code of points and k-spaces of $\mathcal{S}$* and denoted by $C_k(\mathcal{S})^\perp$.

Remark 1.2. A *code word* c of $C_k(\mathcal{S})^\perp$ is an element of the $\mathbb{F}_p$-null space of A, which is equivalent to a mapping from $\mathcal{P}$ to $\mathbb{F}_p$ with the additional property that $\sum_{p \in \pi} c_p = 0$, for all $\pi \in \mathcal{B}$. Hence, code words can be studied as multisets of points such that each k-space on $\mathcal{S}$ contains 0 (mod p) of the points in the multiset.

These codes have primarily been studied for affine and projective spaces (see [1, 3, 7] for an overview of relevant results), and more recently these codes have been investigated for quadrics, Hermitian varieties and generalized quadrangles [2, 8, 9, 10]. In [8], the dual code of points and n-spaces of the Hermitian variety $\mathcal{H}(2n+1, q^2)$ is studied. We will first introduce the basic definitions of Hermitian varieties, then we state the known results on the Hermitian variety code at hand, and finally we will state our main result.

From now on, let $\mathrm{PG}(m, q^2)$ be the m-dimensional projective space over the finite field $\mathbb{F}_{q^2}$. A *non-singular Hermitian variety* is the set of absolute points of a Hermitian polarity, which is

---

defined by a Hermitian matrix and the non-trivial involution $x \mapsto x^q$ of $\mathrm{Aut}(\mathbb{F}_{q^2})$. All non-singular Hermitian varieties are projectively equivalent to the one given by the equation

$$X_0^{q+1} + X_1^{q+1} + \cdots + X_m^{q+1} = 0\,.$$

The projective index of a non-singular Hermitian variety in $\mathrm{PG}(m, q^2)$ equals $\lfloor \frac{m-1}{2} \rfloor$. The maximal subspaces of a Hermitian variety are called *generators*. From now on, we will denote the standard non-singular Hermitian variety in $\mathrm{PG}(m, q^2)$ by $\mathcal{H}(m, q^2)$. A *singular Hermitian variety* in $\mathrm{PG}(m, q^2)$ is a cone with an i-dimensional subspace as vertex and a non-singular Hermitian variety in an $(m - i - 1)$-dimensional subspace, disjoint from the vertex, as base, $-1 \le i \le m$. All singular Hermitian varieties in $\mathrm{PG}(m, q^2)$ with an i-dimensional vertex are projectively equivalent to the one given by the equation

$$X_0^{q+1} + X_1^{q+1} + \cdots + X_{m-i-1}^{q+1} = 0\,.$$

Note that a non-singular Hermitian variety is a singular Hermitian variety with vertex dimension equal to -1.

Lemma 1.3. The number of generators on $\mathcal{H}(2n + 1, q^2)$ is $\prod_{i=0}^{n}(q^{2i+1} + 1)$.

Proof. This, and many other results on Hermitian varieties, can be found in [4, Chapter 23]. $\square$

Notation 1.4. Throughout this article, we will denote the number of points in $\mathrm{PG}(m, q)$ by $\theta_m(q) = \frac{q^{m+1}-1}{q-1}$ and the number of points on $\mathcal{H}(m, q^2)$ by $\mu_m(q^2) = \frac{(q^{m+1}-(-1)^{m+1})(q^m-(-1)^m)}{q^2-1}$.

Definition 1.5. The *support* of a code word c is the set of positions with nonzero entry, i.e. $\mathrm{supp}(c) = \{p : c_p \ne 0\} \subseteq \mathcal{P}$. Note that we identify the set of positions $\mathrm{supp}(c)$ with a set of points of $\mathcal{P}$ using the correspondence between those. The *Hamming weight* $\mathrm{wt}(c)$ of a code word c is the number of nonzero symbols in it, i.e. it is $|\mathrm{supp}(c)|$. The minimum distance d of $C_k(\mathcal{S})^\perp$ is $\min_{c \in C_k(\mathcal{S})^\perp \setminus \{0\}} \mathrm{wt}(c)$.

The following theorems on $C_n(\mathcal{H}(2n + 1, q^2))^\perp$ are known.

Theorem 1.6 ([5, Proposition 3.7])**.** Let $n = 1$. Then the supports of all code words c with $0 < \mathrm{wt}(c) < 3q$ are projectively equivalent, and their Hamming weights are $2(q + 1)$. If $\mathrm{wt}(c) \le \frac{\sqrt{q}(q+1)}{2}$, then c is a linear combination of these code words.

Theorem 1.7 ([8, Theorem 43])**.** Let $n = 2$. If c is a code word with $\mathrm{wt}(c) \le 2(q^3 + q^2)$ and if q is sufficiently large, then there are only two possible projective equivalence classes for $\mathrm{supp}(c)$, and the Hamming weights of the corresponding code words are $2(q^3 + 1)$ and $2(q^3 + q^2)$. These two types of code words are examples of the code words constructed in Theorem 2.4.

In this article, we will discuss the dual code arising from the points and generators of a Hermitian variety. This improves upon earlier work of [8, Section 5]. We determine the minimum Hamming weight for general n, and we show that if q is sufficiently large, a similar statement to the second part of Theorem 1.6 holds for general n. Our main result is as follows.

Theorem 1.8. Let n be any positive integer and let $\delta > 0$ be any constant. If c is a code word with $\mathrm{wt}(c) < 4q^{2n-1}$ and q is sufficiently large, then there are only n possible projective equivalence classes for $\mathrm{supp}(c)$; call S this set of projective equivalence classes. If c is a code word with $\mathrm{wt}(c) < \delta q^{2n-1}$, then c is a linear combination of code words which are an incidence vector of a set in S. The minimum distance of $C_n(\mathcal{H}(2n + 1, q^2))^\perp$ is $2q^{2n-4}(q^3 + 1)$ for $n \ge 2$.

2 The code words

In this section we introduce a set of code words of the code $C_n(\mathcal{H}(2n+1, q^2))^\perp$. From now on, we consider the projective space $\mathrm{PG}(2n + 1, q^2)$, $n \ge 1$.

Lemma 2.1. Consider a non-singular Hermitian variety $\mathcal{H}(2n + 1, q^2)$ in $\mathrm{PG}(2n + 1, q^2)$ and let σ be the corresponding polarity. Let π be a k-dimensional subspace in $\mathrm{PG}(2n + 1, q^2)$ such that $\pi \cap \mathcal{H}(2n + 1, q^2)$ is a cone $\pi_i H_{k-i-1}$ with $H_{k-i-1} \cong \mathcal{H}(k - i - 1, q^2)$ and π_i an i-space, $-1 \leq i \leq \min\{k, n\}$. Then $\pi \cap \pi^\sigma = \pi_i$. Conversely, if $\pi \cap \pi^\sigma$ is an i-space π_i, then $\pi \cap \mathcal{H}(2n + 1, q^2)$ is a cone $\pi_i H_{k-i-1}$ with $H_{k-i-1} \cong \mathcal{H}(k - i - 1, q^2)$.

Proof. The first statement is [4, Lemma 23.2.8]; the second statement is a corollary of the first. $\square$

We will use this theorem mostly in the case $k = n$. Using the above lemma, we can prove an easy counting result.

Theorem 2.2. The number of generators on $\mathcal{H}(2n+1, q^2)$ through a fixed k-space on $\mathcal{H}(2n+1, q^2)$, $0 \leq k \leq n$, equals $\prod_{i=0}^{n-k-1}(q^{2i+1} + 1)$.

Proof. Let π_k be a k-space on $\mathcal{H}(2n+1, q^2)$ and let σ be the polarity corresponding to $\mathcal{H}(2n+1, q^2)$. Then π_k^σ is a $(2n-k)$-space intersecting $\mathcal{H}(2n+1, q^2)$ in a cone $\pi_k H$ with $H \cong \mathcal{H}(2n - 2k - 1, q^2)$. Every generator on $\mathcal{H}(2n + 1, q^2)$ through π_k corresponds uniquely to a generator on H. Hence, there are $\prod_{i=0}^{n-k-1}(q^{2i+1} + 1)$ generators on $\mathcal{H}(2n + 1, q^2)$ through π_k. $\square$

In the construction of the code words we need the following lemma.

Lemma 2.3. Let π be an n-space in $\mathrm{PG}(2n + 1, q^2)$ and let μ be a generator of $\mathcal{H}(2n + 1, q^2)$. Then $\pi \cap \mu$ and $\pi^\sigma \cap \mu$ are subspaces of the same dimension.

Proof. We denote $\mu \cap \pi = \pi_j$, a j-space, possibly empty ($j = -1$). It follows that $2n - j = \dim((\mu \cap \pi)^\sigma) = \dim(\langle \mu^\sigma, \pi^\sigma \rangle)$. Using the Grassmann identity and $\mu = \mu^\sigma$ (μ is a generator), we find $\dim(\mu \cap \pi^\sigma) = \dim(\mu) + \dim(\pi^\sigma) - \dim(\langle \mu^\sigma, \pi^\sigma \rangle) = j$. $\square$

Now, we can give the construction of small weight code words in the code $C_n(\mathcal{H}(2n + 1, q^2))^\perp$. This construction is based on [8, Theorem 58].

Theorem 2.4. Consider $\mathcal{H}(2n + 1, q^2)$ and its corresponding polarity σ. Let π be an n-space in $\mathrm{PG}(2n + 1, q^2)$. Denote the incidence vector of $\pi \cap \mathcal{H}(2n + 1, q^2)$ by v_π and the incidence vector of $\pi^\sigma \cap \mathcal{H}(2n + 1, q^2)$ by v_{π^σ}. Then $\alpha(v_\pi - v_{\pi^\sigma})$, $\alpha \in \mathbb{F}_p$, is a code word of $C_n(\mathcal{H}(2n + 1, q^2))^\perp$.

Proof. Let μ be a generator of $\mathcal{H}(2n + 1, q^2)$ and denote its incidence vector by v_μ. Using Lemma 2.3, we find μ intersects both π and π^σ, or neither. In the first case $|\pi \cap \mu| \equiv |\pi^\sigma \cap \mu| \equiv 1 \pmod{q}$ and in the second case $|\pi \cap \mu| = |\pi^\sigma \cap \mu| = 0$. In both cases $v_\pi \cdot v_\mu = v_{\pi^\sigma} \cdot v_\mu$. The theorem follows. $\square$

Example 2.5. We list the different possibilities for $\pi \cap \pi^\sigma$. Hereby, we use Lemma 2.1 for $k = n$ and Theorem 2.4. We write $\mathcal{H} = \mathcal{H}(2n + 1, q^2)$.

- $\pi \cap \pi^\sigma = \emptyset$. We write $\pi \cap \mathcal{H} = H$ and $\pi^\sigma \cap \mathcal{H} = H'$. We know, $H, H' \cong \mathcal{H}(n, q^2)$. The corresponding code words have weight $2\mu_n(q^2)$.

- $\pi \cap \pi^\sigma = \pi_i$, an i-space, $0 \leq i \leq n - 2$. We write $\pi \cap \mathcal{H} = \pi_i H$ and $\pi^\sigma \cap \mathcal{H} = \pi_i H'$, which are both cones, with $H, H' \cong \mathcal{H}(n - i - 1, q^2)$. The corresponding code words have weight $2q^{2i+2}\mu_{n-i-1}(q^2)$.

- $\pi \cap \pi^\sigma = \pi_{n-1}$, an $(n-1)$-space. Then $\pi \cap \mathcal{H} = \pi^\sigma \cap \mathcal{H} = \pi_{n-1}$ since $\mathcal{H}(0, q^2)$ is empty. The construction gives rise to the zero code word.

- $\pi \cap \pi^\sigma = \pi_n$, an n-space. Then $\pi = \pi^\sigma = \pi_n \subset \mathcal{H}$. Also in this case, the construction gives rise to the zero code word.

It can easily be checked that among these four cases, the code words with smallest weight are the ones corresponding to $i = n - 3$.

Remark 2.6. Consider the construction from Theorem 2.4, with $\pi \cap \mathcal{H} = \pi_i H_{n-i-1}$ and $\pi^\sigma \cap \mathcal{H} = \pi_i H'_{n-i-1}$. Let P be a point of $\pi_i H_{n-i-1}$ and let P' be a point of $\pi_i H'_{n-i-1}$. We know that $P' \in \pi^\sigma \subseteq P^\sigma$ and $P' \in \mathcal{H}$. Hence, the line PP' is a line of $\mathcal{H}$.

3 Some counting results

Lemma 3.1. Consider the non-singular Hermitian variety $\mathcal{H}(2n+1, q^2) \subset \mathrm{PG}(2n+1, q^2)$ and let σ be the corresponding polarity. Let τ be a j-space such that $\tau \cap \mathcal{H}(2n+1, q^2) = H_j \cong \mathcal{H}(j, q^2)$, $-1 \leq j \leq n$. The number of generators on $\mathcal{H}(2n+1, q^2)$ skew to τ equals

$$c_{n,j} := q^{\binom{j+1}{2}} \prod_{k=0}^{n-j-1} (q^{2k+1} + 1) \prod_{l=2(n-j)+1}^{2n-j+1} (q^l - (-1)^l).$$

Proof. By [4, Theorem 23.4.2 (i)] we know that the number of generators skew to τ only depends on the parameters n and j and not on the choice of τ itself.

We will prove this theorem using induction on j. If $j = -1$, τ is the empty space and hence $c_{n,-1}$ equals the total number of generators. By Lemma 1.3 we find $c_{n,-1} = \prod_{k=0}^{n}(q^{2k+1} + 1)$. Now, we prove that a relation between $c_{n,j}$ and $c_{n-1,j-1}$ holds.

By Lemma 2.1 we know $\tau \cap \tau^{\sigma} = \emptyset$. Hence, every point $P \in \mathrm{PG}(2n+1, q^2) \setminus (\tau \cup \tau^{\sigma})$ can uniquely be written as $P_{\tau} + \lambda_P P_{\tau^{\sigma}}$, $P_{\tau} \in \tau$, $P_{\tau^{\sigma}} \in \tau^{\sigma}$, $\lambda_P \in \mathbb{F}_{q^2}^*$. For every point $P \in \mathrm{PG}(2n+1, q^2) \setminus (\tau \cup \tau^{\sigma})$, we define $\phi_{\tau}(P) = P_{\tau}$. This is the projection of P from τ^{σ} on τ. We define a correlation $\overline{\sigma} : \tau \to \tau$ that maps the subspace $U \subset \tau$ to $U^{\sigma} \cap \tau$. It is straightforward to check that $\overline{\sigma}$ defines a polarity on τ. Moreover, it can be seen easily that the points of H_j are the absolute points of $\overline{\sigma}$. Hence, $\overline{\sigma}$ is the polarity of τ corresponding to H_j.

Now, we consider the set $S = \{(P, \mu) \mid P \in \mu \setminus \tau^{\sigma}, \phi_{\tau}(P) \notin H_j, \mu \text{ a generator}, \mu \cap \tau = \emptyset\}$. We count the number of elements of S in two ways. On the one hand, there are $c_{n,j}$ generators skew to τ. Let μ be such a generator. The intersection $\mu \cap \tau^{\sigma}$ is an $(n-j-1)$-space since $\dim(\mu \cap \tau^{\sigma}) + \dim(\langle \mu, \tau \rangle) = 2n$. We also know that $\phi_{\tau}(P) = R$ for every point $P \in \langle R, \mu \cap \tau^{\sigma} \rangle \setminus (\mu \cap \tau^{\sigma})$, $R \in \tau$. Hence, for each generator there are $\theta_n(q^2) - \theta_{n-j-1}(q^2) - \mu_j(q^2)(\theta_{n-j}(q^2) - \theta_{n-j-1}(q^2)) = q^{2(n-j)}(\theta_j(q^2) - \mu_j(q^2))$ points fulfilling the requirements. On the other hand, we count the points $P \in \mathcal{H}(2n+1, q^2) \setminus (\tau \cup \tau^{\sigma})$ fulfilling the requirements. There are $\mu_{2n+1}(q^2) - \mu_j(q^2) - \mu_{2n-j}(q^2)$ points in this set. We must assure that $\phi_{\tau}(P) \notin H_j$. Let R be a point of H_j. Since $\tau^{\sigma} \subseteq R^{\sigma}$, a line RQ, $Q \in \tau^{\sigma}$, is a tangent line (in R) to $\mathcal{H}(2n+1, q^2)$ or a line which is completely contained in $\mathcal{H}(2n+1, q^2)$. Hence, $\phi_{\tau}(P)$ is a point of H_j iff P lies on a line through $\phi_{\tau}(P)$ and a point of $\tau^{\sigma} \cap \mathcal{H}(2n+1, q^2)$. Consequently there are

$$\mu_{2n+1}(q^2) - \mu_j(q^2) - \mu_{2n-j}(q^2) - \mu_j(q^2)\mu_{2n-j}(q^2)(q^2 - 1)$$
$$= q^{2n-j}(\theta_j(q^2) - \mu_j(q^2))(q^{2n-j+1} - (-1)^{2n-j+1})$$

points $P \in \mathcal{H}(2n+1, q^2) \setminus (\tau \cup \tau^{\sigma})$ fulfilling the requirement $\phi_{\tau}(P) \notin H_j$. Now, we fix such a point P and we count the number of generators skew to τ, through it. All these generators are contained in P^{σ}. We know $P^{\sigma} \cap \mathcal{H}(2n+1, q^2)$ is a cone PH_{2n-1}, with $H_{2n-1} \cong \mathcal{H}(2n-1, q^2)$. There is a 1-1 correspondence between the generators of $\mathcal{H}(2n+1, q^2)$ through P and the generators of H_{2n-1}. We also find

$$\tau \cap P^{\sigma} = \tau \cap (\phi_{\tau}(P) + \lambda P')^{\sigma} = \tau \cap ((\phi_{\tau}(P))^{\sigma} + \lambda^q P'^{\sigma}) = \tau \cap (\phi_{\tau}(P))^{\sigma} = (\phi_{\tau}(P))^{\overline{\sigma}},$$

with $P' \in \tau^{\sigma}$ (and thus $\tau \subset P'^{\sigma}$). Hence, the $(j-1)$-space $\tau \cap P^{\sigma}$ intersects $\mathcal{H}(2n+1, q^2)$ in $H_{j-1} \cong \mathcal{H}(j-1, q^2)$, since $\phi_{\tau}(P) \notin H_j$. We can choose the base of the cone PH_{2n-1} such that it contains $\tau \cap P^{\sigma}$. The generators through P and skew to τ correspond to the generators of H_{2n-1}, skew to $\tau \cap P^{\sigma}$. There are $c_{n-1,j-1}$ such generators. We conclude

$$c_{n,j} q^{2(n-j)} \left[\theta_j(q^2) - \mu_j(q^2) \right] = c_{n-1,j-1} q^{2n-j} \left[\theta_j(q^2) - \mu_j(q^2) \right] (q^{2n-j+1} - (-1)^{2n-j+1})$$
$$\Rightarrow \quad c_{n,j} = c_{n-1,j-1} q^j (q^{2n-j+1} - (-1)^{2n-j+1}).$$

An induction calculation now finishes the proof. $\square$

From now on in this section, we use the following notation: $H \cong \mathcal{H}(2n+1, q^2)$ is a non-singular Hermitian variety and σ is the polarity corresponding to it; π is an n-space in $\mathrm{PG}(2n+1, q^2)$, such

that $\pi \cap H$ is a cone $\pi_i H_{n-i-1}$ with $H_{n-i-1} \cong \mathcal{H}(n-i-1, q^2)$ and π_i an i-space, $-1 \le i \le n$. By Lemma 2.1, for $k = n$, we know $\pi \cap \pi^\sigma = \pi_i$ and consequently $\pi^\sigma \cap H$ is a cone $\pi_i H'_{n-i-1}$ with $H'_{n-i-1} \cong \mathcal{H}(n-i-1, q^2)$.

Definition 3.2. The number of generators on H intersecting π in a fixed point $P \in \pi_i H_{n-i-1} \setminus \pi_i$ and no other point of $\pi_i H_{n-i-1}$, and intersecting π^σ in a fixed point $P' \in \pi_i H'_{n-i-1} \setminus \pi_i$ and no other point of $\pi_i H'_{n-i-1}$ is denoted by $N(\pi, P, P')$. The number of generators on H skew to π is denoted by $N'(\pi)$.

By Lemma 2.3 we know that the generators skew to π are also skew to π^σ and that the generators intersecting π in precisely one point also intersect π^σ in precisely one point.

Lemma 3.3. The number $N'(\pi)$ only depends on the intersection parameters (n, i) of π.

Proof. This follows immediately from [4, Theorem 23.4.2 (i)]. $\qquad\square$

Notation 3.4. Consequently, we can denote $N'(\pi)$ by $N'(n, i)$.

Lemma 3.5. For $n \ge 2$, $-1 \le i \le n-2$, $N(\pi, P, P') = N'(n-2, i)$. Consequently, $N(\pi, P, P')$ only depends on the intersection parameters (n, i) of π.

Proof. Consider the points $P \in (\pi_i H_{n-i-1} \setminus \pi_i) \subseteq \pi$ and $P' \in (\pi_i H'_{n-i-1} \setminus \pi_i) \subseteq \pi^\sigma$. Denote $\ell = \langle P, P' \rangle$. Then ℓ^σ is a $(2n-1)$-space intersecting H in a cone with ℓ as vertex and a non-singular $(2n-3)$-dimensional Hermitian variety H_{2n-3} as base. Since $\dim(\ell \cap \pi) = \dim(\ell \cap \pi^\sigma) = 0$, $\ell^\sigma \cap \pi = V$ is an $(n-1)$-space and $\ell^\sigma \cap \pi^\sigma = V'$ is an $(n-1)$-space. Also, $\ell \subset \langle \pi, \pi^\sigma \rangle = \pi_i^\sigma$, hence $\pi_i \subset l^\sigma$. Let W, resp. W', be an $(n-2)$-space in V, resp. V', containing π_i and not through P, resp. P'. Denote the $(2n-i-4)$-space $\langle W, W' \rangle$ by τ'. It can be seen that on the one hand $\tau' \subset \ell^\sigma$ and on the other hand $\ell \cap \tau' = \emptyset$, so the $(2n-3)$-space τ containing the base H_{2n-3} can be chosen such that $\tau' \subseteq \tau$. Let σ' be the polarity of τ corresponding to H_{2n-3}. Analogously to the proof of Lemma 3.1 we can define this polarity as follows: $U^{\sigma'} = \tau \cap U^\sigma$. It now immediately follows that $W^{\sigma'} = W'$ because both are $(n-2)$-spaces contained in W^σ and in τ.

Arguing as in the proof of Lemma 3.1, we see there is a 1-1 correspondence between the generators of H_{2n-3} and the generators of H through ℓ (the generators containing P and P'). If a generator of H through ℓ contains no points of $\pi \cup \pi^\sigma$ but P and P', then its corresponding generator of H_{2n-3} is skew to W and W'. Vice versa, every generator μ of H_{2n-3} skew to W and W', is contained in precisely one generator of H intersecting $\pi \cup \pi^\sigma$ in only the points P and P', namely $\langle \mu, P, P' \rangle$. Since $W^{\sigma'} = W'$, the generators of H_{2n-3} skew to W and W' are the ones skew to W, by Lemma 2.3. Hence, $N(\pi, P, P') = N'(n-2, i)$.

The second statement of the lemma follows immediately from the first one. $\qquad\square$

Notation 3.6. Since $N(\pi, P, P')$ only depends on the intersection parameters (n, i) of π, we can denote it by $N(n, i)$.

The previous theorem now states $N(n, i) = N'(n-2, i)$ for $n \ge 2$, $-1 \le i \le n-2$.

Lemma 3.7. For $n \ge 1$ and $-1 \le i \le n-2$, the following equality holds:

$$N(n, i) = q^{(n-1)^2 - \binom{n-i-1}{2}} \prod_{j=1}^{n-i-2} (q^j - (-1)^j).$$

Proof. We prove this theorem using induction. Using Lemma 3.5, we know that $N(n, -1)$ equals $N'(n-2, -1)$, the number of generators of a Hermitian variety $H' \cong \mathcal{H}(2n-3, q^2)$ skew to an $(n-2)$-space intersecting H' in a Hermitian variety $\mathcal{H}(n-2, q^2)$, if $n \ge 2$. This number equals $c_{n-2, n-2}$. Hence, by Lemma 3.1,

$$N(n, -1) = q^{\binom{n-1}{2}} \prod_{l=1}^{n-1} (q^l - (-1)^l) = q^{(n-1)^2 - \binom{n-(-1)-1}{2}} \prod_{j=1}^{n-(-1)-2} (q^j - (-1)^j),$$

5

which proves the induction base for $n \geq 2$. If $n = 1$, it is easy to prove that $N(1, -1) = 1$. Hence, the formula holds also in this case.

Now, we will prove that $N(n, i) = q^{2n-3}N(n-1, i-1)$. By Lemma 3.5, this is equivalent to proving that $N'(n, i) = q^{2n+1}N'(n-1, i-1)$. Consider the set $S = \{(R, \mu) \mid R \in \mu, \mu$ a generator skew to $\pi, R \notin \langle \pi, \pi^\sigma \rangle = \pi_i^\sigma\}$. This subspace π_i^σ intersects H in a cone $\pi_i H_{2(n-i)-1}$. We will count $|S|$ in two ways.

On the one hand, there are $N'(n, i)$ generators skew to π. Fix such a generator μ. Then $\dim(\mu \cap \pi_i^\sigma) = n - i - 1$ since $\dim(\mu \cap \pi_i^\sigma) + \dim(\langle \mu, \pi_i \rangle) = 2n$. So, μ contains precisely $\theta_n(q^2) - \theta_{n-i-1}(q^2) = q^{2(n-i)}\theta_i(q^2)$ points of $\mathrm{PG}(2n+1, q^2) \setminus \pi_i^\sigma$. Consequently, $|S| = q^{2(n-i)}\theta_i(q^2)N'(n, i)$.

On the other hand, there are $\mu_{2n+1}(q^2) - \theta_i(q^2) - \mu_{2(n-i)-1}(q^2) - (q^2-1)\theta_i(q^2)\mu_{2(n-i)-1}(q^2) = q^{4n-2i+1}\theta_i(q^2)$ points in $H \setminus \pi_i^\sigma$. Fix such a point P. The hyperplane P^σ intersects π in an $(n-1)$-space V and intersects π_i in an $(i-1)$-space $\pi_{i-1} \subset V$. Hence, the intersection $V \cap H$ has intersection parameters $(n-1, i-1)$. The intersection $P^\sigma \cap H$ is a cone PH_{2n-1}, with $H_{2n-1} \cong \mathcal{H}(2n-1, q^2)$. Let τ be the $(2n-1)$-space containing H_{2n-1}. We can choose τ such that it contains V. Then, there is a 1-1 correspondence between the generators of $\mathcal{H}(2n+1, q^2)$ through P, skew to π and the generators of H_{2n-1} skew to V. Consequently, there are $N'(n-1, i-1)$ such generators. Thus, $|S| = q^{4n-2i+1}\theta_i(q^2)N'(n-1, i-1)$.

Comparing both expressions for $|S|$, we find the desired relation between $N'(n, i)$ and $N'(n-1, i-1)$. An easy calculation now finishes the proof. $\square$

Lemma 3.8. Assume $n \geq 2$ and $-1 \leq i \leq n-2$. Let P be a point of $H \setminus (\pi \cup \pi^\sigma)$. Let $n_P(n, i)$ be the number of generators through P intersecting both $\pi \setminus \pi_i$ and $\pi^\sigma \setminus \pi_i$ in precisely one point. Then,

- $n_P(n, i) = N(n-1, i-1)q^{4i}\left(\mu_{n-i-1}(q^2)\right)^2$ if $P \notin \langle \pi, \pi^\sigma \rangle = \pi_i^\sigma$;

- $n_P(n, i) = N(n-1, i)q^{4i+4}\left(\mu_{n-i-2}(q^2)\right)^2$ if $P \in \langle \pi, \pi^\sigma \rangle = \pi_i^\sigma$ but P does not lie on a line of H through a point of $\pi \setminus \pi_i$ and a point of $\pi^\sigma \setminus \pi_i$;

- $n_P(n, i) = N(n-1, i+1)q^{4i+4}\mu_{n-i-3}(q^2)\left[q^4\mu_{n-i-3}(q^2) + q^2 - 1\right]$ if $P \in \langle \pi, \pi^\sigma \rangle = \pi_i^\sigma$ and P lies on a line of H through a point of $\pi \setminus \pi_i$ and a point of $\pi^\sigma \setminus \pi_i$, and $i \leq n-4$.

- $n_P(n, i) = q^{2i+2}N(n, i)$ if $P \in \langle \pi, \pi^\sigma \rangle = \pi_i^\sigma$ and P lies on a line of H through a point of $\pi \setminus \pi_i$ and a point of $\pi^\sigma \setminus \pi_i$, and $i = n-3, n-2$.

The first case can only occur if $i \geq 0$. The second case can only occur if $i \leq n-3$.

Proof. Since $P \notin \pi \cup \pi^\sigma$, $P^\sigma \cap \pi = V$ is an $(n-1)$-space and $P^\sigma \cap \pi^\sigma = V'$ is an $(n-1)$-space. Furthermore $P^\sigma \cap H$ is a cone PH_{2n-1} with $H_{2n-1} \cong \mathcal{H}(2n-1, q^2)$. Let τ be the $(2n-1)$-space containing H_{2n-1}.

First we consider the case $P \notin \langle \pi, \pi^\sigma \rangle = \pi_i^\sigma$. In this case P^σ intersects π_i in an $(i-1)$-space $\pi_{i-1} = V \cap V'$. Also, τ can be chosen so that it contains V and V'. Hence, the number of generators through P fulfilling the requirements equals the number of generators of H_{2n-1} intersecting V and V' in a point. Let σ' be the polarity of τ corresponding to H_{2n-1}. Analogously to the argument in the proof of Lemma 3.5, it can be seen that $V' = V^{\sigma'}$. Consequently there are $N(n-1, i-1)$ generators of this type through a fixed point of $V \setminus \pi_{i-1}$ and a fixed point of $V' \setminus \pi_{i-1}$. There are $q^{2i}\mu_{n-i-1}(q^2)$ possible choices for each of these points. The first part of the lemma follows. Note that $\langle \pi, \pi^\sigma \rangle = \mathrm{PG}(2n+1, q^2)$ if $i = -1$. Hence, this case cannot occur if $i = -1$.

We fix some notation for the remaining cases. Let $W \subseteq \pi$ and $W' \subseteq \pi^\sigma$ be the $(n-i-1)$-spaces containing H_{n-i-1} and H'_{n-i-1}, respectively. Furthermore, let $\overline{\sigma}$ and $\overline{\sigma}'$ be the polarities of W and W', respectively corresponding to H_{n-i-1} and H'_{n-i-1}. In all three remaining cases, $\pi_i \subset P^\sigma$, hence $P^\sigma \cap W = W_1$ and $P^\sigma \cap W' = W'_1$ are $(n-i-2)$-spaces. Now, the point P can be written in a unique way as $P = \lambda P_{\pi_i} + \lambda_P P_W + P_{W'}$, with $P_W \in W, P_{W'} \in W', P_{\pi_i} \in \pi_i$ and $\lambda, \lambda_P \in \mathbb{F}_{q^2}$. Arguing as in the proof of Lemma 3.1 we can see that $W_1 = P^\sigma \cap W = P_W^{\overline{\sigma}}$ and that $W'_1 = P^\sigma \cap W' = P_{W'}^{\overline{\sigma}'}$. Moreover, since P and P_{π_i} are contained in P^σ, neither or both of P_W and $P_{W'}$ are contained in P^σ. Hence, we need to distinguish two cases.

- $P_W \in W_1$ and $P_{W'} \in W'_1$ are both contained in P^σ; consequently, $P_W \in P_W^{\overline{\sigma}}$, thus $P_W \in H_{n-i-1} \subset H$ and $P_W^{\overline{\sigma}} \cap H_{n-i-1}$ is a cone $P_W H_{n-i-3}$, with $H_{n-i-3} \cong \mathcal{H}(n-i-3, q^2)$. Let $W_2 \subset W_1$ be the $(n-i-3)$-space containing H_{n-i-3}. Then, the intersection of $V = \langle \pi_i, W_1 \rangle$ and H is the cone with vertex $\langle \pi_i, P_W \rangle$ and base H_{n-i-3}. Analogously we introduce $H'_{n-i-3} \subset W'_2 \subset W'_1$. Then $V' \cap H$ is the cone with vertex $\langle \pi_i, P_{W'} \rangle$ and base H'_{n-i-3}. Furthermore, since $P_W \in V$, $P_{W'} \in V'$, and $P_{\pi_i} \in V, V'$, P is contained in $\langle V, V' \rangle$. Also, the line PP_W is contained in P^σ and is not a 1-secant since $P, P_W \in H$, hence it is a line of H. This line intersects π^σ in a point of $\langle P_{W'}, \pi_i \rangle \setminus \pi_i$.

- $P_W \notin W_1$ and $P_{W'} \notin W'_1$ are both not contained in P^σ; consequently, $P_W \notin P_W^{\overline{\sigma}}$, thus $P_W \notin H_{n-i-1}$, $P_W \notin H$ and $P_W^{\overline{\sigma}} \cap H_{n-i-1}$ is a non-singular Hermitian variety $H_{n-i-2} \cong \mathcal{H}(n-i-2, q^2)$ in W_1. Then, the intersection of $V = \langle \pi_i, W_1 \rangle$ and H is the cone $\pi_i H_{n-2-i}$. Analogously we introduce $H'_{n-i-2} \subset W'_1$. The intersection $V' \cap H$ is the cone $\pi_i H'_{n-i-2}$. Furthermore, $P \notin \langle V, V' \rangle$ since $P_W \notin W_1$ and $P_{W'} \notin W'_1$. Also, all lines in $\pi_i^{\sigma+}$ through P intersecting $\pi \setminus \pi_i$ and $\pi^\sigma \setminus \pi_i$, are contained in $\langle P_W, P_{W'}, \pi_i \rangle$, but not in $\langle P, \pi_i \rangle$. Since $P_W, P_{W'} \notin P^\sigma$, none of the lines through P can be contained in H.

These two cases clearly correspond to the three remaining cases of the lemma. We will treat them separately.

First of all, we look at the latter, which is the second case in the statement of the lemma. Since $P \notin \langle V, V' \rangle$, we can choose τ such that it contains $\langle V, V' \rangle$. Hence, every generator through P, intersecting both $\pi \setminus \pi_i$ and $\pi^\sigma \setminus \pi_i$ in a point, corresponds to a generator of H_{2n-1} intersecting both $V \setminus \pi_i$ and $V' \setminus \pi_i$ in a point, and vice versa. For a fixed point in $V \setminus \pi_i$ and a fixed point in $V' \setminus \pi_i$, there are $N(n-1, i)$ such generators. We also know that $|V \setminus \pi_i| = |V' \setminus \pi_i| = q^{2i+2}\mu_{n-i-2}(q^2)$. The second part of the lemma follows. Note that $V \setminus \pi_i$ and $V' \setminus \pi_i$ are empty if $i = n-2$. Hence, this case only occurs if $i \leq n-3$.

Finally, we look at the former case, the third and the fourth case in the statement of the lemma. Let ℓ be a line on H through P, a point of $\pi \setminus \pi_i$ and a point of $\pi^\sigma \setminus \pi_i$. By changing, if necessary, the choices for W and W', we can assume $\ell = P_W P_{W'}$. We distinguish between two types of generators: the ones that contain ℓ and the ones that do not contain ℓ. First we look at the ones that contain ℓ. We know $\ell^\sigma \cap H$ is a cone with vertex ℓ and base $H_{2n-3} \cong \mathcal{H}(2n-3, q^2)$. Let τ' be the $(2n-3)$-space containing H_{2n-3}. We can choose τ' so that it contains π_i, W_2 and W'_2. As before, one can see that $\langle \pi_i, W_2 \rangle^{\widehat{\sigma}'} = \langle \pi_i, W'_2 \rangle$, with $\widehat{\sigma}'$ the polarity of τ' corresponding to H_{2n-3}. The number of generators of the requested type through ℓ then equals the number of generators of H_{2n-3} skew to $\langle \pi_i, W_2 \rangle$. This number equals $N'(n-2, i) = N(n, i)$. Furthermore, since ℓ is a line on H through P intersecting $\pi \setminus \pi_i$ and $\pi^\sigma \setminus \pi_i$, every line through P and a point of $\langle P_W, \pi_i \rangle \setminus \pi_i$ lies on H and intersects $\langle P_{W'}, \pi_i \rangle \setminus \pi_i \subset \pi^\sigma \setminus \pi_i$. Thus, there are $\theta_{i+1}(q^2) - \theta_i(q^2) = q^{2i+2}$ such lines. Hence, there are $q^{2i+2}N(n, i)$ generators of the first type. Now, we assume no line through P, intersecting π and π^σ, is contained in the generator. Let Q_W and $Q_{W'}$ be the points of the generator in W and W', respectively. By the previous remarks on this case, we know there are $\mu_{n-i-3}(q^2)q^{2i+4}$ possible choices for Q_W and for $Q_{W'}$. Now, we consider the plane $\langle P, Q_W, Q_{W'} \rangle$. Using arguments, similar to the ones in the previous case, we find $N'(n-3, i+1) = N(n-1, i+1)$ generators fulfilling the requirements for every choice of Q_W and $Q_{W'}$. Hence, the total number of generators in this third case equals

$$
\begin{aligned}
n_P &= q^{2i+2}N(n, i) + \left(\mu_{n-i-3}(q^2)q^{2i+4}\right)^2 N(n-1, i+1) \\
&= \left[q^{2i+2}q^{2i+2}(q^2-1)\mu_{n-i-3}(q^2) + \left(\mu_{n-i-3}(q^2)q^{2i+4}\right)^2\right] N(n-1, i+1) \\
&= q^{4i+4}\mu_{n-i-3}(q^2)\left[q^2 - 1 + q^4\mu_{n-i-3}(q^2)\right] N(n-1, i+1).
\end{aligned}
$$

Hereby we used the relation between $N(n, i)$ and $N(n-1, i+1)$ which can immediately be derived from Lemma 3.7.

Note that $V \setminus \langle \pi_i, P_W \rangle$ and $V' \setminus \langle \pi_i, P_{W'} \rangle$ are empty if $n-3 \leq i \leq n-2$. In this case, we cannot

consider the points Q_W and $Q_{W'}$. So, there are no generators of the second type. Consequently, all generators are of the first type and there are precisely $q^{2i+2}N(n,i)$ such generators. $\square$

4   Classifying the small weight code words

Before giving the new classification theorem, we state the results about the codes $C_1(\mathcal{H}(3,q^2))^\perp$ and $C_2(\mathcal{H}(5,q^2))^\perp$ to which we referred earlier.

Theorem 4.1 ([5, Proposition 3.7]). Let C be the code $C_1(\mathcal{H}(3,q^2))^\perp$. There is only one non-trivial type of code words among the ones described in Example 2.5, namely $i = -1$. These are the code words of minimal weight. Let c be a code word of C with $\mathrm{wt}(c) \leq \frac{\sqrt{q}(q+1)}{2}$. Then c is a linear combination of code words of minimal weight.

Theorem 4.2 ([8, Theorem 43]). Let c be a code word of $C_2(\mathcal{H}(5,q^2))^\perp$, $q > 893$, with $\mathrm{wt}(c) \leq 2(q^3 + q)$, then c is a code word of one of the types described in Theorem 2.4. Regarding Example 2.5, we know that there are precisely two possibilities since $n = 2$, namely $i = -1$ and $i = 0$.

It is our aim to generalise this result. We start our arguments with two lemmas about n-spaces: the second lemma shows the existence of an n-space containing a non-trivial amount of points of the support of a code word, while the first lemma shows that a generator cannot contain many points of the support of a code word. In the proof of the second lemma we use the following result.

Theorem 4.3. Let $c \in C_n(\mathcal{H}(2n+1,q^2))^\perp$ be a code word and denote $\mathrm{supp}(c) = S$. Let P be a point in S. Then $|P^\sigma \cap S| \geq 2 + q^{2n-1}$.

Proof. This is a special case of [8, Proposition 9(d)]. $\square$

Throughout the three following lemmas the value $\Sigma_{n,i}$ is used, $-1 \leq i \leq n-2$. It is defined by

$$\Sigma_{n,i} = \begin{cases} 2q^{2i+2}\mu_{n-i-1}(q^2) + 4\frac{\mu_{n-i-2}(q^2)(q^{n-i-1}-1)}{q^{n-3i-5}(q^2-1)} & n-i \text{ odd}, \\ 2q^{2i+2}\left[\mu_{n-i-1}(q^2) + 2\frac{q^4\mu_{n-i-3}(q^2)+q^2-1}{q^2-1}\right] & n-i \text{ even}. \end{cases}$$

Note that in both cases $\Sigma_{n,i} = 2q^{2n-1} + f$, with $f \in \mathcal{O}(q^{2n-2})$ and $f > 0$ if $q > 0$.

Lemma 4.4. Let $c \in C_n(\mathcal{H}(2n+1,q^2))^\perp$ be a code word with $\mathrm{wt}(c) \leq w = \delta q^{2n-1}$, and denote $\mathrm{supp}(c) = S$. Let π be a generator of $\mathcal{H}(2n+1,q^2)$. Then $|\pi \cap S| \leq \delta \theta_{n-1}(q^2)$.

Proof. The proof is a generalisation of the proof of [8, Lemma 41].

Denote $x = |\pi \cap S|$ and let P be a point in $\pi \cap S$. Then $P^\sigma \cap \mathcal{H}(2n+1,q^2)$ is a cone with vertex P. Let $H' \cong \mathcal{H}(2n-1,q^2)$ be a base of this cone and consider the projection from P onto H'. Denote the projection of $S \cap P^\sigma$ by S'. The projection of π is a generator π' of H'. Note that S' is a blocking set of the generators on H'.

By [6, Lemma 10], we know there are q^{n^2} generators in H' that are skew to π', of which $q^{(n-1)^2}$ pass through a fixed point of $H' \setminus \pi'$. Hence, the blocking set S' contains at least q^{2n-1} points not in π'. Counting the tuples (P,Q), $P \in \pi \cap S$, $Q \in S \setminus \pi$, with $PQ \subset \mathcal{H}(2n+1,q^2)$, in two ways we find

$$xq^{2n-1} \leq \delta q^{2n-1}\theta_{n-1}(q^2),$$

where the upper bound follows from the fact that every point $Q \in S \setminus \pi$ is collinear with the points of an $(n-1)$-space in π and not with the other points in π. The theorem follows immediately. $\square$

Note that the size of a blocking set on a Hermitian variety $\mathcal{H}(2n+1,q^2)$ is at least the size of an ovoid, hence at least $q^{2n+1} + 1$.

Recall that the symmetric difference $A\Delta B$ of two sets A and B is the set $(A \cup B) \setminus (A \cap B)$.

Lemma 4.5. Let p be a fixed prime and denote $q = p^h$, $h \in \mathbb{N}$. Let $c \in C_n(\mathcal{H}(2n+1, q^2))^\perp$ be a code word with $\mathrm{wt}(c) \leq w = \delta q^{2n-1}$, $\delta > 0$ a constant, and denote $\mathrm{supp}(c) = S$. Denote $\mathcal{H}(2n+1, q^2)$ by H and let σ be the polarity related to H. Then a constant $C_n > 0$, a value $Q > 0$ and an n-space π can be found such that $|(\pi \Delta \pi^\sigma) \cap S| > C_n q^{2n-1}$ and such that $\frac{p-1}{p}|(\pi \Delta \pi^\sigma) \cap H| < \Sigma_{n,i} - C_n q^{2n-1}$, if $q \geq Q$. Hereby, i is such that $\pi \cap H$ is a cone with an i-dimensional vertex and $i \leq n-2$.

Proof. We introduce the notion of a *semi-arc*. A semi-arc $\mathcal{A}$ is a set of $k \geq n$ points in $\mathrm{PG}(2n+1, q^2)$ such that no $n+1$ points of $\mathcal{A}$ are contained in an $(n-1)$-space. We make two remarks about these semi-arcs. First, if $|S| > \binom{k}{n}\theta_{n-1}(q^2)$, then S contains a semi-arc with $k+1$ points, since it is possible to construct the semi-arc point by point: we start with a set of n linearly independent points in S and we extend the semi-arc point by point until we have $k+1$ points, which is possible by the condition on S. Secondly, if we choose K points $\{P_1, \dots, P_K\}$ in a semi-arc $\mathcal{A} \subseteq S$, then

$$\sum_{\{i\} \in S_{K,1}} |P_i^\sigma \cap S| - \sum_{\{i,j\} \in S_{K,2}} |P_i^\sigma \cap P_j^\sigma \cap S| + \dots$$
$$+ \sum_{\{i_1, \dots, i_{2l+1}\} \in S_{K,2l+1}} |P_{i_1}^\sigma \cap P_{i_2}^\sigma \cap \dots \cap P_{i_{2l+1}}^\sigma \cap S| \geq |(P_1^\sigma \cup P_2^\sigma \cup \dots \cup P_K^\sigma) \cap S|, \quad (1)$$

since every point of $(P_1^\sigma \cup P_2^\sigma \cup \dots \cup P_K^\sigma) \cap S$ is counted at least once on the left hand side. Also

$$\sum_{\{i\} \in S_{K,1}} |P_i^\sigma \cap S| - \sum_{\{i,j\} \in S_{K,2}} |P_i^\sigma \cap P_j^\sigma \cap S| + \dots$$
$$- \sum_{\{i_1, \dots, i_{2l}\} \in S_{K,2l}} |P_{i_1}^\sigma \cap P_{i_2}^\sigma \cap \dots \cap P_{i_{2l}}^\sigma \cap S| \leq |(P_1^\sigma \cup P_2^\sigma \cup \dots \cup P_K^\sigma) \cap S|, \quad (2)$$

since every point of $(P_1^\sigma \cup P_2^\sigma \cup \dots \cup P_K^\sigma) \cap S$ is counted at most once on the left hand side. In both expressions we denoted the set of all subsets of $\{1, \dots, K\}$ of size j by $S_{K,j}$.

Now, we prove using induction, for every $0 \leq t \leq n$, that we can find for any $(t+1)$-tuple $(c_0, \dots, c_t)$, $c_j > 0$ a constant (independent of q), a constant $K_t \in \mathbb{N}$ such that

$$\forall K \geq K_t, \forall \{P_1, \dots, P_K\} \subseteq \mathcal{A} \subseteq S : \sum_{\{i_0, \dots, i_t\} \in S_{K,t+1}} |P_{i_0}^\sigma \cap P_{i_1}^\sigma \cap \dots \cap P_{i_t}^\sigma \cap S| \geq c_t q^{2n-1}.$$

We consider the case $t = 0$, the induction base. Let $\{P_1, \dots, P_K\}$ be a set of points in $\mathcal{A} \subseteq S$ (without restriction on K). By Theorem 4.3, we know

$$\sum_{i=1}^{K} |P_i^\sigma \cap S| \geq K q^{2n-1}.$$

Hence, it is sufficient to choose $K_0 = \lceil c_0 \rceil$.

Next, we prove the induction step. We distinguish between two cases: t even and t odd. We look at the former, so we assume the inequality to be proven for $t \leq 2l - 1$ and we prove it for $t = 2l$. Let K_m be the constant arising from the $(m+1)$-tuple $(c_0, \dots, c_m)$, $m < 2l$, and let $\{P_1, \dots, P_K\}$ be a set of points in $\mathcal{A} \subseteq S$ with $K \geq K_{2l-1}$. By (1), we know that

$$\sum_{\{i\} \in S_{K,1}} |P_i^\sigma \cap S| - \sum_{\{i,j\} \in S_{K,2}} |P_i^\sigma \cap P_j^\sigma \cap S| + \dots$$
$$+ \sum_{\{i_0, \dots, i_{2l}\} \in S_{K,2l+1}} |P_{i_0}^\sigma \cap P_{i_1}^\sigma \cap \dots \cap P_{i_{2l}}^\sigma \cap S| \geq |(P_1^\sigma \cup P_2^\sigma \cup \dots \cup P_K^\sigma) \cap S|.$$

9

Using the induction hypothesis and Theorem 4.3, we find

$$\sum_{\{i_0,\ldots,i_{2l}\}\in S_{K,2l+1}} |P_{i_0}^\sigma \cap P_{i_1}^\sigma \cap \cdots \cap P_{i_{2l}}^\sigma \cap S| \geq \frac{\binom{K}{K_{2l-1}}}{\binom{K-2l}{K_{2l-1}-2l}}c_{2l-1}q^{2n-1} + \frac{\binom{K}{K_{2l-3}}}{\binom{K-2l+2}{K_{2l-3}-2l+2}}c_{2l-3}q^{2n-1}$$

$$+ \cdots + \frac{\binom{K}{K_1}}{\binom{K-2}{K_1-2}}c_1 q^{2n-1}$$

$$- \left[\binom{K}{2l-1} + \binom{K}{2l-3} + \cdots + K\right]\delta q^{2n-1}$$

$$+ q^{2n-1}$$

and thus

$$\sum_{\{i_0,\ldots,i_{2l}\}\in S_{K,2l+1}} |P_{i_0}^\sigma \cap P_{i_1}^\sigma \cap \cdots \cap P_{i_{2l}}^\sigma \cap S|$$

$$\geq \frac{\binom{K}{2l}}{\binom{K_{2l-1}}{2l}}c_{2l-1}q^{2n-1} + \frac{\binom{K}{2l-2}}{\binom{K_{2l-3}}{2l-2}}c_{2l-3}q^{2n-1} + \cdots + \frac{\binom{K}{2}}{\binom{K_1}{2}}c_1 q^{2n-1}$$

$$- \left[\binom{K}{2l-1} + \binom{K}{2l-3} + \cdots + K\right]\delta q^{2n-1} + q^{2n-1}$$

$$= q^{2n-1}f(K,\delta,l,K_1,K_3,\ldots,K_{2l-1},c_1,c_3,\ldots,c_{2l-1}).$$

Note that $\frac{\binom{K}{K_{2i-1}}}{\binom{K-2i}{K_{2i-1}-2i}} = \frac{\binom{K}{2i}}{\binom{K_{2i-1}}{2i}}$. We now study the function f, which is clearly independent of q.

Considering f as a function of K and comparing the exponents, we see that the term $\frac{\binom{K}{2l}}{\binom{K_{2l-1}}{2l}}c_{2l-1}$ dominates the others. Hence, we can find a value $K_{2l} \geq K_{2l-1}$ such that the right hand side is at least $c_{2l}q^{2n-1}$ for all $K \geq K_{2l}$, with c_{2l} as chosen above. Then the statement follows. Note that K_{2l} depends on the parameters $l, c_1, \ldots, c_{2l}$ chosen before (the values K_i, $0 \leq i < 2l$, depend themselves on $i, c_1, \ldots, c_i$).

For the latter case, t odd, the argument is similar, in this case starting from (2).

We will now apply the previous result for $t = n$. In order to do this, we need a semi-arc containing at least K_n points. We argued in the beginning of the proof that $\delta q^{2n-1} = |S| > \binom{K_n-1}{n}\theta_{n-1}(q^2)$ is a sufficient condition. Since K_n is a constant, independent of q, and $\theta_{n-1}(q^2) = q^{2n-2} + q^{2n-4} + \cdots + q^2 + 1$, we can find $Q_1' > 0$ such that this inequality is true for all $q \geq Q_1'$. Then we know

$$\sum_{\{i_0,\ldots,i_n\}\in S_{K_n,n+1}} |P_{i_0}^\sigma \cap P_{i_1}^\sigma \cap \cdots \cap P_{i_n}^\sigma \cap S| \geq c_n q^{2n-1}$$

for the points $\{P_1, P_2, \ldots, P_{K_n}\}$ defining a semi-arc in S. Hence, we can find $n+1$ points - without loss of generality the points $\{P_1, \ldots, P_{n+1}\}$ - such that

$$|P_1^\sigma \cap P_2^\sigma \cap \cdots \cap P_{n+1}^\sigma \cap S| \geq \frac{c_n}{\binom{K_n}{n+1}}q^{2n-1}.$$

We can find a constant $\overline{K} > 0$ and a value $Q' \geq Q_1'$ such that $\frac{c_n}{\binom{K_n}{n+1}}q^{2n-1} \geq \overline{K}q^{2n-1} + \theta_{n-2}(q^2)$ for $q \geq Q'$. We write $C_n = \overline{K} - \epsilon$, $\max\{0, \overline{K} - \frac{2}{p}\} < \epsilon < \overline{K}$, and we denote the n-space $P_1^\sigma \cap P_2^\sigma \cap \cdots \cap P_{n+1}^\sigma$ by π. Note that π is an n-space since the points $P_1, P_2, \ldots, P_{n+1}$ belong to a semi-arc. Then $|\pi \cap S| > C_n q^{2n-1} + \theta_{n-2}(q^2)$.

We know the intersection $\pi \cap H$ can be written as $\pi_i H_{n-i-1}$, with $H_{n-i-1} \cong \mathcal{H}(n-i-1, q^2)$ and π_i an i-space, $-1 \leq i \leq n$. Let $Q'' \geq Q'$ be such that $C_n q^{2n-1} + \theta_{n-2}(q^2) > \delta\theta_{n-1}(q^2)$ for all $q \geq Q''$. Such a value exists since the first term on the left hand side dominates the right hand

side. If $i \geq n - 1$, then $\pi \cap H$ is contained in a generator of H. Thus, using Lemma 4.4 and the assumption $q \geq Q''$ we find a contradiction. Hence, $i \leq n - 2$. We find:

$$|(\pi \Delta \pi^\sigma) \cap S| \geq |(\pi \setminus \pi_i) \cap S| \geq C_n q^{2n-1} + \theta_{n-2}(q^2) - \theta_i(q^2) \geq C_n q^{2n-1} .$$

We still need to check the second claim in the statement of the lemma: $\frac{p-1}{p}|(\pi \Delta \pi^\sigma) \cap H| < \Sigma_{n,i} - C_n q^{2n-1}$. Looking at the terms of highest degree in $\Sigma_{n,i} - C_n q^{2n-1} - \frac{p-1}{p}|(\pi \Delta \pi^\sigma) \cap H|$, we find $2 - C_n - 2\frac{p-1}{p} = \epsilon - \frac{c_n}{\binom{K_n}{n+1}} + \frac{2}{p} > 0$. Hence, we can find $Q \geq Q''$ such that the inequality $\frac{p-1}{p}|(\pi \Delta \pi^\sigma) \cap H| < \Sigma_{n,i} - C_n q^{2n-1}$ holds for all $q \geq Q$. $\qquad\square$

In this proof $\frac{c_n}{\binom{K_n}{n+1}}$ depends also on the choice of $c_0, \ldots, c_{n-1}$. So, investigating the possible values for $c_0, \ldots, c_n$, we can find many different values for C_n. With each of these values, a value Q corresponds. We pick one of the possible values for C_n. By investigating different possibilities for C_n, we can see there is a trade-off between the choice of C_n and the corresponding value Q.

From now on, we consider C_n and the corresponding value Q to be fixed.

Lemma 4.6. Let $c \in C_n(\mathcal{H}(2n+1, q^2))^\perp$ be a code word with $\mathrm{wt}(c) \leq w = \delta q^{2n-1}$, $\delta > 0$ a constant, and denote $\mathrm{supp}(c) = S$. Consider $H \cong \mathcal{H}(2n+1, q^2)$. Let π be an n-space such that $\pi \cap H$ is a cone $\pi_i H_{n-i-1}$ with $H_{n-i-1} \cong \mathcal{H}(n-i-1, q^2)$. Assume that $|S \cap (\pi \setminus \pi_i)| = x$ and $|S \cap (\pi^\sigma \setminus \pi_i)| = t$. Then there exists a value $Q_{n,i} \geq 0$ such that $x + t \leq C_n q^{2n-1}$ or $x + t \geq \Sigma_{n,i} - C_n q^{2n-1}$ if $q \geq Q_{n,i}$.

Proof. Let P be a point of $S \cap (\pi \setminus \pi_i)$ and let P' be a point of $((\pi^\sigma \cap H) \setminus \pi_i) \setminus S$ and denote $\ell = PP'$. By Lemma 3.7 we know the number $N(n, i)$ of generators through ℓ intersecting π and π^σ in precisely one point, namely P and P'. Each of these generators contains an additional point of S. Let R be a point of $H \setminus (\pi \cup \pi^\sigma)$. By Lemma 3.8 we know the number $n_R(n, i)$ of generators through R intersecting both π and π^σ in a point. Hence, $S \setminus (\pi \cup \pi^\sigma)$ contains at least

$$x(|(\pi^\sigma \cap H) \setminus \pi_i| - t)\frac{N(n, i)}{n_{\max}(n, i)} = x(q^{2i+2}\mu_{n-i-1}(q^2) - t)\frac{N(n, i)}{n_{\max}(n, i)}$$

points, whereby $n_{\max}(n, i) = \max_{R \in S \setminus (\pi \cup \pi^\sigma)} n_R(n, i)$. Switching the roles of π and π^σ, and adding these two inequalities, we find after dividing by two

$$x(q^{2i+2}\mu_{n-i-1}(q^2) - t)\frac{N(n, i)}{2n_{\max}(n, i)} + t(q^{2i+2}\mu_{n-i-1}(q^2) - x)\frac{N(n, i)}{2n_{\max}(n, i)} + x + t \leq |S| \leq w .$$

Rewriting this inequality yields

$$(x + t)\left(q^{2i+2}\mu_{n-i-1}(q^2)N(n, i) + 2n_{\max}(n, i)\right) - 2xtN(n, i) \leq 2w\, n_{\max}(n, i) .$$

Using the inequality $2xt \leq \frac{1}{2}(x + t)^2$ and writing $y = x + t$, we find

$$\frac{1}{2}y^2 N(n, i) - \left[q^{2i+2}\mu_{n-i-1}(q^2)N(n, i) + 2n_{\max}(n, i)\right]y + 2w\, n_{\max}(n, i) \geq 0 .$$

We now distinguish between two cases: $n - i$ odd and $n - i$ even. First we look at the former. By detailed analysis one can see that in this case

$$N(n-1, i)q^{4i+4}\left(\mu_{n-i-2}(q^2)\right)^2$$
$$\geq N(n-1, i-1)q^{4i}\left(\mu_{n-i-1}(q^2)\right)^2$$
$$\geq N(n-1, i+1)q^{4i+4}\mu_{n-i-3}(q^2)\left[q^4\mu_{n-i-3}(q^2) + q^2 - 1\right]$$

if $n - i > 3$ and

$$N(n-1, n-3)q^{4n-8}(q+1)^2 \geq N(n-1, n-4)q^{4n-12}\left(q^3 + 1\right)^2 \geq N(n, n-3)q^{2n-4} .$$

These inequalities correspond to $i = n - 3$. Hence, $n_{\max}(n, i) = N(n - 1, i)q^{4i+4}\left(\mu_{n-i-2}(q^2)\right)^2$. Using the formula for $N(n, i)$ from Lemma 3.7, and simplifying, we can rewrite this inequality as

$$\frac{1}{2}q^{n-3i-5}y^2 - \left[q^{n-i-3}\mu_{n-i-1}(q^2) + 2\mu_{n-i-2}(q^2)\frac{q^{n-i-1}-1}{q^2-1}\right]y$$
$$+ 2\delta q^{2n-1}\mu_{n-i-2}(q^2)\frac{q^{n-i-1}-1}{q^2-1} \geq 0 . \quad (3)$$

Let $\alpha_{n,i}(q^2)$ and $\alpha'_{n,i}(q^2)$ be the two solutions of the corresponding equation, with $\alpha_{n,i}(q^2) \leq \alpha'_{n,i}(q^2)$. Then $x + t \leq \alpha_{n,i}(q^2)$ or $x + t \geq \alpha'_{n,i}(q^2)$. Moreover,

$$\alpha_{n,i}(q^2) + \alpha'_{n,i}(q^2) = 2q^{2i+2}\mu_{n-i-1}(q^2) + 4\frac{\mu_{n-i-2}(q^2)(q^{n-i-1}-1)}{q^{n-3i-5}(q^2-1)} = \Sigma_{n,i} .$$

For the given δ we calculate

$$\overline{\alpha_{n,i}} = \lim_{q\to\infty} \alpha_{n,i}(q^2) = \lim_{q\to\infty} \frac{B' - \sqrt{B'^2 - 4\delta q^{3n-3i-6}C'}}{q^{n-3i-5}} ,$$

with

$$B' = q^{n-i-3}\mu_{n-i-1}(q^2) + 2\mu_{n-i-2}(q^2)\frac{q^{n-i-1}-1}{q^2-1} ,$$
$$C' = \mu_{n-i-2}(q^2)\frac{q^{n-i-1}-1}{q^2-1} .$$

Since $\overline{\alpha_{n,i}} \in O(q^{2n-2})$, we can find $Q_{n,i} > 0$ such that $\alpha_{n,i}(q^2) \leq C_n q^{2n-1}$ for $q \geq Q_{n,i}$.

In the latter case, $n - i$ even, similar arguments can be used. However, in this case we need to distinguish between $n - i > 2$ and $i = n - 2$. First, we discuss $n - i > 2$. We can deduce that

$$N(n - 1, i)q^{4i+4}\left(\mu_{n-i-2}(q^2)\right)^2$$
$$\leq N(n - 1, i - 1)q^{4i}\left(\mu_{n-i-1}(q^2)\right)^2$$
$$\leq N(n - 1, i + 1)q^{4i+4}\mu_{n-i-3}(q^2)\left[q^4\mu_{n-i-3}(q^2) + q^2 - 1\right] ,$$

hence $n_{\max}(n, i) = N(n - 1, i + 1)q^{4i+4}\mu_{n-i-3}(q^2)\left[q^4\mu_{n-i-3}(q^2) + q^2 - 1\right]$. We find the inequality

$$\frac{q^2 - 1}{2}y^2 - q^{2i+2}\left[\mu_{n-i-1}(q^2)(q^2 - 1) + 2(q^4\mu_{n-i-3}(q^2) + q^2 - 1)\right]y$$
$$+ 2\delta q^{2n-1}q^{2i+2}(q^4\mu_{n-i-3}(q^2) + q^2 - 1) \geq 0 . \quad (4)$$

Just as in the previous case, we define $\Sigma_{n,i}$, which is the sum of the solutions of the corresponding equation, and $\overline{\alpha_{n,i}}$:

$$\Sigma_{n,i} = 2q^{2i+2}\left[\mu_{n-i-1}(q^2) + 2\frac{q^4\mu_{n-i-3}(q^2) + q^2 - 1}{q^2 - 1}\right] ,$$
$$\overline{\alpha_{n,i}} = \lim_{q\to\infty} \frac{B'' - \sqrt{B''^2 - 4\delta q^{2n-1}(q^2 - 1)C''}}{q^2 - 1} ,$$

with

$$B'' = q^{2i+2}\left[\mu_{n-i-1}(q^2)(q^2 - 1) + 2(q^4\mu_{n-i-3}(q^2) + q^2 - 1)\right] ,$$
$$C'' = q^{2i+2}(q^4\mu_{n-i-3}(q^2) + q^2 - 1) .$$

Since $\overline{\alpha_{n,i}} \in O(q^{2n-2})$ also holds in this case, we again can find $Q_{n,i} > 0$ such that $\alpha_{n,i}(q^2) \leq C_n q^{2n-1}$ for $q \geq Q_{n,i}$.

Finally, we consider the case $i = n - 2$. The second possibility in Lemma 3.8 can thus not occur. We note that

$$N(n-1, n-3)q^{4(n-2)}(q+1)^2 \leq q^{2n-2}N(n, n-2).$$

The arguments in this case are analogous.

Hence, in all cases we can find $Q_{n,i} > 0$ such that $x + t \leq C_n q^{2n-1}$ or $x + t \geq \Sigma_{n,i} - C_n q^{2n-1}$ for $q \geq Q_{n,i}$. $\qquad\square$

Using the three previous lemmas, we can now prove a classification theorem for the small weight code words in $C_n(\mathcal{H}(2n+1, q^2))^\perp$.

Theorem 4.7. Let p be a fixed prime, $\delta > 0$ be a fixed constant and n be a fixed positive integer. Then there is a constant $\overline{Q}$ such that, for any $q = p^h$ with $h \in \mathbb{N}$ and $q \geq \overline{Q}$, and any $c \in C_n(\mathcal{H}(2n+1, q^2))^\perp$ with $\mathrm{wt}(c) \leq w = \delta q^{2n-1}$, c is a linear combination of code words described in Theorem 2.4.

Proof. For the given values p and δ we have found a set of possible C_n-values, of which we have chosen one, in Lemma 4.5, with Q, a power of p, corresponding to it. By the proof of this lemma, we know that $C_n q^{2n-1} > \delta\theta_{n-1}(q^2)$ for all $q \geq Q$. Define $\overline{Q} = \max(\{Q\} \cup \{Q_{n,i} \mid -1 \leq i \leq n-2\})$, with $Q_{n,i}$ as in Lemma 4.6, corresponding to the chosen value C_n. We assume $q \geq \overline{Q}$.

Denote $\mathrm{supp}(c) = S$. By Lemma 4.5, we find an n-space π such that $N := |(\pi\Delta\pi^\sigma) \cap S| > C_n q^{2n-1}$. The intersection $\pi \cap H$ can be written as $\pi_i H_{n-i-1}$, with $H_{n-i-1} \cong \mathcal{H}(n-i-1, q^2)$, $-1 \leq i \leq n-2$.

Since $N > C_n q^{2n-1}$ and $q \geq Q_{n,i}$, we know by Lemma 4.6 that $N \geq \Sigma_{n,i} - C_n q^{2n-1}$. For each element $\alpha \in \mathbb{F}_p^*$, we denote by N_α the sum of the number of points $P \in \pi$ such that $c_P = \alpha$ and the number of points $Q \in \pi^\sigma$ such that $c_Q = -\alpha$. We can find $\beta \in \mathbb{F}_p^*$ such that $N_\beta \geq \frac{N}{p-1}$. We now consider the code word $c' = c - \beta(v_\pi - v_{\pi^\sigma})$, with v_π and v_{π^σ} as in Theorem 2.4. We know

$$\mathrm{wt}(c') = (N - N_\beta) + (|(\pi\Delta\pi^\sigma) \cap H| - N) = |(\pi\Delta\pi^\sigma) \cap H| - N_\beta \leq |(\pi\Delta\pi^\sigma) \cap H| - \frac{N}{p-1}.$$

We also know that $N \geq \Sigma_{n,i} - C_n q^{2n-1} > \frac{p-1}{p}|(\pi\Delta\pi^\sigma) \cap H|$ by Lemma 4.5. It follows that

$$\mathrm{wt}(c') < \frac{p}{p-1}N - \frac{N}{p-1} = N \leq \mathrm{wt}(c).$$

Hence, the theorem follows using induction on $w = \mathrm{wt}(c)$. $\qquad\square$

We now focus on the code words that we described in Section 2.

Remark 4.8. Let c be a small weight code word and q sufficiently large. Following the arguments in the proof of Theorem 4.7, we know that $c = c_1 + \cdots + c_m$, with c_i, $1 \leq i \leq m$, a code word that we described in Theorem 2.4 and Example 2.5, such that $\mathrm{wt}(c_1 + \cdots + c_{m'}) < \mathrm{wt}(c_1 + \cdots + c_{m'+1})$ for all $1 \leq m' \leq m$. From this observation, it immediately follows that the code words that we described in Theorem 2.4 and Example 2.5 are the code words of smallest weights.

Now we consider small weight code words different from the ones described in Theorem 2.4. Let c be a code word c of weight smaller than $4q^{2n-1}$, q sufficiently large. Since c is not of the type we described in Theorem 2.4, c can be written as a linear combination of at least two of these code words. By the above arguments, we can find a code word c' which is a linear combination of precisely two of these code words, such that $\mathrm{wt}(c') \leq \mathrm{wt}(c)$. In particular, we can find $\alpha, \alpha' \in \mathbb{F}_p^*$ and n-spaces π, π', $\pi \notin \{\pi', \pi'^\sigma\}$, such that $c' = \alpha(v_\pi - v_{\pi^\sigma}) + \alpha'(v_{\pi'} - v_{\pi'^\sigma})$ and $\mathrm{wt}(c') < 4q^{2n-1}$. Let S be the support of c'. We know $S \subseteq ((\pi\Delta\pi^\sigma) \cup (\pi'\Delta\pi'^\sigma)) \cap \mathcal{H}(2n+1, q^2)$. However, it can be seen that $|(\pi\Delta\pi^\sigma) \cap (\pi'\Delta\pi'^\sigma)| \leq 4q^{2n-2}$. Hence,

$$|S| \geq \mathrm{wt}(\alpha(v_\pi - v_{\pi^\sigma})) + \mathrm{wt}(\alpha'(v_{\pi'} - v_{\pi'^\sigma})) - |(\pi\Delta\pi^\sigma) \cap (\pi'\Delta\pi'^\sigma)| \geq 4q^{2n-1},$$

13

a contradiction. It follows that the only code words of weight smaller than $4q^{2n-1}$ are of the type described in Theorem 2.4.

Note that Theorem 4.7 only proves the second half of Theorem 1.8. From Remark 4.8 now the first half also follows.

References

[1] E.F. Assmus and J.D. Key. Designs and their Codes. *Cambridge Tracts in Mathematics*, vol. 103, Cambridge University Press, Cambridge, 1992.

[2] S.V. Droms, K.E. Mellinger and C. Meyer. LDPC codes generated by conics in the classical projective plane. *Des. Codes Cryptogr.*, 40(3): 343–356, 2006.

[3] Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck and V.D. Tonchev. Entanglement-assisted quantum low-density parity-check codes. *Phys. Rev. A* 82(4): 042338, 2010.

[4] J.W.P. Hirschfeld and J.A. Thas. General Galois Geometries. *Oxford Mathematical Monographs*, Oxford University Press, Oxford, 1991.

[5] J.-L. Kim, K. Mellinger and L. Storme. Small weight codewords in LDPC codes defined by (dual) classical generalised quadrangles. *Des. Codes Cryptogr.*, 42(1): 73–92, 2007.

[6] A. Klein, K. Metsch and L. Storme. Small maximal partial spreads in classical finite polar spaces. *Adv. Geom.*, 10(3): 379–402, 2010.

[7] M. Lavrauw, L. Storme and G. Van de Voorde. Linear codes from projective spaces. *Error-Correcting Codes, Finite Geometries, and Cryptography*. A.A. Bruen and D.L. Wehlau, editors. *AMS Contemporary Mathematics (CONM) book series*, vol. 523, 185–202, 2010.

[8] V. Pepe, L. Storme and G. Van de Voorde. On codewords in the dual code of classical generalised quadrangles and classical polar spaces. *Discrete Math.*, 310(22): 3132–3148, 2010.

[9] P. Vandendriessche. Some low-density parity-check codes derived from finite geometries. *Des. Codes. Cryptogr.*, 54: 287–297, 2010.

[10] P. Vandendriessche. LDPC codes associated with linear representations of geometries. *Adv. Math. Commun.*, 4: 405–417, 2010.