# Counting Configurations of Vectors in a Finite Vector Space with an Orthogonal, Symplectic or Unitary Geometry

M. Q. Rieck

**Abstract**

Given a finite-dimensional vector space $V$ over a finite field $F$ of odd characteristic, and equipping $V$ with an orthogonal (symplectic, unitary) geometry, the following two questions are considered:

1. Given some linearly independent vectors $w_1, w_2, ..., w_k \in V$ and the $k \times k$ matrix $\Lambda = (\langle w_i, w_j \rangle)$, and given scalars $\alpha_1, \alpha_2, ..., \alpha_k$, $\beta \in F$, how many vectors $v \in V$, not in the linear span of $w_1, w_2, ..., w_k$, satisfy $\langle w_i, v \rangle = \alpha_i$ $(i = 1, 2, ..., k)$ and $\langle v, v \rangle = \beta$?
2. Given a $k \times k$ matrix $\Lambda = (\lambda_{ij})$ with entries from $F$, how many $k$-tuples $(v_1, v_2, ..., v_k)$ of linearly independent vectors from $V$ satisfy $\langle v_i, v_j \rangle = \lambda_{ij}$ $(i, j = 1, 2, ..., k)$?

An exact answer to the first question is derived. Here there are two cases to consider, depending on whether or not the column vector $(\alpha_i)$ is in the column space of $\Lambda$. This result can then be applied iteratively to address the second question.

Key words: finite vector space, orthogonal (symplectic, unitary) geometry, totally isotropic subspace, pseudo-orthogonal complement.
AMS 1991 subject classification: primary 11E39, 15A63; secondary 15A33.

# 1 Introduction

The purpose of this paper is to derive formulas which allow one to rapidly compute the number of configurations of $k$ vectors in a finite vector space $V$, equipped with an orthogonal (symplectic, unitary) geometry, where these vectors are required to have some given relationships with respect to the geometry on $V$. The computation involves solving a certain system of linear equations, as well as diagonalizing the coefficient matrix of this system with respect to matrix congruence. Researchers involved with finite vector spaces might find it worthwhile to incorporate these methods in a symbolic manipulation software package dealing with linear algebra over finite fields.

In the following discussion, attention will be restricted to the case where the field of scalars $F$ is a Galois field $GF(q)$ with $q$ odd. $V$ will be an $n$-dimensional $F$-vector space. A nondegenerate bilinear or sesquilinear form $\langle \cdot , \cdot \rangle$ will be fixed on $V$, and it is assumed that this is one of the three classical types (symmetric, alternating, hermitian), inducing one of the three classical geometries (orthogonal, symplectic, unitary) on $V$. Two related questions will be addressed:

1. Given some linearly independent vectors $w_1, w_2, ..., w_k \in V$ and the $k \times k$ matrix $\Lambda = (\langle w_i, w_j \rangle)$, and given scalars $\alpha_1, \alpha_2, ..., \alpha_k, \beta \in F$, how many vectors $v \in V$, not in the linear span of $w_1, w_2, ..., w_k$, satisfy $\langle w_i, v \rangle = \alpha_i$ $(i = 1, 2, ..., k)$ and $\langle v, v \rangle = \beta$?

2. Given a $k \times k$ matrix $\Lambda = (\lambda_{ij})$ with entries from $F$, how many $k$-tuples $(v_1, v_2, ..., v_k)$ of linearly independent vectors from $V$ satisfy $\langle v_i, v_j \rangle = \lambda_{ij}$ $(i, j = 1, 2, ..., k)$?

We will make use of the following three parameters. Let $\epsilon = 1$ if the geometry is orthogonal or unitary, and let $\epsilon = -1$ if the geometry is symplectic. Let $g = 0, \frac{1}{2}, 1$, respectively, in the symplectic, unitary, orthogonal case. Let $d$ be the (Witt) index of the form $\langle \cdot , \cdot \rangle$. That is, $d$ is the dimension of any maximal subspace on which the form vanishes identically. Subspaces on which the form vanishes identically are called *totally isotropic subspaces*. Subspaces on which the form is nondegenerate are called *nondegenerate subspaces*.

Recall that in the case of unitary geometry, $q$ is necessarily a perfect square, and the form is sesquilinear with respect to the involution $\lambda \longmapsto \bar{\lambda} = \lambda^{\sqrt{q}}$ on $F$. In the other two cases, we will define $\bar{\lambda} = \lambda$ for all $\lambda \in F$. In all cases, $F_0$ will denote the fixed field of the automorphism $\lambda \longmapsto \bar{\lambda}$ on $F$.

## 2 Single vectors

Before considering the counting problems discussed in the introduction, it is necessary to determine the number of vectors $v \in V$ with a prescribed value of $\langle v, v\rangle$. This will be the goal of this section, although the results can also be found in the references cited here. Some (mostly nonstandard) definitions will be required.

DEFINITION. $\tau$ will identify the isometry type of the geometry given to $V$ by the form $\langle\cdot,\cdot\rangle$, as follows. Take $\tau$ to be the symbol "Sp" if the geometry is symplectic. Take $\tau$ to be the symbol "U" if the geometry is unitary. When the geometry is orthogonal and $n$ is even, take $\tau$ to be "O$^+$" if $n = 2d$, and take $\tau$ to be "O$^-$" if $n = 2d+2$. When the geometry is orthogonal and $n$ is odd, consider whether or not $V$ admits an orthogonal basis $\{e_1, e_2, ..., e_n\}$ such that $\langle e_i, e_i\rangle = 1$ when $i$ is odd, and $\langle e_i, e_i\rangle = -1$ when $i$ is even ($i = 1, 2, ..., n$). If such a basis exists, then take $\tau$ to be "O$^+$". Otherwise, take $\tau$ to be "O$^-$". It is known that $n$ and $\tau$ uniquely determine $V$ and $\langle\cdot,\cdot\rangle$ up to an isometry (*i.e.* up to an isomorphism which preserves the form).

DEFINITION. $F^*$ is the multiplicative group of $F$ (*i.e.* $F^* = F\backslash\{0\}$). $F^2$ is $\{\lambda^2 \mid \lambda \in F\}$. $F^{*2}$ is $F^* \cap F^2$. When the geometry is unitary, $F_0 = GF(\sqrt{q})$, and $F_0^*, F_0^2, F_0^{*2}$ have the evident meanings. $\delta_0$, $\delta_+$, $\delta_-$, $\chi$ will denote functions from $F$ to the ring of (rational) integers. They are defined as follows:

$$\delta_0(\lambda) = \begin{cases} 1 \text{ if } \lambda = 0 \\ 0 \text{ if } \lambda \neq 0, \end{cases} \qquad \delta_+(\lambda) = \begin{cases} 1 \text{ if } \lambda \in F^{*2} \\ 0 \text{ if } \lambda \notin F^{*2}, \end{cases}$$

$$\delta_-(\lambda) = \begin{cases} 1 \text{ if } \lambda \notin F^2 \\ 0 \text{ if } \lambda \in F^2, \end{cases} \qquad \chi(\lambda) = \delta_+(\lambda) - \delta_-(\lambda).$$

DEFINITION. $[n;\tau;q\,|\,\lambda]$ is defined to be the number of nonzero vectors $v \in V$ with $\langle v, v\rangle = \lambda$, where $\lambda \in F$.

The following result, which gives $[n;\tau;q\,|\,\lambda]$ explicitly, can be found already in the existing literature.

THEOREM 2.1. *Fix $\lambda \in F$. Then*

$$[n;\mathrm{Sp};q\,|\,\lambda] = \delta_0(\lambda)(q^n - 1);$$

$$[n;\mathrm{U};q\,|\,\lambda] = \begin{cases} q^{n-\frac{1}{2}} + (-1)^n\delta_0(\lambda)q^{\frac{n}{2}} - (-1)^n q^{\frac{n-1}{2}} - \delta_0(\lambda) & \\ \qquad = [q^{\frac{n}{2}} - (-1)^n][q^{\frac{n-1}{2}} + (-1)^n\delta_0(\lambda)] & \text{if } \lambda \in F_0, \\ 0 & \text{if } \lambda \notin F_0; \end{cases}$$

$$[n;\mathrm{O}^{\pm};q\,|\,\lambda] = \begin{cases} q^{n-1} \pm \chi(\lambda)q^{\frac{n-1}{2}} - \delta_0(\lambda) \\ \qquad = [q^{\frac{n-1}{2}} \pm \delta_+(\lambda) \pm \delta_0(\lambda)][q^{\frac{n-1}{2}} \mp \delta_-(\lambda) \mp \delta_0(\lambda)] \\ \qquad \text{if } n \text{ is odd,} \\ q^{n-1} \pm \delta_0(\lambda)q^{\frac{n}{2}} \mp q^{\frac{n}{2}-1} - \delta_0(\lambda) \\ \qquad = [q^{\frac{n}{2}} \mp 1][q^{\frac{n}{2}-1} \pm \delta_0(\lambda)] \\ \qquad \text{if } n \text{ is even.} \end{cases}$$

Proof. The symplectic case follows immediately. The orthogonal cases are dealt with in [5, Section 6.10]. (The $\mathrm{O}^+$ case with $n$ odd is handled by negating equation (66) in [5]. The $\mathrm{O}^-$ case with $n$ odd follows from the $\mathrm{O}^+$ case.) The unitary case with $\lambda = 0$ is dealt with in [2, Theorem 8.1]. The unitary case in general can be proved by the following induction argument. This proof can be adapted for the orthogonal cases as well.

Clearly $[n;\mathrm{U};q\,|\,\lambda] = 0$ if $\lambda \notin F_0$. Assume then that $\lambda \in F_0$. We will argue by induction on $n$. When $n = 1$, the claim is that $[n;\mathrm{U};q\,|\,\lambda] = (\sqrt{q}+1)(1-\delta_0(\lambda))$, which is correct. For general $n$, let $\#\left\{\sum_{i=1}^{n} x_i^{\sqrt{q}+1} = \lambda\right\}$ denote the number of solutions to the equation $\sum_{i=1}^{n} x_i^{\sqrt{q}+1} = \lambda$. Now with $n > 1$, assume as an induction hypothesis, that the theorem is true when $n$ is replaced by $n-1$. Observe that $V$ has an orthonormal basis (cf. [2, Theorem 4.1 and its corollary] and [6, Theorem 28]), and that the norm map $\lambda \mapsto \lambda^{\sqrt{q}+1}$ from $F$ to $F_0$ is onto, and is $(\sqrt{q}+1)$-to-1 when restricted to $F^*$. So,

$$[n;\mathrm{U};q\,|\,\lambda] + \delta_0(\lambda) = \#\left\{\sum_{i=1}^{n} x_i^{\sqrt{q}+1} = \lambda\right\} =$$

$$\#\left\{\sum_{i=1}^{n-1} x_i^{\sqrt{q}+1} = \lambda\right\} + (\sqrt{q}+1)\sum_{\rho\in F_0^*} \#\left\{\sum_{i=1}^{n-1} x_i^{\sqrt{q}+1} = \lambda - \rho\right\} =$$

$$q^{n-\frac{3}{2}} + (-1)^{n-1}\delta_0(\lambda)q^{\frac{n-1}{2}} - (-1)^{n-1}q^{\frac{n-2}{2}} +$$

$$(\sqrt{q}+1)\sum_{\rho\in F_0^*}\left[q^{n-\frac{3}{2}} + (-1)^{n-1}\delta_0(\lambda-\rho)q^{\frac{n-1}{2}} - (-1)^{n-1}q^{\frac{n-2}{2}}\right] =$$

$$[(1+(\sqrt{q}+1)(\sqrt{q}-1)][q^{n-\frac{3}{2}} + (-1)^n q^{\frac{n}{2}-1}] -$$

$$(-1)^n q^{\frac{n-1}{2}}[\delta_0(\lambda) + (\sqrt{q}+1)(1-\delta_0(\lambda))] =$$

$$q\left(q^{n-\frac{3}{2}} + (-1)^n q^{\frac{n}{2}-1}\right) - (-1)^n q^{\frac{n-1}{2}}\left[\sqrt{q}+1-\delta_0(\lambda)\sqrt{q}\right] =$$

$$q^{n-\frac{1}{2}} + (-1)^n\delta_0(\lambda)q^{\frac{n}{2}} - (-1)^n q^{\frac{n-1}{2}}. \qquad \square$$

# 3 Configurations of vectors

The following (known) lemma will be required in the proof of Theorem 3.2.

LEMMA 3.1. *If $U$ and $U'$ are both totally isotropic $m$-subspaces of $V$, and if $U + U'$ is nondegenerate, then for any basis $\{e_1, ..., e_m\}$ of $U$, there exists a unique basis $\{e'_1, ..., e'_m\}$ of $U'$ satisfying $\langle e_i, e'_j \rangle = \delta_{ij}$ for all $i, j = 1, 2, ..., m$.*

Proof. First, note that $U \cap U' = 0$. $U \oplus U'$ is nondegenerate and so, by dimensional reasoning, contains a vector $f_1 + e'_1$ ($f_1 \in U, e'_1 \in U'$) orthogonal to $span\{e_2, ..., e_m\}$ but not to $e_1$. Clearly the same claim can be made about the vector $e'_1$. By rescaling $e'_1$ if necessary it may be assumed that $\langle e_i, e'_1 \rangle = \delta_{i1}$. Likewise, for $j = 2, ..., m$, there exists $e'_j$ with $\langle e_i, e'_j \rangle = \delta_{ij}$. Now, $e'_1, ..., e'_m$ are linearly independent and together span $U'$. This shows the existence of the basis $\{e'_1, ..., e'_m\}$. The uniqueness follows easily from this. □

Another (known) result with many applications is the following generalization of Witt's Extension Theorem (cf. [5, Sections 6.5, 6.9, 6.11] and [4, Section 1.11]).

THEOREM 3.1. *Let $U$ and $U'$ be subspaces of $V$. Then any isometry from $U$ onto $U'$ can be extended to an isometry from $V$ onto $V$.*

The notation $[n; r; q \mid \lambda]$ will now be extended as follows. Fix some scalars $\alpha_1, \alpha_2, ..., \alpha_k, \beta \in F$. Let $\Lambda = (\lambda_{ij})$ be a $k \times k$ matrix with the property that there exist linearly independent vectors $w_1, w_2, ..., w_k \in V$ such that $\langle w_i, w_j \rangle = \lambda_{ij}$, for all $i, j = 1, 2, ..., k$. Let $r$ be the rank of $\Lambda$. In the orthogonal case, it is known that $\Lambda$ is congruent to a diagonal matrix whose only nonzero entries are the first $r$ entries of the diagonal, with all except possibly the first entry being ones (cf. [6, Theorem 11]). Let $\rho$ be the first diagonal entry of this diagonal matrix.

DEFINITION. The number of vectors $v \in V$, not contained in the linear span of $w_1, ..., w_k$, and satisfying the conditions $\langle v, v \rangle = \beta$ and $\langle w_i, v \rangle = \alpha_i$ ($i = 1, 2, ..., k$) will be denoted by

$$\left[\begin{array}{ccc|c} \multicolumn{3}{c|}{n\;;\;r\;;\;q} & \beta \\ \hline \lambda_{11} & \cdots & \lambda_{1k} & \alpha_1 \\ \vdots & & \vdots & \vdots \\ \lambda_{k1} & \cdots & \lambda_{kk} & \alpha_k \end{array}\right].$$

Notice that Theorem 3.1 assures that this definition is well-defined, in that it is independent of the particular vectors $w_1, ..., w_k$ used. We will now see how to compute these numbers. In the following, it will be supposed that $\beta = 0$ if $\tau = \mathrm{Sp}$, and that $\beta \in F_0$ if $\tau = \mathrm{U}$. The number sought is clearly zero in the cases which are contrary to this.

THEOREM 3.2. *Assume that $\beta = 0$ if $\tau = \mathrm{Sp}$, and that $\beta \in F_0$ if $\tau = \mathrm{U}$. Then*

$$\left[\begin{array}{ccc|c} & n\,;\,\tau\,;\,q & & \beta \\ \hline \lambda_{11} & \cdots & \lambda_{1k} & \alpha_1 \\ \vdots & & \vdots & \vdots \\ \lambda_{k1} & \cdots & \lambda_{kk} & \alpha_k \end{array}\right] =$$

$$\begin{cases} q^{k-r}\left[n-2k+r\,;\,\tau'\,;\,q \,\middle|\, \beta - \sum_{j=1}^{k} \alpha_j \overline{\gamma}_j\right] & \textit{if } \alpha_i = \sum_{j=1}^{k} \lambda_{ij}\gamma_j \\ & (i = 1, 2, ..., k), \\ q^{n-k-g} & \textit{if } \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{bmatrix} \textit{ is not in the} \\ & \textit{column space of } \Lambda, \end{cases}$$

*where the $\gamma_j$ are any scalars, and where $\tau' = \tau$, except possibly in the orthogonal case, where say $\tau = O^I$, and where $\tau' = O^J$ with $J =$*
$$\begin{cases} I\chi((-1)^{\lceil\frac{r}{2}\rceil}\rho) & \textit{if } n \textit{ is even,} \\ I\chi((-1)^{\lfloor\frac{r}{2}\rfloor}\rho) & \textit{if } n \textit{ is odd.} \end{cases}$$
*(Here "+" and "-" are identified with the integers 1 and -1, respectively.)*

Proof. Let $W = span\{w_1, ..., w_k\}$. Let $U = W^{\perp} = \{v \in V \mid \langle u, v\rangle = 0$ for all $u \in W\}$. Let $U'$ be a pseudo-orthogonal complement of $U$, which exists by [7, Corollary 2]. This means that $V = U \oplus U'$, and that $U \cap U'^{\perp}$ and $U' \cap U^{\perp}$ are maximal nondegenerate subspaces of $U$ and $U'$, respectively. Let $H = rad(U) \oplus rad(U')$, $M = U \cap U'^{\perp}$ and $M' = U' \cap W$. Then $V = H \oplus M \oplus M'$, an orthogonal direct sum of nondegenerate subspaces, by [7, Proposition 3]. Also, $U = rad(U) \oplus M, U' = rad(U') \oplus M'$ and $W = rad(U) \oplus M'$. Consider the linear map from $V = U \oplus U'$ to $F^k$ taking $v$ to $(\langle w_1, v\rangle, ..., \langle w_k, v\rangle)$. $U$ is the kernel of this map. Clearly there exists a unique $v_0 \in U'$ with $\langle w_i, v_0\rangle = \alpha_i\,(i = 1, 2, ..., k)$, and moreover, $v_0 + U$ consists of all the vectors $v$ for which $\langle w_i, v\rangle = \alpha_i\,(i = 1, 2, ..., k)$. We seek to count certain vectors contained in the coset $v_0 + U$. Write $v_0 = v_1 + v_2$, where $v_1 \in rad(U')$ and $v_2 \in M'$.

Let us establish the equivalence of the following three conditions:

(i) $v_1 = 0$ ,

(ii) $(v_0 + U) \cap W \neq \emptyset$ ,

(iii) $\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{bmatrix}$ is in the column space of $\Lambda$.

If (i) holds, then $v_0 \in W$ and so (ii) certainly holds. If (ii) holds, then there exists $u \in U$ with $v_0 + u \in W$. So $v_0 + u = w + z$, for some $w \in rad(U) = rad(W)$ and $z \in M'$. But then $v_0 - z = w - u \in U' \cap U = 0$. So $v_0 = z \in M'$. So (i) holds. This shows that (i) $\Leftrightarrow$ (ii). Now (ii) $\Leftrightarrow$ (iii) is straightforward to check, since the coset $v_0 + U$ consists of those vectors $v$ satisfying $\langle w_i, v\rangle = \alpha_i$ $(i = 1, ..., k)$. We now have two cases to consider.

Case 1: Suppose that $v_1 = 0$, so that $v_0 = v_2 \in M' \subseteq W$. Now $\langle v_0 + u, v_0 + u\rangle = \langle v_0, v_0\rangle + \langle u, u\rangle$, for all $u \in U$. We seek the number of $u \in U \backslash W$ such that $\langle u, u\rangle = \beta - \langle v_0, v_0\rangle$. Now write $v_0 = \sum_{i=1}^{k} \overline{\gamma}_i w_i$, for some scalars $\gamma_i$. Then $\alpha_i = \langle w_i, v_0\rangle = \sum_{j=1}^{k} \gamma_j \langle w_i, w_j\rangle = \sum_{j=1}^{k} \gamma_j \lambda_{ij}$. Also, $\langle v_0, v_0\rangle = \sum_{i,j} \overline{\gamma}_i \gamma_j \lambda_{ij} = \sum_{i=1}^{k} \overline{\gamma}_i \alpha_i$. So we seek the number of vectors $u \in U\backslash W$ with $\langle u, u\rangle = \beta - \sum_{i=1}^{k} \alpha_i \overline{\gamma}_i$. But $U \backslash W = U \backslash rad(U)$ and the number we seek is $|rad(U)|$ times the number of nonzero vectors $u \in M$ with $\langle u, u\rangle = \beta - \sum_{i=1}^{k} \alpha_i \overline{\gamma}_i$, which is just $q^{k-r} \left[ n - 2k + r; \tau'; q \,\middle|\, \beta - \sum_{i=1}^{k} \alpha_i \overline{\gamma}_i \right]$, where $\tau'$ is the type of geometry on the nondegenerate subspace $M$, inherited from that of $V$. (Notice that $W$ has dimension $k$, $rad(W) = rad(U)$ has dimension $k - r$, $U$ has dimension $n - k$ and $M$ has dimension $n - 2k + r$.) Clearly $\tau' = \tau$ when $\tau$ is either Sp or U.

When $\tau$ is $\text{O}^{\pm}$, the situation is not so clear, except that $M$ has an orthogonal geometry of course. So let us say then that $\tau$ is $\text{O}^{I}$ and $\tau'$ is $\text{O}^{J}$, where $I$ and $J$ may be "+" or "-". $W = M' \oplus rad(W)$ has an orthogonal basis $w_1', ..., w_k'$ such that $M' = span\{w_1', ..., w_r'\}$, $rad(W) = span\{w_{r+1}', ..., w_k'\}$, $\langle w_1', w_1'\rangle = \rho$, and $w_2', w_3', ..., w_r'$ are unit vectors (cf. [6, Theorem 11]). By Lemma 3.1, $rad(U')$ has a basis $u_1', ..., u_{k-r}'$ such that $\langle w_{r+i}', u_j'\rangle = \delta_{ij}$ $(i, j = 1, 2, ..., k - r)$. Now $M$ has an orthogonal basis $u_1, ..., u_{n-2k+r}$ with $u_2$, $u_3$, ..., $u_{n-2k+r}$ all unit vectors. Let $\omega = \langle u_1, u_1\rangle$.

Combining the selected bases for the various subspaces to form a basis for $V$. we see that the discriminant of $\langle \cdot, \cdot \rangle$ with respect to this basis is $\omega\rho(-1)^{k-r}$. This forces $\chi(\omega\rho(-1)^{k-r}) = I\chi((-1)^{\lfloor \frac{n}{2} \rfloor})$, since $V$ has a geometry of type $\mathrm{O}^I$. So $\chi(\omega) = I\chi((-1)^{\lfloor \frac{n}{2} \rfloor + k - r}\rho)$. But this must equal $J\chi((-1)^{\lfloor \frac{n-2k+r}{2} \rfloor})$, since $M$ has a geometry of type $\mathrm{O}^J$. From here, one can deduce that $I$ and $J$ are related as stated in the theorem. This concludes case 1.

Case 2: Here we suppose that $v_1 \neq 0$. So $v_0 \notin W$. There exists a basis $u_1, u_2, ..., u_{k-r}$ of $rad(U) = rad(W)$ with $\langle u_i, v_1 \rangle = \delta_{1i}$ $(i = 1, 2, ..., k-r)$. Consider some $u \in U$ and write $u = \sum_{i=1}^{k-r} \gamma_i u_i + z$, for scalars $\gamma_i$ and for $z \in M$. Then $\langle v_0 + u, v_0 + u \rangle = \langle v_1 + v_2 + \sum_{i=1}^{k-r} \gamma_i u_i + z, v_1 + v_2 + \sum_{i=1}^{k-r} \gamma_i u_i + z \rangle = \langle v_1 + \sum_{i=1}^{k-r} \gamma_i u_i, v_1 + \sum_{i=1}^{k-r} \gamma_i u_i \rangle + \langle v_2, v_2 \rangle + \langle z, z \rangle = \gamma_1 + \epsilon\overline{\gamma}_1 + \langle v_2, v_2 \rangle + \langle z, z \rangle$. We seek the number of $u$ for which this equals $\beta$. In the symplectic case, since $\langle v_0 + u, v_0 + u \rangle = 0 = \beta$, for all $u \in U$, we get a count of $|U| = q^{n-k} = q^{n-k-g}$. Next consider the orthogonal case. As $u$ ranges over all of $U$, $\gamma_1 + \epsilon\overline{\gamma}_1 = 2\gamma_1$ ranges uniformly over all of $F$. (For a fixed value of $z \in M$, but with $\gamma_1, ..., \gamma_k$ varying, we see that $\langle v_0 + u, v_0 + u \rangle$ varies uniformly over all of $F$. This is then still the case as $z$ is allowed to vary as well.) Hence, the number of $u \in U$ with $\langle v_0 + u, v_0 + u \rangle = \beta$ is equal to $\frac{1}{q}|U| = q^{n-k-1} = q^{n-k-g}$. Lastly, we consider the unitary case. Here $\langle v_0 + u, v_0 + u \rangle = \gamma_1 + \overline{\gamma}_1 + \langle v_2, v_2 \rangle + \langle z, z \rangle$. Now the trace map $\zeta \mapsto \zeta + \bar{\zeta}$ from $F$ to $F_0$ is $F_0$-linear and onto. So as $\gamma_1$ varies, $\gamma_1 + \overline{\gamma}_1$ varies uniformly over all of $F_0$. It follows, by reasoning as in the orthogonal case, that the number of $u \in U$ with $\langle v_0 + u, v_0 + u \rangle = \beta$ is $|U|/|F_0| = q^{n-k-\frac{1}{2}} = q^{n-k-g}$. This concludes case 2. □

The numbers discussed in Theorem 3.2 can be used to iteratively compute the following numbers.

Definition. Let $\Lambda = (\lambda_{ij})$ be a $k \times k$ matrix with entries taken from $F$. The number of $k$-tuples of vectors $(v_1, v_2, ..., v_k)$ from $V$ satisfying $\langle v_i, v_j \rangle = \lambda_{ij}$ $(i, j = 1, 2, ..., k)$ will be denoted by

$$\left[\begin{array}{ccc} & n\ ;\ r\ ;\ q & \\ \hline \lambda_{11} & \cdot\ \cdot\ \cdot & \lambda_{1k} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{k1} & \cdot\ \cdot\ \cdot & \lambda_{kk} \end{array}\right].$$

In order for this number to be nonzero, it is of course required that $\Lambda^T = \epsilon\overline{\Lambda}$. The next section provides an example, demonstrating how to compute the above number.

# 4 An example

Consider, as an example, the number

$$\left[\begin{array}{ccc} \multicolumn{3}{c}{4\,;\,O^{+}\,;\,7} \\ \hline 1 & 2 & 3 \\ 2 & 0 & 4 \\ 3 & 4 & 5 \end{array}\right].$$

In this count, three vectors are required to satisfy certain relationships with respect to an orthogonal geometry. To compute this number, simply select (subject to the restrictions) the vectors one at a time, in any order, and make use of Theorems 2.1 and 3.2. The following three computations of this number use different orderings for selecting the three vectors.

1.

$$[4;O^{+};7\,|\,1]\cdot\left[\begin{array}{c|c} 4\,;\,O^{+}\,;\,7 & 0 \\ \hline 1 & 2 \end{array}\right]\cdot\left[\begin{array}{cc|c} \multicolumn{2}{c|}{4\,;\,O^{+}\,;\,7} & 5 \\ \hline 1 & 2 & 3 \\ 2 & 0 & 4 \end{array}\right] =$$

$$[4;O^{+};7\,|\,1]\cdot[3;O^{-};7\,|\,3]\cdot[2;O^{+};7\,|\,4] =$$

$$7(7^2-1)\cdot 7(7+1)\cdot(7-1) = 7^2(7-1)^2(7+1)^2 = 112896.$$

(Note that $\begin{bmatrix} 1 & 3 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix}$, and that $\begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 2 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$.)

2.

$$[4;O^{+};7\,|\,0]\cdot\left[\begin{array}{c|c} 4\,;\,O^{+}\,;\,7 & 5 \\ \hline 0 & 4 \end{array}\right]\cdot\left[\begin{array}{cc|c} \multicolumn{2}{c|}{4\,;\,O^{+}\,;\,7} & 1 \\ \hline 0 & 4 & 2 \\ 4 & 5 & 3 \end{array}\right] =$$

$$[4;O^{+};7\,|\,0]\cdot q^2\cdot[2;O^{+};7\,|\,1] =$$

$$(7^2-1)(7+1)\cdot 7^2\cdot(7-1) = 7^2(7-1)^2(7+1)^2 = 112896.$$

(Note that $\begin{bmatrix} 1 & 1 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 0 & 4 \\ 4 & 5 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix}$, and that $\begin{bmatrix} 0 & 4 \\ 4 & 5 \end{bmatrix}\begin{bmatrix} 1 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$.)

3.

$$[4;O^+;7\,|\,5] \cdot \left[\begin{array}{c|c} 4\,;\,O^+\,;\,7 & 1 \\ \hline 5 & 3 \end{array}\right] \cdot \left[\begin{array}{cc|c} \multicolumn{2}{c|}{4\,;\,O^+\,;\,7} & 0 \\ \hline 5 & 3 & 4 \\ 3 & 1 & 2 \end{array}\right] =$$

$$[4;O^+;7\,|\,5] \cdot [3;O^+;7\,|\,4] \cdot [2;O^+;7\,|\,4] =$$

$$7(7^2-1)\cdot 7(7+1)\cdot(7-1) = 7^2(7-1)^2(7+1)^2 = 112896.$$

(Note that $\begin{bmatrix} 3 & 5 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 5 & 3 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 3 & 0 \\ 5 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 0 \\ 0 & 1 \end{bmatrix}$, and that $\begin{bmatrix} 5 & 3 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$.)

# References

[1] E. Artin, *Geometric Algebra*, Interscience Publishers (Wiley), New York, 1957.

[2] R. C. Bose and I. M. Chakravarti, Hermitian varieties in a finite projective space $PG(N,q^2)$, *Can. J. Math.* 18 (1966), 1161-1187.

[3] P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin, 1968.

[4] J. Dieudonné, *La Géométrie des Groupes Classiques*, 2nd ed., Springer-Verlag, Berlin, 1963.

[5] N. Jacobson, *Basic Algebra, Volume One*, 2nd. ed., W. H. Freeman, New York, 1985.

[6] I. Kaplansky, *Linear Algebra and Geometry*, Chelsea, New York, 1969.

[7] M. Q. Rieck, Totally isotopic subspaces, subspace complements and generalized inverses, *Linear Algebra and Appl.* 251 (1997), 239-248.