The geometry of orthogonal groups over finite fields

Akihiro Munemasa
Graduate School of Mathematics
Kyushu University

Preface

This lecture note is based on the lectures given at Kyushu University in 1994 and at Ateneo de Manila University in 1995. In these lectures I presented the theory of quadratic forms over finite fields. The emphasis is placed on geometric and combinatorial objects, rather than the orthogonal group itself. Our goal is to introduce dual polar spaces as distance-transitive graphs in a self contained way. Prerequisites are linear algebra, and finite fields. In the later part of the lecture, familiarity with counting the number of subspaces of a vector space over a finite field is helpful.

This lecture note is not intended as a full account of dual polar spaces. It merely treats those of type $D_n(q)$, $B_n(q)$ and ${}^2D_n(q)$. One can treat other types, namely, those coming from symplectic groups and unitary groups, in a uniform manner, but I decided to restrict our attention to the above three types in order to save time. Once the reader finishes this note, he/she should be able to learn the other cases with ease.

A motivation of writing this note, as well as giving the lecture, is to make the reader get acquainted with nontrivial examples of distance-transitive graphs. I consider Hamming graphs and Johnson graphs trivial, as one can establish their distance-transitivity without any special knowledge. The book by Brouwer–Cohen–Neumaier [2] seems too advanced for the beginning students, while other books on the classical groups and their geometries are oriented toward group theory. I hope this lecture note serves as a starting point for the reader to further study of distance-transitive and distance-regular graphs.

The presentation of this lecture note is strictly toward an introduction of dual polar spaces of type $D_n(q)$, $B_n(q)$ and ${}^2D_n(q)$. I have tried to throw away whatever unnecessary, to make it short. The Witt's extension theorem is included in the appendix for the sake of completeness. This fundamental theorem will not be used in the main text.

This lecture note was completed while the author was visiting Ateneo de Manila University, under a grant from JSPS–DOST. I would like to thank these organizations for their financial support. I would like to thank William Kantor for a helpful discussion on Witt's theorem. I also would like to thank faculty members of Mathematics Department of Ateneo de Manila University for their hospitality.

Contents

1 Symmetric bilinear forms and quadratic forms

All vector spaces are assumed to be finite dimensional.

Definition. A symmetric bilinear form on a vector space V over a field K is a mapping $B : V \times V \longrightarrow K$ satisfying

$$\begin{aligned} B(u,v) &= B(v,u), \\ B(u_1+u_2,v) &= B(u_1,v)+B(u_2,v), \\ B(\alpha u,v) &= \alpha B(u,v) \end{aligned}$$

for any $u, u_1, u_2, v \in V$ and $\alpha \in K$. Then clearly

$$\begin{aligned} B(u,v_1+v_2) &= B(u,v_1)+B(u,v_2), \\ B(u,\alpha v) &= \alpha B(u,v) \end{aligned}$$

hold for any $u, v_1, v_2, v \in V$ and $\alpha \in K$.

Definition. If U is a subset of a vector space V and B is a symmetric bilinear form on V, then we define the orthogonal complement of U by

$$U^\perp = \{v \in V | B(u,v) = 0 \text{ for any } u \in U\}.$$

The subspace $V^\perp$ is also denoted by $\mathrm{Rad}\,B$ which is called the radical of the symmetric bilinear form B. The symmetric bilinear form B is said to be non-degenerate if $\mathrm{Rad}\,B = 0$. If U is a subspace, then $B|_U : U \times U \longrightarrow K$ is a symmetric bilinear form on U, so by the definition $\mathrm{Rad}\,(B|_U) = U \cap U^\perp$. The subspace U is said to be non-degenerate if the restriction of B to U is non-degenerate, that is, $\mathrm{Rad}\,(B|_U) = 0$. If U is a direct sum of two subspaces U_1, U_2 and if $B(u_1, u_2) = 0$ for any $u_1 \in U_1$ and $u_2 \in U_2$, then we write $U = U_1 \perp U_2$. In this case $\mathrm{Rad}\,(B|_U) = \mathrm{Rad}\,(B|_{U_1}) \perp \mathrm{Rad}\,(B|_{U_2})$ holds.

Proposition 1.1 *Let B be a symmetric bilinear form on a vector space V, U a subspace of V. Then we have the following.*

(i) $\dim U + \dim U^\perp = \dim V + \dim U \cap \mathrm{Rad}\,B$.

(ii) $U^{\perp\perp} = U + \mathrm{Rad}\,B$.

(iii) *If U is non-degenerate, then $V = U \perp U^\perp$.*

Proof. (i) Suppose $\dim V = n$ and fix a basis $\{v_1, \ldots, v_n\}$ of V in such a way that $\langle v_1, v_2, \ldots, v_k\rangle \perp U \cap \mathrm{Rad}\,B = U$ holds. Then $U^\perp$ is isomorphic to the space of solutions of the system of linear equations

$$\sum_{i=1}^{n} B(v_i, v_j)x_i = 0 \quad (j = 1, \ldots, k).$$

Since $\langle v_1, v_2, \ldots, v_k\rangle \cap \mathrm{Rad}\,B = 0$, the $n \times k$ coefficient matrix $(B(v_i, v_j))$ of the above equations has rank k. Thus $\dim U^\perp = n - k$, proving (i).

(ii) Clearly, $U \perp \operatorname{Rad} B \subset U^{\perp\perp}$ holds. By (i) we have

$$\begin{aligned}\dim U^{\perp\perp} &= \dim V - \dim U^{\perp} + \dim U^{\perp} \cap \operatorname{Rad} B \\ &= \dim U - \dim U \cap \operatorname{Rad} B + \dim \operatorname{Rad} B \\ &= \dim(U + \operatorname{Rad} B).\end{aligned}$$

Therefore $U^{\perp\perp} = U + \operatorname{Rad} B$.

(iii) Since $0 = \operatorname{Rad} U = U \cap U^{\perp} \supset U \cap \operatorname{Rad} B$, we have $\dim U + \dim U^{\perp} = \dim V$ by (i) and hence $V = U \perp U^{\perp}$. ■

Definition. A quadratic form f on a vector space V over a field K is a mapping $f : V \times V \longrightarrow K$ satisfying

$$\begin{aligned}f(\alpha v) &= \alpha^2 f(v), \\ f(u+v) &= f(u) + f(v) + B_f(u,v)\end{aligned}$$

for any $u, v \in V$ and $\alpha \in K$, where B_f is a symmetric bilinear form.

Proposition 1.2 *If V is a vector space of dimension n, then there is a one-to-one correspondence between quadratic forms on V and homogeneous polynomials of degree 2 in n variables.*

Proof. Fix a basis $v_1, \ldots, v_n$ of V. If

$$p = p(x_1, \ldots, x_n) = \sum_{i \le j} \alpha_{ij} x_i x_j \tag{1.1}$$

is a homogeneous polynomial of degree 2 in $x_1, \ldots, x_n$, then define a mapping f by $f(v) = p(\lambda_1, \ldots, \lambda_n)$, where $v = \sum_{i=1}^n \lambda_i v_i$. Clearly

$$f(\alpha v) = f(\sum_{i=1}^n \alpha \lambda_i v_i) = p(\alpha\lambda_1, \ldots, \alpha\lambda_n) = \alpha^2 p(\lambda_1, \ldots, \lambda_n).$$

If we define B_f by

$$B_f(u,v) = \sum_{i \le j} \alpha_{ij}(\mu_i \lambda_j + \mu_j \lambda_i)$$

where $u = \sum_{i=1}^n \mu_i v_i$, $v = \sum_{i=1}^n \lambda_i v_i$, then B_f is a symmetric bilinear form on V and we have

$$\begin{aligned}f(u+v) &= \sum_{i \le j} \alpha_{ij}(\mu_i + \lambda_i)(\mu_j + \lambda_j) \\ &= \sum_{i \le j} \alpha_{ij}\mu_i\mu_j + \sum_{i \le j} \alpha_{ij}\lambda_i\lambda_j + \sum_{i \le j} \alpha_{ij}(\mu_i\lambda_j + \mu_j\lambda_i) \\ &= f(u) + f(v) + B_f(u,v)\end{aligned}$$

Thus f is a quadratic form. Notice that the coefficients of the polynomial p can be recovered by the formula

$$\alpha_{ii} = f(v_i), \tag{1.2}$$

$$\alpha_{ij} = B_f(v_i, v_j) \quad (i < j). \tag{1.3}$$

Conversely, given a quadratic form f, define a homogeneous polynomial p by (1.1), (1.2) and (1.3). Then we have

$$\begin{aligned} f(v) &= f(\sum_{i=1}^{n} \lambda_i v_i) \\ &= \sum_{i=1}^{n} f(\lambda_i v_i) + \sum_{i<j} B_f(\lambda_i v_i, \lambda_j v_j) \\ &= \sum_{i=1}^{n} \lambda_i^2 f(v_i) + \sum_{i<j} \lambda_i \lambda_j B_f(v_i, v_j) \\ &= \sum_{i=1}^{n} \alpha_{ii} \lambda_i^2 + \sum_{i<j} \alpha_{ij} \lambda_i \lambda_j \\ &= \sum_{i \le j} \alpha_{ij} \lambda_i \lambda_j \\ &= p(\lambda_1, \ldots, \lambda_n). \end{aligned}$$

This establishes a one-to-one correspondence. ∎

Definition. If f is a quadratic form on a vector space V, a vector $v \in V$ is called singular if $f(v) = 0$. A subspace U of V is called singular if it consists of singular vectors.

Example. Let $p = x_1x_2 + x_3x_4$, and consider the corresponding quadratic form f determined by p with respect to the standard basis of

$$V = \mathrm{GF}(2)^4 = \{(\alpha_1, \alpha_2, \alpha_3, \alpha_4) | \alpha_i = 0 \text{ or } 1\}.$$

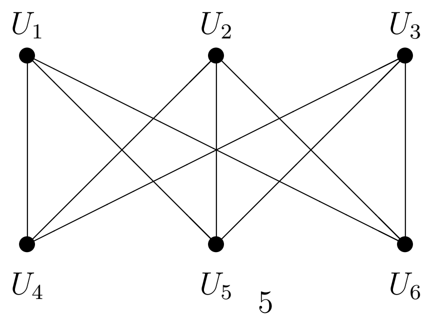
Nonzero singular vectors are

$$\begin{array}{lllll} (1,0,0,0), & (0,1,0,0), & (0,0,1,0), & (0,0,0,1), & (1,1,1,1) \\ (1,0,1,0), & (1,0,0,1), & (0,1,1,0), & (0,1,0,1), & \end{array}$$

while singular 2-dimensional subspaces are

$$\begin{aligned} U_1 &= \{(0,0,0,0), (1,0,0,0), (0,0,1,0), (1,0,1,0)\}, \\ U_2 &= \{(0,0,0,0), (0,1,0,0), (0,0,0,1), (0,1,0,1)\}, \\ U_3 &= \{(0,0,0,0), (1,0,0,1), (0,1,1,0), (1,1,1,1)\}, \\ U_4 &= \{(0,0,0,0), (1,0,0,0), (0,0,0,1), (1,0,0,1)\}, \\ U_5 &= \{(0,0,0,0), (0,1,0,0), (0,0,1,0), (0,1,1,0)\}, \\ U_6 &= \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}. \end{aligned}$$

Let us construct a graph by taking vertices as singular 2-dimensional subspaces, joining two vertices when they intersect nontrivially. The graph is isomorphic to the complete bipartite graph $K_{3,3}$ depicted below.



Definition. The radical of a quadratic form f on a vector space V over a field K is defined to be

$$\mathrm{Rad}\, f = f^{-1}(0) \cap \mathrm{Rad}\, B_f.$$

The quadratic form f is said to be non-degenerate if $\mathrm{Rad}\, f = 0$. If U is a subspace of V, then $f|_U : U \longrightarrow K$ is a quadratic form on U, so by the definition $\mathrm{Rad}\,(f|_U) = f^{-1}(0) \cap U \cap U^{\perp}$. The subspace U is said to be non-degenerate if the restriction of f to U is non-degenerate, that is, $\mathrm{Rad}\,(f|_U) = 0$.

We denote by $\mathrm{ch}K$ the characteristic of a field K. The whole theory of quadratic forms looks quite different if $\mathrm{ch}K$ is 2, but we shall try to take as unified an approach as possible. First notice that $\mathrm{Rad}\, f = \mathrm{Rad}\, B_f$ if $\mathrm{ch}K \neq 2$. Indeed,

$$2f(v) = B_f(v, v) \tag{1.4}$$

holds for any $v \in V$, thus if $\mathrm{ch}K \neq 2$, then $f(v) = 0$ for any $v \in \mathrm{Rad}\, B_f$. Notice also that $\mathrm{Rad}\, f$ is a subspace even if $\mathrm{ch}K = 2$.

Proposition 1.3 *Let f be a non-degenerate quadratic form on a vector space V, U a subspace of V. If $B_f|_U$ is non-degenerate, then we have $V = U \perp U^{\perp}$ and $U^{\perp}$ is non-degenerate.*

Proof. The first part follows from Proposition 1.1 (iii). Since

$$\mathrm{Rad}\, B_f = \mathrm{Rad}\,(B_f|_U) \perp \mathrm{Rad}\,(B_f|_{U^{\perp}}) = \mathrm{Rad}\,(B_f|_{U^{\perp}}),$$

we have

$$\mathrm{Rad}\,(f|_{U^{\perp}}) = f^{-1}(0) \cap \mathrm{Rad}\,(B_f|_{U^{\perp}}) = f^{-1}(0) \cap \mathrm{Rad}\, B_f = \mathrm{Rad}\, f = 0.$$

Thus $U^{\perp}$ is non-degenerate. ∎

Lemma 1.4 *Let f be a non-degenerate quadratic form on V. If U is a singular subspace of V, then $\dim U^{\perp} = \dim V - \dim U$ and $\mathrm{Rad}\,(f|_{U^{\perp}}) = U$.*

Proof. Since f is non-degenerate, we have $U \cap \mathrm{Rad}\, B = 0$, so that by Proposition 1.1, $\dim U^{\perp} = \dim V - \dim U$ and $U^{\perp\perp} = U \perp \mathrm{Rad}\, B$ hold. The latter equality implies $U^{\perp} \cap U^{\perp\perp} = U \perp \mathrm{Rad}\, B$, and hence $\mathrm{Rad}\,(f|_{U^{\perp}}) = f^{-1}(0) \cap (U \perp \mathrm{Rad}\, B) = U$. ∎

If $\mathrm{ch}K = 2$, then $B_f(v, v) = 0$, that is, the symmetric bilinear form B_f is also alternating. Recall that a square matrix $A = (a_{ij})$ is alternating if $a_{ii} = 0$ and $a_{ij} + a_{ji} = 0$ for all i, j.

Proposition 1.5 *If an alternating matrix is nonsingular, then its size must be even.*

Proof. Let A be an alternating matrix of size n. This is trivial when $\mathrm{ch}K \neq 2$, as $|A| = |A^T| = |-A| = (-1)^n |A|$. If $\mathrm{ch}K = 2$, then consider the definition of determinant. If n is odd, there is no fixed-point-free permutation of order 2. Thus all terms are canceled out in pairs, so that the determinant is zero. Suppose $\mathrm{rank}A = r$. Let B be a nonsingular matrix whose first $n - r$ columns form the right null space of A. Then the matrix ${}^tBAB$

has rank r and contains a $r \times r$ alternating submatrix with all other part 0. By the first part we see r is even. ∎

From now on we assume that K is a finite field. If $\mathrm{ch}K = 2$, then the multiplicative group $K^\times$ is a cyclic group of odd order, and consequently a square root of an element is uniquely determined. Moreover, $\sqrt{\alpha+\beta} = \sqrt{\alpha} + \sqrt{\beta}$ holds, as taking the square root is the inverse of the Frobenius automorphism $\alpha \mapsto \alpha^2$. We need this fact to prove the following proposition.

Proposition 1.6 *If f is a non-degenerate quadratic form on a vector space V over K, then either B_f is non-degenerate, or* $\mathrm{ch}K = 2$, $\dim V$ *is odd, and* $\dim \mathrm{Rad}\, B_f = 1$.

Proof. As shown before, $\mathrm{Rad}\, f = \mathrm{Rad}\, B_f$ if $\mathrm{ch}K \neq 2$. Thus, if $\mathrm{Rad}\, B_f \neq 0$, then $\mathrm{ch}K = 2$. Then the mapping from $\mathrm{Rad}\, B_f$ to K defined by $v \mapsto \sqrt{f(v)}$ is an isomorphism of K-vector spaces. It remains to show that $n = \dim V$ is odd. Fix a basis $\{v_1, \ldots, v_n\}$ of V such that v_n is a basis of $\mathrm{Rad}\, B_f$. Then the matrix $A = (B_f(v_i, v_j))_{1 \leq i,j \leq n-1}$ is a nonsingular alternating matrix of size $n-1$. By Proposition 1.5 we conclude that n is odd. ∎

Definition. Let f be a quadratic form on a vector space V over K. A hyperbolic pair is a pair of vectors $\{u, v\}$ of V satisfying $f(u) = 0$, $f(v) = 0$ and $B_f(u, v) = 1$. Clearly, a hyperbolic pair is a set of linearly independent vectors. The 2-dimensional subspace $\langle u, v\rangle$ spanned by the hyperbolic pair $\{u, v\}$ is called a hyperbolic plane.

If $\{v_1, v_2\}$ is a hyperbolic pair, then the quadratic form $f|_{\langle v_1, v_2\rangle}$ corresponds to the monomial x_1x_2 in the sense of Proposition 1.2. Indeed, $f(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1^2 f(v_1) + \lambda_2^2 f(v_2) + \lambda_1\lambda_2 B_f(v_1, v_2) = \lambda_1\lambda_2$. A hyperbolic plane P is clearly non-degenerate. Indeed, $B_f|_P$ is non-degenerate.

Proposition 1.7 *If f is a quadratic form on a vector space V, u is a nonzero singular vector, and $B_f(u, w) \neq 0$, then there exists a vector $v \in \langle u, w\rangle$ such that $\{u, v\}$ is a hyperbolic pair.*

Proof. Let $w_1 = B_f(u, w)^{-1}w$. Then $B_f(u, w_1) = 1$ and $v = -f(w_1)u + w_1$ has the desired property. ∎

Proposition 1.8 *If f is a non-degenerate quadratic form on a vector space V and u is a nonzero singular vector, then there exists a vector v such that $\{u, v\}$ is a hyperbolic pair.*

Proof. Since $f(u) = 0$, $u \notin \mathrm{Rad}\, B_f$. Thus there exist a vector w such that $B_f(u, w) \neq 0$. The result follows from Proposition 1.7. ∎

Definition. Let f, f' be quadratic forms on vector spaces V, V' over K, respectively. An isometry $\sigma : (V, f) \longrightarrow (V', f')$ is an injective linear mapping from V to V' satisfying $f(v) = f'(\sigma(v))$ for all $v \in V$. The two quadratic forms f, f' are called equivalent if there exists an isometry from V onto V'.

We shall use the following lemma to check a given linear mapping is an isometry.

Lemma 1.9 *Let f, f' be quadratic forms on vector spaces V, V' over K, respectively, and let $\{v_1, \ldots, v_n\}$ be a basis of V. An injective linear mapping $\sigma : V \longrightarrow V'$ is an isometry if and only if*

$$\begin{aligned} f(v_i) &= f'(\sigma(v_i)) && \text{for all } i = 1, \ldots, n, \\ B_f(v_i, v_j) &= B_{f'}(\sigma(v_i), \sigma(v_j)) && \text{for all } i, j = 1, \ldots, n. \end{aligned}$$

Proof. Under the stated conditions, we have

$$\begin{aligned} f(\sum_{i=1}^{n} \lambda_i v_i) &= \sum_{i=1}^{n} \lambda_i^2 f(v_i) + \sum_{i<j} \lambda_i \lambda_j B_f(v_i, v_j) \\ &= \sum_{i=1}^{n} \lambda_i^2 f'(\sigma(v_i)) + \sum_{i<j} \lambda_i \lambda_j B_{f'}(\sigma(v_i), \sigma(v_j)) \\ &= f'(\sum_{i=1}^{n} \lambda_i \sigma(v_i)) \\ &= f'(\sigma(\sum_{i=1}^{n} \lambda_i v_i)), \end{aligned}$$

so that σ is an isometry. The converse is obvious. ■

2 Classification of quadratic forms

In this section we classify non-degenerate quadratic forms. As before, we let V be a finite-dimensional vector space over a finite field K.

Definition. Let f be a quadratic form on V. The Witt index of f is defined to be the maximum of the dimensions of singular subspaces of V.

Proposition 2.1 *Let f be a quadratic form of Witt index d on V. Then any maximal singular subspace of V has dimension d.*

Proof. Let U be a singular subspace of dimension d. We want to show that any singular subspace W of dimension less than d cannot be maximal. Since $W^\perp + U \subset (W \cap U)^\perp$, we have, by Proposition 1.1 (i)

$$\begin{aligned}
\dim W^\perp \cap U &= \dim W^\perp + \dim U - \dim(W^\perp + U) \\
&\geq \dim V + \dim W \cap \operatorname{Rad} B_f - \dim W \\
&\quad + \dim U - \dim(W \cap U)^\perp \\
&\geq \dim V + \dim W \cap U \cap \operatorname{Rad} B_f - \dim(W \cap U)^\perp \\
&\quad + \dim U - \dim W \\
&= \dim W \cap U + \dim U - \dim W \\
&> \dim W \cap U.
\end{aligned}$$

This implies that there exists a nonzero vector $u \in W^\perp \cap U$ with $u \notin W$. The subspace $W \perp \langle u \rangle$ is a singular subspace containing W, so that W is not maximal. ∎

The assertion of Proposition 2.1 is also a consequence of the Witt's extension theorem (see Theorem A.6). Indeed, the Witt's extension theorem implies that the group of isometries acts transitively on the set of maximal singular subspaces. Yet another proof of this fact will be given in Appendix B.

Lemma 2.2 *Let K be a finite field of odd characteristic. Then for any $\alpha \in K$ there exist elements $\lambda, \mu \in K$ such that $\alpha = \lambda^2 + \mu^2$ holds.*

Proof. If α is a square, then we may take $\mu = 0$, so let us assume that α is a non-square. Thus it suffices to show that every non-square can be expressed as the sum of two squares. To show this, it is then suffices to prove that some non-square can be expressed as the sum of two squares. Suppose contrary. Then the sum of two squares is always a square, so that the set of all squares becomes an additive subgroup of K of order $(|K| + 1)/2$, which is not a divisor of $|K|$, contradiction. ∎

Lemma 2.3 *Let f be a non-degenerate quadratic form on V. If $\dim V \geq 3$, then the Witt index of f is greater than 0.*

Proof. Case 1. $\mathrm{ch} K \neq 2$. Let $v_1 \in V$ be a nonzero vector. We may assume $f(v_1) \neq 0$. Then $B_f|_{\langle v_1 \rangle}$ is non-degenerate, so that by Proposition 1.1 (iii), we have $V = \langle v_1 \rangle \perp \langle v_1 \rangle^\perp$. Let $v_2 \in \langle v_1 \rangle^\perp$ be a nonzero vector. Again we may assume $f(v_2) \neq 0$. If we put $P =$

$\langle v_1, v_2\rangle$, then we can see easily that $B_f|_P$ is non-degenerate. Again by Proposition 1.1 (iii), we have $V = P \perp P^\perp = \langle v_1\rangle \perp \langle v_2\rangle \perp P^\perp$. Let $v_3 \in P^\perp$ be a nonzero vector. We may assume $f(v_3) \neq 0$. Then

$$\{f(v_1), f(v_2), f(v_3)\} \subset K^\times = (K^\times)^2 \cup \varepsilon(K^\times)^2,$$

where ε is a non-square, hence two of the three elements belong to the same part. Without loss of generality we may assume $f(v_1)$ and $f(v_2)$ belong to the same part, that is, $f(v_1)f(v_2)^{-1} = \alpha^2 \in (K^\times)^2$. Replacing v_2 by αv_2, we may assume $f(v_1) = f(v_2)$. By Lemma 2.2, there exist elements $\alpha, \beta \in K$ such that $-f(v_3)f(v_1)^{-1} = \alpha^2 + \beta^2$. Now the vector $v = \alpha v_1 + \beta v_2 + v_3$ has the desired property $f(v) = 0$.

Case 2. $\mathrm{ch}K = 2$. Let W be a subspace of V of dimension 3. If $f|_W$ is degenerate, then $f^{-1}(0) \neq 0$, so the assertion holds. If $f|_W$ is non-degenerate, then let $\langle v\rangle = \mathrm{Rad}\, B_{f|_W}$. Pick an element $u \in W$, $u \notin \mathrm{Rad}\, B_{f|_W}$. Then $f(\sqrt{f(v)}u + \sqrt{f(u)}v) = 0$ as desired. ■

Proposition 2.4 *Let f be a non-degenerate quadratic form on V. If U is a maximal singular subspace of V and* $\dim U = d$, *then there exist hyperbolic pairs* $\{v_{2i-1}, v_{2i}\}$ $(i = 1, \ldots, d)$ *such that* $U = \langle v_1, v_3, \ldots, v_{2d-1}\rangle$ *and*

$$V = \langle v_1, v_2\rangle \perp \cdots \perp \langle v_{2d-1}, v_{2d}\rangle \perp W,$$

where W is a subspace containing no nonzero singular vectors. In particular, $\dim V = 2d + e$, $e = 0, 1$ *or* 2.

Proof. We prove by induction on d. The case $d = 0$ is trivial except the assertion on $\dim W$, which follows from Lemma 2.3. Suppose $d \geq 1$. Pick a nonzero vector $v_1 \in U$ and take a complementary subspace U' in U: $U = \langle v_1\rangle \perp U'$. The subspace U' is singular, so by Lemma 1.4, we have $\mathrm{Rad}\,(f|_{U'^\perp}) = U'$. Since $f(v_1) = 0$ and $v_1 \notin U'$, we see $v_1 \notin \mathrm{Rad}\,(B_f|_{U'^\perp})$. This implies that there exists a vector $v \in U'^\perp$ such that $B_f(v_1, v) \neq 0$. By Proposition 1.7 there exists a vector $v_2 \in \langle v_1, v\rangle \subset U'^\perp$ such that $\{v_1, v_2\}$ is a hyperbolic pair. By Proposition 1.3, we have $V = P \perp P^\perp$, where $P = \langle v_1, v_2\rangle$, and $P^\perp$ is non-degenerate. Since $v_1, v_2 \in U'^\perp$, we see $U' \subset P^\perp$. Also, U' is a maximal singular subspace of $P^\perp$, since otherwise U would not be a maximal singular subspace of V. By induction we find hyperbolic pairs $\{v_{2i-1}, v_{2i}\}$ $(i = 2, \ldots, d)$ such that

$$P^\perp = \langle v_3, v_4\rangle \perp \cdots \perp \langle v_{2d-1}, v_{2d}\rangle \perp W,$$

where W is a subspace of dimension $0, 1$ or 2, containing no nonzero singular vectors. This gives the desired orthogonal decomposition of V. ■

Theorem 2.5 *Let f be a non-degenerate quadratic form on V with* $\dim V = 2m + 1$. *Then f has Witt index m and there exists a basis $\{v_1, \ldots, v_{2m+1}\}$ of V such that*

$$f(\sum_{i=1}^{2m+1} \xi_i v_i) = \sum_{i=1}^{m} \xi_{2i-1}\xi_{2i} + \xi_{2m+1}^2 \tag{2.1}$$

or ε is a non-square in K with $\mathrm{ch}K \neq 2$ *and*

$$f(\sum_{i=1}^{2m+1} \xi_i v_i) = \sum_{i=1}^{m} \xi_{2i-1}\xi_{2i} + \varepsilon\xi_{2m+1}^2 \tag{2.2}$$

Proof. Clearly f has Witt index m by the second part of Proposition 2.4. Also by Proposition 2.4, there exists a basis $\{v_1, \ldots, v_{2m}, w\}$ such that

$$V = \langle v_1, v_2 \rangle \perp \cdots \perp \langle v_{2m-1}, v_{2m} \rangle \perp \langle w \rangle,$$

where $\{v_{2i-1}, v_{2i}\}$ $(i = 1, \ldots, m)$ are hyperbolic pairs, $f(w) \neq 0$. If $f(w)$ is a square in K, say $f(w) = \alpha^2$ for some $\alpha \in K$, then defining $v_{2m+1} = \alpha^{-1} w$, we obtain the desired form of f. If $f(w)$ is a non-square in K (this occurs only when $\mathrm{ch} K \neq 2$), then $f(w) = \varepsilon\alpha^2$ for some $\alpha \in K$. Again defining $v_{2m+1} = \alpha^{-1} w$, we obtain the desired form of f. ∎

Corollary 2.6 *Let f, f' be non-degenerate quadratic forms on vector spaces V, V', respectively, over K with* $\dim V = \dim V' = 2m + 1$.

(i) *If* $\mathrm{ch} K = 2$, *then f is equivalent to f'.*

(ii) *If* $\mathrm{ch} K$ *is odd, let ε be a non-square. Then f is equivalent to either f' or $\varepsilon f'$.*

Proof. (i) This follows immediately from Theorem 2.5.

(ii) Let

$$f(\sum_{i=1}^{2m+1} \xi_i v_i) = \sum_{i=1}^{m} \xi_{2i-1}\xi_{2i} + \xi_{2m+1}^2,$$
$$f'(\sum_{i=1}^{2m+1} \xi_i v_i') = \sum_{i=1}^{m} \xi_{2i-1}\xi_{2i} + \varepsilon\xi_{2m+1}^2,$$

for some bases $\{v_1, \ldots, v_{2m+1}\}$, $\{v_1', \ldots, v_{2m+1}'\}$ of V, V', respectively. We want to construct an isometry from (V, f) to $(V', \varepsilon f')$. Define a new basis $\{v_1'', \ldots, v_{2m+1}''\}$ of V' by

$$\begin{aligned} v_{2i-1}'' &= \varepsilon^{-1} v_{2i-1}' & i &= 1, \ldots, m+1, \\ v_{2i}'' &= v_{2i}' & i &= 1, \ldots, m. \end{aligned}$$

Then we have

$$\begin{aligned} \varepsilon f'(\sum_{i=1}^{2m+1} \xi_i v_i'') &= \varepsilon f'(\sum_{i=1}^{m+1} \varepsilon^{-1}\xi_{2i-1} v_{2i-1}' + \sum_{i=1}^{m} \xi_{2i} v_{2i}') \\ &= \varepsilon(\sum_{i=1}^{m} \varepsilon^{-1}\xi_{2i-1}\xi_{2i} + \varepsilon(\varepsilon^{-1}\xi_{2m+1})^2) \\ &= \sum_{i=1}^{m} \xi_{2i-1}\xi_{2i} + \xi_{2m+1}^2. \end{aligned}$$

Thus, the correspondence $v_i \mapsto v_i''$ is an isometry from (V, f) to $(V', \varepsilon f')$. Next suppose

$$f(\sum_{i=1}^{2m+1} \xi_i v_i) = \sum_{i=1}^{m} \xi_{2i-1}\xi_{2i} + \varepsilon\xi_{2m+1}^2,$$

$$f'(\sum_{i=1}^{2m+1} \xi_i v_i') = \sum_{i=1}^{m} \xi_{2i-1}\xi_{2i} + \xi_{2m+1}^2.$$

By the above argument, there exists an isometry from (V', f') to $(V, \varepsilon f)$. This implies the existence of an isometry from $(V, \varepsilon^2 f)$ to $(V', \varepsilon f')$. Since there is an isometry from (V, f) to $(V, \varepsilon^2 f)$, we obtain the desired isometry from (V, f) to $(V', \varepsilon f')$. ∎

Proposition 2.7 *The two quadratic forms given in* (2.1) *and* (2.2) *are not equivalent to each other.*

Proof. Let f, f' be the quadratic forms given in (2.1), (2.2), respectively. Suppose that $\sigma : (V, f) \longrightarrow (V, f')$ is an isometry and write $\sigma(v_j) = \sum_{i=1}^{2m+1} \alpha_{ij} v_i$, $A = (\alpha_{ij})$. Then

$$\begin{aligned} B_f(v_i, v_j) &= B_{f'}(\sigma(v_i), \sigma(v_j)) \\ &= \sum_{k=1}^{2m+1} \sum_{l=1}^{2m+1} \alpha_{ki}\alpha_{lj} B_{f'}(v_k, v_l), \end{aligned}$$

$$(B_f(v_i, v_j)) = {}^tA(B_{f'}(v_i, v_j))A.$$

Taking the determinants, we find $(-1)^m = (\det A)^2(-1)^m\varepsilon$. This is a contradiction since ε is a non-square. ∎

Lemma 2.8 *Let f be a non-degenerate quadratic form on a vector space V of dimension 2 over K with* $\mathrm{ch}K \neq 2$. *Let ε be a non-square in K. Suppose that the Witt index of f is zero. Then there exists a basis $\{v_1, v_2\}$ of V such that*

$$f(\xi_1 v_1 + \xi_2 v_2) = \xi_1^2 - \varepsilon\xi_2^2.$$

Proof. If v is a nonzero vector, then $f(v) \neq 0$, so $B_f(v, v) \neq 0$. This implies that $B_f|_{\langle v\rangle}$ is non-degenerate. By Proposition 1.3 we have $V = \langle v\rangle \perp \langle v\rangle^\perp$. Since $\dim\langle v\rangle^\perp = 1$, we may put $\langle w\rangle = \langle v\rangle^\perp$. We claim that there exists a vector v_1 with $f(v_1) = 1$. If $f(v)$ or $f(w)$ is a square, say $f(v) = \alpha^2$ or $f(w) = \alpha^2$, then we may put $v_1 = \alpha^{-1}v$ or $v_1 = \alpha^{-1}w$, respectively. If neither $f(v)$ nor $f(w)$ is a square, then we can write $f(v) = \varepsilon\alpha^2$, $f(w) = \varepsilon\beta^2$ for some $\alpha, \beta \in K$. By Lemma 2.2, there exist elements $\lambda, \mu \in K$ such that $\varepsilon^{-1} = \lambda^2 + \mu^2$. Defining $v_1 = \frac{\lambda}{\alpha}v + \frac{\mu}{\beta}w$, we find $f(v_1) = 1$.

Now $V = \langle v_1\rangle \perp \langle v_1\rangle^\perp$, and put $\langle u\rangle = \langle v_1\rangle^\perp$. If $-f(u)$ is a square, say $-f(u) = \alpha^2$, then $f(\alpha v_1 + u) = \alpha^2 f(v_1) + f(u) = 0$, contradicting to the fact that the Witt index of f is zero. Thus $-f(u)$ is a non-square, that is, $f(u) = -\varepsilon\alpha^2$ for some $\alpha \in K$. If we define v_2 by $v_2 = \alpha^{-1}u$, then we obtain $f(v_2) = -\varepsilon$ and $f(\xi_1 v_1 + \xi_2 v_2) = \xi_1^2 - \varepsilon\xi_2^2$ as desired. ∎

Lemma 2.9 *Let K be a finite field of characteristic* 2.

(i) *The mapping $\varphi : K \longrightarrow K$ defined by $\varphi(\alpha) = \alpha^2 + \alpha$ is an additive homomorphism, and its image* $\mathrm{Im}\,\varphi$ *is a subgroup of K of index* 2.

(ii) *If $\alpha, \beta \in K$ and the polynomials $t^2 + t + \alpha, t^2 + t + \beta \in K[t]$ are irreducible over K, then there exists an element $\lambda \in K$ such that $\alpha = \lambda^2 + \lambda + \beta$.*

Proof. (i) Clearly φ is an additive homomorphism:

$$\varphi(\alpha + \beta) = (\alpha + \beta)^2 + (\alpha + \beta) = \alpha^2 + \beta^2 + \alpha + \beta = \varphi(\alpha) + \varphi(\beta).$$

If $\alpha \in \mathrm{Ker}\,\varphi$, then $\alpha(\alpha + 1) = 0$, hence $\mathrm{Ker}\,\varphi = \{0, 1\}$. Thus $|\mathrm{Im}\,\varphi| = |K|/|\mathrm{Ker}\,\varphi| = |K|/2$.

(ii) Note that the polynomial $t^2 + t + \alpha$ is irreducible over K if and only if $\alpha \notin \mathrm{Im}\,\varphi$. Thus, if both $t^2 + t + \alpha$ and $t^2 + t + \beta$ are irreducible over K, then $\alpha \notin \mathrm{Im}\,\varphi$ and $\beta \notin \mathrm{Im}\,\varphi$. By (i), it follows that $\alpha \in \mathrm{Im}\,\varphi + \beta$, proving the assertion. ∎

Lemma 2.10 *Let f be a non-degenerate quadratic form on a vector space V of dimension 2 over K with $\mathrm{ch}K = 2$. Let α be an element of K such that the polynomial $t^2 + t + \alpha$ is irreducible over K. Suppose that the Witt index of f is zero. Then there exists a basis $\{v_1, v_2\}$ of V such that*

$$f(\xi_1 v_1 + \xi_2 v_2) = \xi_1^2 + \xi_1\xi_2 + \alpha\xi_2^2.$$

Proof. If v is a nonzero vector, then $f(v) \neq 0$. Defining $v_1 = \sqrt{f(v)}^{-1} v$, we have $f(v_1) = 1$. Since B_f is non-degenerate by Proposition 1.6, there exists a vector w such that $B_f(v_1, w) \neq 0$. Since $B_f(v_1, v_1) = 0$, we see $w \notin \langle v_1 \rangle$, hence $V = \langle v_1 \rangle \oplus \langle w \rangle$. Replacing w by $B_f(v_1, w)^{-1}w$, we may assume $B_f(v_1, w) = 1$. If $t^2+t+f(w)$ is reducible over K, that is, if there exists an element ξ such that $\xi^2+\xi+f(w) = 0$, then $f(\xi v_1+w) = 0$, contradicting to the fact that the Witt index of f is zero. Thus $t^2 + t + f(w)$ is irreducible over K, and hence by Lemma 2.9 (ii), there exists an element $\lambda \in K$ such that $\alpha = \lambda^2 + \lambda + f(w)$. Put $v_2 = \lambda v_1 + w$. Then $\{v_1, v_2\}$ is a basis of V and,

$$\begin{aligned} f(\xi_1 v_1 + \xi_2 v_2) &= \xi_1^2 f(v_1) + \xi_2^2 f(v_2) + \xi_1\xi_2 B_f(v_1, v_2) \\ &= \xi_1^2 + \xi_2^2 f(\lambda v_1 + w) + \xi_1\xi_2 B_f(v_1, \lambda v_1 + w) \\ &= \xi_1^2 + \xi_2^2(\lambda^2 + f(w) + \lambda) + \xi_1\xi_2 \\ &= \xi_1^2 + \xi_1\xi_2 + \alpha\xi_2^2, \end{aligned}$$

as desired. ∎

Theorem 2.11 *Let f be a non-degenerate quadratic form on V with $\dim V = 2m$. Then one of the following occurs.*

(i) *f has Witt index m, and there exists a basis $\{v_1, \ldots, v_{2m}\}$ of V such that*

$$f(\sum_{i=1}^{2m} \xi_i v_i) = \sum_{i=1}^{m} \xi_{2i-1}\xi_{2i}.$$

(ii) *f has Witt index $m - 1$, and there exists a basis $\{v_1, \ldots, v_{2m}\}$ of V such that*

(a) $\mathrm{ch}K$ *is odd, ε is a non-square in K, and*

$$f(\sum_{i=1}^{2m} \xi_i v_i) = \sum_{i=1}^{m-1} \xi_{2i-1}\xi_{2i} + \xi_{2m-1}^2 - \varepsilon\xi_{2m}^2.$$

(b) $\mathrm{ch}K = 2$, *$t^2 + t + \alpha$ is an irreducible polynomial over K, and*

$$f(\sum_{i=1}^{2m} \xi_i v_i) = \sum_{i=1}^{m-1} \xi_{2i-1}\xi_{2i} + \xi_{2m-1}^2 + \xi_{2m-1}\xi_{2m} + \alpha\xi_{2m}^2.$$

Proof. Let d be the Witt index of f. By the second part of Proposition 2.4, we have $d = m$ or $m - 1$. Also by Proposition 2.4, there exist hyperbolic pairs $\{v_{2i-1}, v_{2i}\}$ $(i = 1, \ldots, d)$ such that

$$V = \langle v_1, v_2 \rangle \perp \cdots \perp \langle v_{2d-1}, v_{2d} \rangle \perp W,$$

where W is a subspace containing no nonzero singular vectors, and $\dim W = 0$ or 2. If $d = m$, that is, $\dim W = 0$, then we obtain the case (i). If $d = m-1$, that is, $\dim W = 2$, then W is non-degenerate by Proposition 1.3. Now we obtain the case (ii) by Lemma 2.8 and Lemma 2.10. ■

Corollary 2.12 *Let f,f' be non-degenerate quadratic forms on vector spaces V, V', respectively, over K with $\dim V = \dim V' = 2m$. If the Witt indices of f and f' coincide, then f and f' are equivalent.*

Proof. This follows immediately from Theorem 2.11. Note that the non-square ε and the element α in Theorem 2.11 (ii) can be chosen to be a prescribed one. ■

Exercise. Show that the quadratic form f on $\mathrm{GF}(2)^6$ defined by the homogeneous polynomial $x_1^2 + x_5^2 + x_6^2 + x_1x_2 + x_3x_4 + x_4x_6 + x_5x_6$ is non-degenerate. Find the Witt index of f.

3 Dual polar spaces as distance-transitive graphs

In this section we introduce three types of dual polar spaces associated with non-degenerate quadratic forms. We shall show that the dual polar spaces admit a natural metric induced by a graph structure, and the orthogonal group, which is the group of isometries, acts distance-transitively on the dual polar space.

Definition. Let f be a non-degenerate quadratic form on a vector space V over a field K. The orthogonal group $O(V, f)$ is the group of automorphisms of f. More precisely,

$$O(V, f) = \{\sigma \in GL(V) | f(v) = f(\sigma(v)) \text{ for all } v \in V\}.$$

If V is a vector space of dimension $2m$ over a finite field $K = \mathrm{GF}(q)$, and f has Witt index m or $m-1$, we denote the orthogonal group $O(V, f)$ by $O_+(2m, q)$, $O_-(2m, q)$, respectively. Note that by Corollary 2.12, there is no ambiguity as to which quadratic form we refer to; the groups $O_+(2m, q)$ and $O_-(2m, q)$ are determined up to conjugacy in $\mathrm{GL}(V)$. If V is a vector space of dimension $2m + 1$ over a finite field $K = \mathrm{GF}(q)$, we denote the orthogonal group $O(V, f)$ by $O(2m + 1, q)$. Again by Corollary 2.6 (i), there is no ambiguity when $\mathrm{ch}K = 2$. If $\mathrm{ch}K$ is odd, then any non-degenerate quadratic form is equivalent to either f or εf, where ε is a non-square in K. Since $O(V, f) = O(V, \varepsilon f)$, there is no ambiguity in this case either.

Definition. Let f be a non-degenerate quadratic form on a vector space V over a finite field $K = \mathrm{GF}(q)$. A dual polar space is the set of all maximal singular subspaces of V:

$$X = \{U | U \text{ is a maximal singular subspace of } V\}.$$

If f has Witt index d, then by Proposition 2.4, we see $\dim V = 2d + e$, $e = 0, 1$ or 2. Also by Proposition 2.1, X consists of subspaces of dimension d. We say that the dual polar space is of type $D_d(q)$, $B_d(q)$ or ${}^2D_{d+1}(q)$, according as $e = 0, 1$ or 2. By specifying a type, a dual polar space is uniquely determined up to the action of $\mathrm{GL}(V)$. Indeed by Corollary 2.6 and Corollary 2.12, the only case we must consider is where $\dim V$ and q are both odd. Then any non-degenerate quadratic form is equivalent to either f or εf, where ε is a non-square in $K = \mathrm{GF}(q)$. A subspace is singular with respect to f if and only if it is singular with respect to εf, so there is no ambiguity in the definition of X.

The usual definition of dual polar space includes those coming from an alternating bilinear form and a hermitian form. In this lecture, however, we restrict our attention to the dual polar space of the above three types.

For the remainder of this section, we denote by X the dual polar space defined by a non-degenerate quadratic form f on V of Witt index d.

Lemma 3.1 *Let $U_1, U_2 \in X$ and $\dim U_1 \cap U_2 = d - k$. Then there exist hyperbolic pairs $\{u_{2i-1}, u_{2i}\}$ $(i = 1, \ldots, k)$ such that*

$$U_1 = \langle u_1, u_3, \ldots, u_{2k-1}\rangle \perp U_1 \cap U_2,$$

$$U_2 = \langle u_2, u_4, \ldots, u_{2k}\rangle \perp U_1 \cap U_2,$$

and

$$U_1 + U_2 = \langle u_1, u_2\rangle \perp \cdots \perp \langle u_{2k-1}, u_{2k}\rangle \perp U_1 \cap U_2.$$

Proof. The assertion is trivial if $U_1 = U_2$, so let us assume $U_1 \neq U_2$. We prove by induction on d. The case $d = 0$ is again trivial. Suppose $d \geq 1$. Pick a vector $u_1 \in U_1$ with $u_1 \notin U_2$. Then $u_1 \notin U_2^\perp$, since otherwise $U_2 \perp \langle u_1 \rangle$ would be a singular subspace, contradicting the maximality of U_2. Thus there exists a vector $u_2 \in U_2$ not orthogonal to u_1. Replacing u_2 by $B_f(u_1, u_2)^{-1} u_2$, we obtain a hyperbolic pair $\{u_1, u_2\}$. By Proposition 1.3, we have $V = P \perp P^\perp$ and $f|_{P^\perp}$ is non-degenerate, where $P = \langle u_1, u_2 \rangle$. Since f is non-degenerate and $f(u_2) = 0$, $\langle u_2 \rangle^\perp$ is a hyperplane of V by Lemma 1.4. Also $\langle u_2 \rangle^\perp$ does not contain U_1 since $u_1 \notin \langle u_2 \rangle^\perp$. It follows that $\dim U_1 \cap P^\perp = \dim U_1 \cap \langle u_1 \rangle^\perp \cap \langle u_2 \rangle^\perp = \dim U_1 \cap \langle u_2 \rangle^\perp = d - 1$. This implies that $U_1 \cap P^\perp$ is a maximal singular subspace of $(P^\perp, f|_{P^\perp})$, since the Witt index of $f|_{P^\perp}$ cannot exceed $d - 1$. Similarly, $U_2 \cap P^\perp$ is a maximal singular subspace of $(P^\perp, f|_{P^\perp})$, and $U_1 \cap U_2 \cap P^\perp = U_1 \cap U_2$. The induction hypothesis applied to $U_1 \cap P^\perp$ and $U_2 \cap P^\perp$ implies the existence of hyperbolic pairs $\{u_{2i-1}, u_{2i}\}$ $(i = 2, \ldots, k)$ such that

$$U_1 \cap P^\perp = \langle u_3, u_5, \ldots, u_{2k-1} \rangle \perp U_1 \cap U_2,$$
$$U_2 \cap P^\perp = \langle u_4, u_6, \ldots, u_{2k} \rangle \perp U_1 \cap U_2,$$

and

$$U_1 \cap P^\perp + U_2 \cap P^\perp = \langle u_3, u_4 \rangle \perp \cdots \perp \langle u_{2k-1}, u_{2k} \rangle \perp U_1 \cap U_2.$$

Since $U_1 = \langle u_1 \rangle \perp U_1 \cap P^\perp$ and $U_2 = \langle u_2 \rangle \perp U_2 \cap P^\perp$, we obtain the desired result. ∎

Theorem 3.2 *If $U_1, U_2, U_1', U_2' \in X$ and $\dim U_1 \cap U_2 = \dim U_1' \cap U_2'$, then there exists an isometry σ of V such that $\sigma(U_1) = U_1'$, $\sigma(U_2) = U_2'$.*

Proof. Suppose $\dim U_1 \cap U_2 = d - k$. Then by Lemma 3.1, there exist hyperbolic pairs $\{v_{2i-1}, v_{2i}\}$ $(i = 1, \ldots, k)$ such that

$$U_1 = \langle v_1, v_3, \ldots, v_{2k-1} \rangle \perp U_1 \cap U_2,$$

$$U_2 = \langle v_2, v_4, \ldots, v_{2k} \rangle \perp U_1 \cap U_2,$$

and

$$U_1 + U_2 = H \perp U_1 \cap U_2,$$

where $H = \langle v_1, v_2 \rangle \perp \cdots \perp \langle v_{2k-1}, v_{2k} \rangle$. By Proposition 1.3, we have $V = H \perp H^\perp$ and $H^\perp$ is non-degenerate. Also, $H^\perp$ contains a singular subspace $U_1 \cap U_2$ of dimension $d - k$. It follows that $U_1 \cap U_2$ is a maximal singular subspace of $H^\perp$ and $f|_{H^\perp}$ has Witt index $d - k$. By Proposition 2.4, there exist hyperbolic pairs $\{v_{2i-1}, v_{2i}\}$ $(i = k+1, \ldots, d)$ such that

$$U_1 \cap U_2 = \langle v_{2k+1}, v_{2k+3}, \ldots, v_{2d-1} \rangle,$$
$$H^\perp = \langle v_{2k+1}, v_{2k+2} \rangle \perp \cdots \perp \langle v_{2d-1}, v_{2d} \rangle \perp W,$$

where W is a subspace containing no nonzero singular vectors, and $\dim W = 0, 1$ or 2. Therefore,

$$V = \langle v_1, v_2 \rangle \perp \cdots \perp \langle v_{2d-1}, v_{2d} \rangle \perp W.$$

Similarly, we can find hyperbolic pairs $\{v_{2i-1}', v_{2i}'\}$ $(i = 1, \ldots, d)$ such that

$$V = \langle v_1', v_2' \rangle \perp \cdots \perp \langle v_{2d-1}', v_{2d}' \rangle \perp W',$$

where W is a subspace containing no nonzero singular vectors, $\dim W = 0, 1$ or 2,

$$U_1' = \langle v_1', v_3', \ldots, v_{2k-1}' \rangle \perp U_1' \cap U_2',$$

$$U_2' = \langle v_2', v_4', \ldots, v_{2k}' \rangle \perp U_1' \cap U_2',$$

$$U_1' \cap U_2' = \langle v_{2k+1}', v_{2k+3}', \ldots, v_{2d-1}' \rangle.$$

We want to show that $f|_W$ and $f|_{W'}$ are equivalent. This is the case if $\dim W = \dim W' = 0$ or 2, by Corollary 2.12. If $\dim W = \dim W' = 1$, and $f|_W$ is not equivalent to $f|_{W'}$, then f would be equivalent to both quadratic forms (2.1) and (2.2). This contradicts to Proposition 2.7. Therefore, there exists an isometry from W to W'. Extending this isometry by defining $v_i \mapsto v_i'$ $(i = 1, \ldots, 2d)$, we obtain the desired isometry. ■

The dual polar space becomes a metric space by defining a metric ∂ by $\partial(U_1, U_2) = d - \dim U_1 \cap U_2$. In order to check that ∂ is a metric, we need to verify the following.

(i) $\partial(U_1, U_2) \geq 0$,

(ii) $\partial(U_1, U_2) = 0$ if an only if $U_1 = U_2$,

(iii) $\partial(U_1, U_2) = \partial(U_2, U_1)$,

(iv) $\partial(U_1, U_2) + \partial(U_2, U_3) \geq \partial(U_1, U_3)$.

All but (iv) are obvious. The property (iv) is a consequence of the following lemma.

Lemma 3.3 *Let $U_1, U_2, U_3 \in X$. Then we have*

$$\dim U_1 \cap U_2 + \dim U_2 \cap U_3 \leq d + \dim U_1 \cap U_3. \tag{3.1}$$

Moreover, equality holds if and only if $U_1 \cap U_3 \subset U_2 = U_1 \cap U_2 + U_2 \cap U_3$.

Proof. We have

$$\begin{aligned} &\dim U_1 \cap U_2 + \dim U_2 \cap U_3 \\ &\quad = \dim(U_1 \cap U_2 + U_2 \cap U_3) + \dim U_1 \cap U_2 \cap U_3 \\ &\quad \leq \dim U_2 + \dim U_1 \cap U_3 \\ &\quad = d + \dim U_1 \cap U_3. \end{aligned}$$

Moreover, equality holds if and only if $U_1 \cap U_2 + U_2 \cap U_3 = U_2$ and $U_1 \cap U_2 \cap U_3 = U_1 \cap U_3$. ■

Lemma 3.4 *Let $U_1, U_2, U_3 \in X$. If $U_2 = U_1 \cap U_2 + U_2 \cap U_3$, then $U_1 \cap U_3 \subset U_2$. In particular, equality in* (3.1) *holds if and only if $U_2 = U_1 \cap U_2 + U_2 \cap U_3$.*

Proof. Since

$$\begin{aligned} U_1 \cap U_3 &\subset U_1^\perp \cap U_3^\perp \\ &\subset (U_1 \cap U_2)^\perp \cap (U_2 \cap U_3)^\perp \\ &= (U_1 \cap U_2 + U_2 \cap U_3)^\perp \\ &= U_2^\perp, \end{aligned}$$

the subspace $U_1 \cap U_3 + U_2$ is singular. By the maximality of U_2, we obtain $U_1 \cap U_3 \subset U_2$. ■

Our next task is to show that this metric coincides with the distance in a graph defined on X.

Definition. The dual polar graph of type $D_d(q), B_d(q), {}^2D_{d+1}(q)$ is the graph with the dual polar space X of type $D_d(q), B_d(q), {}^2D_{d+1}(q)$, respectively, as the vertex set, where two vertices $U_1, U_2 \in X$ are adjacent if and only if $\dim U_1 \cap U_2 = d - 1$.

In a graph, the distance between two vertices is the minimum of the length of paths joining the two vertices.

Lemma 3.5 *Let $W_0, W_1, \dots, W_k \in X$ be a path, that is, (W_{i-1}, W_i) is an edge of the dual polar graph for all $i = 1, \dots, k$. Then $\dim W_0 \cap W_k + k \geq d$.*

Proof. We prove by induction on k. If $k = 0$ the assertion is trivial. Suppose $k > 1$. By induction we have $\dim W_0 \cap W_{k-1} + k - 1 \geq d$, so that

$$\begin{aligned} \dim W_0 \cap W_k + k &\geq \dim W_0 \cap W_{k-1} \cap W_k + k \\ &= \dim W_0 \cap W_{k-1} + \dim W_{k-1} \cap W_k \\ &\quad - \dim(W_0 \cap W_{k-1} + W_{k-1} \cap W_k) + k \\ &\geq (d - k + 1) + (d - 1) - \dim W_{k-1} + k \\ &= d, \end{aligned}$$

as desired. ■

Proposition 3.6 *The metric ∂ on the dual polar space X coincides with the distance in the dual polar graph on X.*

Proof. Let $U_1, U_2 \in X$ and $\partial(U_1, U_2) = j$. By Lemma 3.1, there exist hyperbolic pairs $\{u_{2i-1}, u_{2i}\}$ $(i = 1, \dots, j)$ such that

$$U_1 = \langle u_1, u_3, \dots, u_{2j-1} \rangle \perp (U_1 \cap U_2),$$

$$U_2 = \langle u_2, u_4, \dots, u_{2j} \rangle \perp (U_1 \cap U_2).$$

and

$$U_1 + U_2 = \langle u_1, u_2 \rangle \perp \cdots \perp \langle u_{2j-1}, u_{2j} \rangle \perp (U_1 \cap U_2).$$

Define a sequence of singular subspaces $W_0, \ldots, W_j$ by

$$\begin{aligned}
W_0 &= \langle u_1, u_3, \ldots, u_{2j-1} \rangle \perp (U_1 \cap U_2) = U_1, \\
W_1 &= \langle u_2, u_3, \ldots, u_{2j-1} \rangle \perp (U_1 \cap U_2), \\
&\vdots \\
W_{j-1} &= \langle u_2, u_4, \ldots, u_{2j-2}, u_{2j-1} \rangle \perp (U_1 \cap U_2), \\
W_j &= \langle u_2, u_4, \ldots, u_{2j-2}, u_{2j} \rangle \perp (U_1 \cap U_2) = U_2.
\end{aligned}$$

Then each pair (W_i, W_{i+1}) is adjacent in the dual polar graph. Thus the distance between U_1 and U_2 in the dual polar graph is at most j.

Conversely, let $U_1 = W_0, \ldots, W_k = U_2$ be a path of length k joining U_1 and U_2. By Lemma 3.5, we have $k \geq d - \dim W_0 \cap W_k = \partial(U_1, U_2) = j$. Therefore, the distance between U_1 and U_2 in the dual polar graph is exactly j. ■

Definition. Let Γ be a connected graph whose distance is denoted by ∂. The graph Γ is called distance-transitive if, for any vertices x, x', y, y' with $\partial(x, y) = \partial(x', y')$, there exists an automorphism σ of Γ such that $\sigma(x) = x'$ and $\sigma(y) = y'$.

Theorem 3.7 *The dual polar graph is distance-transitive.*

Proof. This follows immediately from Theorem 3.2 and Proposition 3.6. ■

4 Computation of parameters

Definition. Let Γ be a graph. We denote by $\Gamma_i(x)$ the set of vertices of Γ which are distance i from x. We also write $\Gamma(x) = \Gamma_1(x)$. A connected graph is called distance-regular if, for any vertices x, y with $y \in \Gamma_i(x)$, $|\Gamma_{i+1}(x) \cap \Gamma(y)| = b_i$ and $|\Gamma_{i-1}(x) \cap \Gamma(y)| = c_i$ hold, where b_i and c_i depend only on i and independent of the vertices x, y. If Γ has diameter d, then the numbers b_i $(0 \le i \le d-1)$ and c_i $(1 \le i \le d)$ are called the parameters of the distance-regular graph Γ.

Clearly, a distance-transitive graph is distance-regular. In particular, the dual polar graph is distance-regular of diameter d, where d is the Witt index. In this section we compute the parameters of dual polar graphs explicitly.

Definition. If V is a vector space of dimension n over $\mathrm{GF}(q)$, then the number of m-dimensional subspaces of V is denoted by $\begin{bmatrix} n \\ m \end{bmatrix}$. As is well-known, we have

$$\begin{bmatrix} n \\ m \end{bmatrix} = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-m+1} - 1)}{(q^m - 1)(q^{m-1} - 1) \cdots (q - 1)}, \tag{4.1}$$

$$\begin{bmatrix} n \\ m \end{bmatrix} = \begin{bmatrix} n \\ n-m \end{bmatrix}. \tag{4.2}$$

Indeed, counting in two ways the number of elements in the set

$$\{(v_1, v_2, \ldots, v_m, U) | U = \langle v_1, v_2, \ldots, v_m \rangle,\ \dim U = m\}$$

we obtain

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{m-1}) = \begin{bmatrix} n \\ m \end{bmatrix} (q^m - 1)(q^m - q) \cdots (q^m - q^{m-1}),$$

from which (4.1) follows. The equality (4.2) follows immediately from (4.1).

For the remainder of this section, we assume that f is a non-degenerate quadratic form of Witt index d on a vector space V over $\mathrm{GF}(q)$, and $\dim V = 2d + e$, $e = 0, 1, 2$. We begin by counting the number of singular vectors.

Proposition 4.1 *The number of singular vectors in V is given by*

$$q^{2d+e-1} - q^{d+e-1} + q^d.$$

Proof. We prove by induction on d. The case $d = 0$ is trivial. Suppose $d \ge 1$. By Proposition 2.4, we can write $V = P_1 \perp P_2 \perp \cdots \perp P_d \perp W$, where P_i $(i = 1, \ldots, d)$ are hyperbolic planes, W is a subspace containing no nonzero singular vectors, $\dim W = e$. Let $\{v_1, v_2\}$ be a hyperbolic pair spanning P_1, and put $V' = P_2 \perp \cdots \perp P_d \perp W$. Then by induction, the number of singular vectors in V' is $q^{2d+e-3} - q^{d+e-2} + q^{d-1}$. Thus the number of singular vectors in V is given by

$$\begin{aligned} &|\{v \in V | f(v) = 0\}| \\ &= |\{\lambda_1 v_1 + \lambda_2 v_2 + v' | \lambda_1, \lambda_2 \in K,\ v' \in V',\ \lambda_1 \lambda_2 + f(v') = 0\}| \end{aligned}$$

$$\begin{aligned}
&= |\{\lambda_1 v_1 + \lambda_2 v_2 + v' | \lambda_1, \lambda_2 \in K,\ v' \in V',\ \lambda_1\lambda_2 = 0,\ f(v') = 0\}| \\
&\quad +|\{\lambda_1 v_1 + \lambda_2 v_2 + v' | \lambda_1, \lambda_2 \in K,\ v' \in V',\ \lambda_1\lambda_2 = -f(v') \neq 0\}| \\
&= (2q-1)|\{v' \in V' | f(v') = 0\}| \\
&\quad +(q-1)(q^{\dim V'} - |\{v' \in V' | f(v') = 0\}|) \\
&= q^{\dim V'}(q-1) + q|\{v' \in V' | f(v') = 0\}| \\
&= q^{2(d-1)+e}(q-1) + q(q^{2d+e-3} - q^{d+e-2} + q^{d-1}) \\
&= q^{2d+e-1} - q^{d+e-1} + q^d.
\end{aligned}$$

as desired. ■

Lemma 4.2 *If W is a singular subspaces of V, then f induces a non-degenerate quadratic form of Witt index $d - \dim W$ on $W^\perp/W$. There is a one-to-one correspondence between singular subspaces of $W^\perp/W$ and singular subspaces of V containing W.*

Proof. First note that $f(v+w) = f(v)$ for any $v \in W^\perp$ and $w \in W$. Thus the mapping $\bar{f} : W^\perp/W \longrightarrow K$, $\bar{f}(v+w) = f(v)$ is well-defined. One checks easily that $\bar{f}$ is a quadratic form. If $v + W \in \text{Rad}\,\bar{f}$, then $f(v) = 0$ and $B_{\bar{f}}(v+W, v'+W) = 0$ for all $v' \in W^\perp$. Since

$$\begin{aligned}
B_{\bar{f}}(v+W, v'+W) &= \bar{f}((v+W) + (v'+W)) - \bar{f}(v+W) - \bar{f}(v'+W) \\
&= f(v+v') - f(v) - f(v') \\
&= B_f(v, v'),
\end{aligned}$$

it follows that $v \in \text{Rad}\,(f|_{W^\perp})$. By Lemma 1.4, we have $v \in W$. Therefore, $\text{Rad}\,\bar{f} = 0$. Note that any singular subspace containing W is contained in $W^\perp$. Note also that there is a one-to-one correspondence between subspaces of $W^\perp/W$ and subspaces of $W^\perp$ containing W. Clearly, singular subspaces of $W^\perp/W$ correspond to singular subspaces of $W^\perp$ containing W. ■

Proposition 4.3 *The number of singular k-dimensional subspaces of V is given by*

$$\begin{bmatrix} d \\ k \end{bmatrix} \prod_{i=0}^{k-1} (q^{d+e-i-1} + 1).$$

Proof. We prove by induction on k. The case $k = 0$ is trivial. Suppose that the formula is valid up to k. We want to count the number of elements in the set

$$S = \{(U, \tilde{U}) | U, \tilde{U} \text{ are singular, } \dim U = k,\ \dim \tilde{U} = k+1 \text{ and } U \subset \tilde{U}\}.$$

Clearly

$$|S| = |\{\tilde{U} | \tilde{U} \text{ is singular, } \dim \tilde{U} = k+1\}| \begin{bmatrix} k+1 \\ k \end{bmatrix}.$$

By Lemma 4.2 and induction, we have

$$\begin{aligned}
|S| &= |\{U | U \text{ is singular, } \dim U = k\}| \\
&\times\ |\{\bar{W} \subset U^\perp/U | \bar{W} \text{ is singular, } \dim \bar{W} = 1\}| \\
&= \begin{bmatrix} d \\ k \end{bmatrix} \prod_{i=0}^{k-1} (q^{d+e-i-1} + 1) \frac{(q^{d-k} - 1)(q^{d-k+e-1} + 1)}{q-1}.
\end{aligned}$$

Therefore, the number of singular $(k+1)$-dimensional subspaces is

$$\begin{aligned}
&\begin{bmatrix} d \\ k \end{bmatrix} \prod_{i=0}^{k-1} (q^{d+e-i-1}+1) \frac{(q^{d-k}-1)(q^{d-k+e-1}+1)}{q-1} \frac{q-1}{q^{k+1}-1} \\
&= \frac{(q^d-1)\cdots(q^{d-k+1}-1)(q^{d-k}-1)}{(q^{k+1}-1)(q^k-1)\cdots(q-1)} \prod_{i=0}^{k} (q^{d+e-i-1}+1) \\
&= \begin{bmatrix} d \\ k+1 \end{bmatrix} \prod_{i=0}^{k} (q^{d+e-i-1}+1),
\end{aligned}$$

as desired. ■

Theorem 4.4 *Let Γ be the dual polar graph with vertex set X consisting of the maximal singular subspaces of V. Then Γ is a distance-regular graph with parameters*

$$b_i = \frac{q^{i+e}(q^{d-i}-1)}{q-1} \quad (i = 0, \dots, d-1), \tag{4.3}$$

$$c_i = \frac{q^i - 1}{q-1} \quad (i = 1, \dots, d), \tag{4.4}$$

Proof. Let $U_1, U_2 \in X$ and $\partial(U_1, U_2) = i$. To prove (4.3), assume $0 \le i \le d-1$ and put

$$Y = \{(W, U) | U \in X, \ \dim U \cap U_1 = d - i - 1, \ W = U \cap U_2, \ \dim W = d-1\}.$$

Clearly the correspondence $(W, U) \mapsto U$, $Y \longrightarrow \Gamma_{i+1}(U_1) \cap \Gamma(U_2)$ is a bijection, so $|Y| = b_i$. If $(W, U) \in Y$, then W is a hyperplane of U_2. Moreover, since $W \cap (U_1 \cap U_2) = U \cap U_1 \cap U_2 \subset U \cap U_1$ and $\dim U \cap U_1 = d - i - 1 < d - i = \dim U_1 \cap U_2$, W does not contain $U_1 \cap U_2$. Let Z be the set of such subspaces W, that is,

$$Z = \{W | W \subset U_2, \ \dim W = d-1, \ W \not\supset U_1 \cap U_2\}.$$

For $W \in Z$, set

$$Y_W = \{U \in X | W \subset U \neq U_2\}.$$

Note that if $U \in Y_W$, then $W = U \cap U_2$. Indeed, $W \subset U \cap U_2$ and $\dim W = d-1$, $\dim U \cap U_2 < d$. Thus the sets Y_W $(W \in Z)$ are mutually disjoint. We want to show

$$Y = \bigcup_{W \in Z} \{(W, U) | U \in Y_W\}. \tag{4.5}$$

We have already shown that Y is contained in the right hand side. To prove the reverse containment, pick $W \in Z$ and $U \in Y_W$. Then $W = U \cap U_2$. Since $W = U \cap U_2$ is a hyperplane of U_2 not containing $U_1 \cap U_2$, we have $U_2 = U \cap U_2 + U_1 \cap U_2$. By Lemma 3.4, we have

$$\dim U \cap U_2 + \dim U_1 \cap U_2 = d + \dim U \cap U_1.$$

In other words, $\dim U \cap U_1 = d - i - 1$, which establishes $(W, U) \in Y$. This completes the proof of (4.5). Now $|Y|$ can be computed as follows. Note that there exists a one-to-one correspondence between singular d-dimensional subspaces containing W and singular 1-dimensional subspaces in $W^\perp/W$ in the sense of Lemma 4.2. Since $W^\perp/W$ has Witt index 1 and dimension $2+e$, the number of singular 1-dimensional subspaces in $W^\perp/W$ is q^e+1 by Proposition 4.3. It follows that $|Y_W| = q^e$ for any $W \in Z$ and hence

$$|Z| = \begin{bmatrix} d \\ d-1 \end{bmatrix} - \begin{bmatrix} i \\ i-1 \end{bmatrix} = \frac{q^d - q^i}{q-1},$$

$$|Y| = \frac{q^{e+i}(q^{d-i}-1)}{q-1}.$$

This proves the formula (4.3).

To prove (4.4), assume $1 \le i \le d$ and set

$$Y = \{W | U_1 \cap U_2 \subset W \subset U_2,\ \dim W = d-1\}.$$

We want to show that the mapping $\varphi : \Gamma_{i-1}(U_1) \cap \Gamma(U_2) \longrightarrow Y$, $U \mapsto U \cap U_2$ is a bijection. If $U \in \Gamma_{i-1}(U_1) \cap \Gamma(U_2)$, then by the second part of Lemma 3.3 we see $U_1 \cap U_2 \subset U$. Thus we have $U_1 \cap U_2 \subset U \cap U_2 \subset U_2$ which shows that φ is well-defined. We shall show that the inverse mapping of φ is given by $\psi : Y \longrightarrow \Gamma_{i-1}(U_1) \cap \Gamma(U_2)$, $W \mapsto W + W^\perp \cap U_1$. First note that $W \cap U_1 = U_1 \cap U_2$ for any $W \in Y$. By Lemma 1.4,

$$\begin{aligned}
\dim W^\perp \cap U_1 &= \dim W^\perp + \dim U_1 - \dim(W^\perp + U_1) \\
&\ge \dim V - \dim W + d - \dim((U_1 \cap U_2)^\perp + U_1) \\
&= \dim V + 1 - \dim(U_1 \cap U_2)^\perp \\
&= 1 + \dim U_1 \cap U_2 \\
&= d - i + 1. \qquad (4.6)
\end{aligned}$$

Thus

$$\begin{aligned}
\dim(W + W^\perp \cap U_1) &= \dim W + \dim W^\perp \cap U_1 - \dim W \cap W^\perp \cap U_1 \\
&\ge (d-1) + (d-i+1) - \dim W \cap U_1 \\
&= 2d - i - \dim U_1 \cap U_2 \\
&= d.
\end{aligned}$$

Clearly $W + W^\perp \cap U_1$ is singular, so $\dim(W + W^\perp \cap U_1) = d$ and equality in (4.6) holds. This means $(W + W^\perp \cap U_1) \cap U_1 = W \cap U_1 + W^\perp \cap U_1 = W^\perp \cap U_1$ has dimension $d-i+1$, that is, $W + W^\perp \cap U_1 \in \Gamma_{i-1}(U_1)$. Also $(W + W^\perp \cap U_1) \cap U_2 = W + W^\perp \cap U_1 \cap U_2 = W$. This shows $W + W^\perp \cap U_1 \in \Gamma(U_2)$, and at the same time $\varphi \circ \psi$ is the identity mapping on Y. It remains to show $\psi \circ \varphi(U) = U$ for all $U \in \Gamma_{i-1}(U_1) \cap \Gamma(U_2)$. By Lemma 3.3, we have

$$\begin{aligned}
U &= U \cap U_2 + U \cap U_1 \\
&\subset U \cap U_2 + (U \cap U_2)^\perp \cap U_1 \\
&= \psi \circ \varphi(U).
\end{aligned}$$

Since we already know $\psi \circ \varphi(U) \in X$, this forces $U = \psi \circ \varphi(U)$. Therefore, we have established a one-to-one correspondence between Y and $\Gamma_{i-1}(U_1) \cap \Gamma(U_2)$. Since the set Y is in one-to-one correspondence with the set of hyperplanes in $U_2/U_1 \cap U_2$, we see

$$c_i = |\Gamma_{i-1}(U_1) \cap \Gamma(U_2)| = |Y| = \begin{bmatrix} i \\ i-1 \end{bmatrix} = \frac{q^i - 1}{q - 1}.$$

This completes the proof. ■

Definition. A graph is called complete (or clique) if any two of its vertices are adjacent. A coclique is a graph in which no two vertices are adjacent. A graph is called bipartite if its vertex set can be partitioned into two cocliques.

Theorem 4.5 *The dual polar graph of type $D_d(q)$ is bipartite.*

Proof. Fix a vertex $U \in X$. By Theorem 4.4,

$$b_i + c_i = \frac{q^i(q^{d-i} - 1)}{q - 1} + \frac{q^i - 1}{q - 1} = \frac{q^d - 1}{q - 1} = b_0 \quad (i = 0, 1, \dots, d),$$

with the convention $b_d = c_0 = 0$. This implies that $\Gamma_i(U)$ is a coclique for every $i = 0, 1, \dots, d$. Thus X is partitioned into the sets

$$X_1 = \Gamma_1(U) \cup \Gamma_3(U) \cup \cdots,$$

$$X_2 = \{U\} \cup \Gamma_2(U) \cup \Gamma_4(U) \cup \cdots,$$

which are cocliques. ■

5 Structure of subconstituents

In this section we discuss the structure of the subconstituents $\Gamma(U)$ and $\Gamma_d(U)$ of the dual polar graph Γ of diameter d. As before, let f be a non-degenerate quadratic form of Witt index d on a vector space V over $\mathrm{GF}(q)$, and $\dim V = 2d+e$, $e=0,1,2$. Let Γ be the dual polar graph with vertex set X consisting of the maximal singular subspaces of V.

Theorem 5.1 *Let $U_1 \in X$. The subgraph $\Gamma(U_1)$ is the disjoint union of cliques*

$$\{U \in X | W \subset U \neq U_1\} \quad (W \subset U,\ \dim W = d-1), \tag{5.1}$$

without edges joining them, each of which has size q^e.

Proof. Clearly, the sets (5.1) are mutually disjoint cliques. By Lemma 4.2, the number of elements in X containing W is the same as the number of singular 1-dimensional subspace in $W^\perp/W$, which is, by Proposition 4.3, q^e+1. Thus we see that each of the sets (5.1) has size q^e. By Theorem 4.4, the valency of $\Gamma(U_1)$ is

$$b_0 - b_1 - c_1 = \frac{q^e(q^d-1)}{q-1} - \frac{q^{e+1}(q^{d-1}-1)}{q-1} - 1 = q^e - 1.$$

This implies that there are no edges in $\Gamma(U_1)$ other than those contained in some subset of the form (5.1). ∎

Definition. The graph of alternating bilinear form $\mathrm{Alt}(d,q)$ has

$$Y = \{A | A \text{ is an alternating matrix with entries in } \mathrm{GF}(q)\}$$

as vertex set, two vertices A, B are adjacent whenever $\mathrm{rank}(A-B) = 2$.

Theorem 5.2 *Let Γ be the dual polar graph of type $D_d(q)$, U_0 a vertex of Γ. Let Δ be the graph with vertex set $\Gamma_d(U_0)$, where two vertices U_1, U_2 are adjacent whenever* $\dim U_1 \cap U_2 = d-2$. *Then Δ is isomorphic to* $\mathrm{Alt}(d,q)$.

Proof. In view of Theorem 2.11, we may assume the quadratic form f is defined by

$$f(\sum_{i=1}^{2d} \xi_i u_i) = \sum_{i=1}^{d} \xi_i \xi_{d+i},$$

where $\{u_1, u_2, \ldots, u_{2d}\}$ is a basis of V. Also by Theorem 3.2 we may assume $U_0 = \langle u_1, u_2, \ldots, u_d \rangle$. Define a mapping φ from Y to $\Gamma_d(U_0)$ by

$$A = (a_{ij}) \mapsto \langle \sum_{i=1}^{d} a_{ij} u_i + u_{d+j} | j = 1, 2, \ldots, d \rangle.$$

Since

$$f(\sum_{i=1}^{d} a_{ij} u_i + u_{d+j}) = B_f(\sum_{i=1}^{d} a_{ij} u_i, u_{d+j}) = a_{jj}, \tag{5.2}$$

$$
\begin{aligned}
&B_f(\sum_{i=1}^{d} a_{ij}u_i + u_{d+j}, \sum_{i=1}^{d} a_{ik}u_i + u_{d+k}) \\
&\quad = B_f(\sum_{i=1}^{d} a_{ij}u_i, u_{d+k}) + B_f(u_{d+j}, \sum_{i=1}^{d} a_{ik}u_i) \\
&\quad = a_{kj} + a_{jk}, \qquad (5.3)
\end{aligned}
$$

and (a_{ij}) is alternating, we see that $\varphi(A)$ is singular. One checks easily $\dim \varphi(A) = d$ and $U_0 \cap \varphi(A) = 0$. Thus we have shown that φ is well-defined. Next we show that φ is injective. Suppose $\varphi((a_{ij})) = \varphi((b_{ij}))$. Then we have

$$
\sum_{i=1}^{d} a_{ij}u_i + u_{d+j} = \sum_{k=1}^{d} \lambda_k (\sum_{i=1}^{d} b_{ik}u_i + u_{d+k})
$$

for some $\lambda_k \in \mathrm{GF}(q)$. Comparing the coefficients of u_{d+k} for $k = 1, \ldots, d$, we find $\lambda_k = \delta_{jk}$ and $\sum_{i=1}^{d} a_{ij}u_i = \sum_{i=1}^{d} b_{ij}u_i$. This implies $a_{ij} = b_{ij}$, hence φ is injective. Next we show that φ is surjective. Suppose $U \in \Gamma_d(U_0)$. Let $\{v_1, \ldots, v_d\}$ be a basis of U and write

$$
v_j = \sum_{i=1}^{d} b_{ij}u_i + \sum_{i=1}^{d} c_{ij}u_{d+i} \quad (j = 1, 2, \ldots, d).
$$

If the $d \times d$ matrix $C = (c_{ij})$ is singular, then there exists a nonzero vector $(\alpha_1, \ldots, \alpha_d)$ $\in \mathrm{GF}(q)^d$ such that $\sum_{j=0}^{d} \alpha_j c_{ij} = 0$ for all $i = 1, \ldots, d$. But this implies $0 \neq \sum_{j=0}^{d} \alpha_j v_j \in U_0 \cap U$, which is a contradiction. Thus C is nonsingular. Put $A = (a_{ij}) = (b_{ij})C^{-1}$ and $w_k = \sum_{i=1}^{d} a_{ik}u_i + u_{d+k}$ $(k = 1, \ldots, d)$. Then

$$
\begin{aligned}
w_k &= \sum_{i=1}^{d}\sum_{j=1}^{d} b_{ij}(C^{-1})_{jk}u_i + \sum_{i=1}^{d} \delta_{ik}u_{d+i} \\
&= \sum_{j=1}^{d} (C^{-1})_{jk} \sum_{i=1}^{d} b_{ij}u_i + \sum_{i=1}^{d}\sum_{j=1}^{d} c_{ij}(C^{-1})_{jk}u_{d+i} \\
&= \sum_{j=1}^{d} (C^{-1})_{jk}v_j,
\end{aligned}
$$

so that $\{w_1, \ldots, w_d\}$ is a basis of U. Since U is singular, (5.2) and (5.3) imply that A is alternating. This shows $\varphi(A) = U$, proving the surjectivity. Finally we want to prove that φ preserves adjacency. Let $A, B \in Y$. Then

$$
\begin{aligned}
\dim \varphi(A) \cap \varphi(B) &= 2d - \dim(\varphi(A) + \varphi(B)) \\
&= 2d - \mathrm{rank} \begin{pmatrix} A & B \\ I & I \end{pmatrix} \\
&= 2d - \mathrm{rank} \begin{pmatrix} A - B & B \\ 0 & I \end{pmatrix} \\
&= d - \mathrm{rank}(A - B).
\end{aligned}
$$

This implies $\mathrm{rank}(A - B) = 2$ if and only if $\dim \varphi(A) \cap \varphi(B) = d - 2$. Therefore, φ is an isomorphism of the graphs $\mathrm{Alt}(d, q)$ and Δ. ■

Definition. Let Γ be a bipartite graph whose vertex set X has a bipartition $X_1 \cup X_2$. A bipartite half of Γ is the graph with vertex set X_1, and two vertices are adjacent if and only if their distance in Γ is 2.

Theorem 5.3 *Let $\tilde{\Gamma}, \Gamma$ be the dual polar graphs of type $D_{d+1}(q), B_d(q)$, respectively. Let $\tilde{\Lambda}$ be a bipartite half of $\tilde{\Gamma}$, and let Λ be the graph with the same vertex set as Γ, and two vertices U_1, U_2 of Λ are adjacent whenever $\dim U_1 \cap U_2 = d-1$ or $d-2$. Then $\tilde{\Lambda}$ is isomorphic to Λ. Choose a vertex $\tilde{U}_0$ of $\tilde{\Gamma}$ such that $\tilde{\Gamma}_{d+1}(\tilde{U}_0)$ is contained in the vertex set of $\tilde{\Lambda}$, and pick a vertex U_0 of Γ. Let $\tilde{\Delta}$ be the subgraph of $\tilde{\Lambda}$ induced on $\tilde{\Gamma}_{d+1}(\tilde{U}_0)$, and let Δ be the subgraph of Λ induced on $\Gamma_d(U_0)$. Then $\tilde{\Delta}$ is isomorphic to Δ.*

Proof. Let f be a non-degenerate quadratic form of Witt index $d+1$ on $\tilde{V}$, where $\dim \tilde{V} = 2d+2$. We may assume that f is given by

$$f(\sum_{i=1}^{2d+2} \xi_i u_i) = \sum_{i=1}^{d} \xi_i \xi_{d+i} + \xi_{2d+1}\xi_{2d+2}.$$

where $\{u_1, \dots, u_{2d+2}\}$ is a basis of $\tilde{V}$. Let $\tilde{\Gamma}$ be the dual polar graph of type $D_{d+1}(q)$ with vertex set $\tilde{X}$ consisting of the maximal singular subspaces of $\tilde{V}$. We may assume $\tilde{U}_0 = \langle u_1, u_2, \dots, u_d, u_{2d+1}\rangle$, and that $\tilde{\Lambda}$ is the bipartite half of $\tilde{\Gamma}$ with vertex set $\tilde{X}_1$ containing $\tilde{\Gamma}_{d+1}(\tilde{U}_0)$. Put $v = u_{2d+1} + u_{2d+2}$, $V = \langle v\rangle^{\perp}$. Since $f(v) = 1$, V is non-degenerate by Proposition 1.3. Let Γ be the dual polar graph of type $B_d(q)$ with vertex set X consisting of the maximal singular subspaces of V. We may assume $U_0 = \langle u_1, u_2, \dots, u_d\rangle$. We define a mapping $\varphi : \tilde{X}_1 \longrightarrow X$ by $\varphi(\tilde{U}) = \tilde{U} \cap V$ and show that φ is an isomorphism from $\tilde{\Lambda}$ to Λ.

Clearly, $\tilde{U} \cap V$ is a singular d-dimensional subspace of V for any $\tilde{U} \in \tilde{X}_1$. If $\tilde{U}_1 \cap V = \tilde{U}_2 \cap V$ for some $\tilde{U}_1, \tilde{U}_2 \in \tilde{X}_1$, then $\dim \tilde{U}_1 \cap \tilde{U}_2 \geq d$. Since $\tilde{X}_1$ is a coclique in $\tilde{\Gamma}$, this forces $\tilde{U}_1 = \tilde{U}_2$. Thus φ is injective. If $U \in X$, then by Lemma 4.2, the number of elements in $\tilde{X}$ containing U is the same as the number of singular 1-dimensional subspace in $U^{\perp}/U$, which is 2 by Proposition 4.3. Let $\tilde{U}_1, \tilde{U}_2$ be the elements of $\tilde{X}$ containing U. Then $\tilde{U}_1$ and $\tilde{U}_2$ are adjacent in $\tilde{\Gamma}$. Thus one of $\tilde{U}_1$ or $\tilde{U}_2$ belongs to $\tilde{X}_1$. Also $U = \tilde{U}_1 \cap V = \tilde{U}_2 \cap V$. This proves the surjectivity of φ.

Suppose $\tilde{U}_1, \tilde{U}_2 \in \tilde{X}_1$. Since $\varphi(\tilde{U}_1) \cap \varphi(\tilde{U}_2) = \tilde{U}_1 \cap \tilde{U}_2 \cap V$, we have $\dim \tilde{U}_1 \cap \tilde{U}_2 = \dim \varphi(\tilde{U}_1) \cap \varphi(\tilde{U}_2)$ or $\dim \varphi(\tilde{U}_1) \cap \varphi(\tilde{U}_2) + 1$. Since $d + 1 - \dim \tilde{U}_1 \cap \tilde{U}_2 = \partial(\tilde{U}_1, \tilde{U}_2)$ is even, this implies that

$$\dim \tilde{U}_1 \cap \tilde{U}_2 = d-1 \quad \Longleftrightarrow \quad \dim \varphi(\tilde{U}_1) \cap \varphi(\tilde{U}_2) = d-1 \text{ or } d-2.$$

Therefore, φ is an isomorphism from $\tilde{\Lambda}$ to Λ.

Let us restrict the isomorphism φ to $\tilde{\Gamma}_{d+1}(\tilde{U}_0)$. Note that $\varphi(\tilde{U}) \cap U_0 = \tilde{U} \cap \tilde{U}_0 \cap V$ for any $\tilde{U} \in \tilde{X}_1$. Thus, in particular, $\varphi(\tilde{U}) \in \Gamma_d(U_0)$ for any $\tilde{U} \in \tilde{\Gamma}_{d+1}(\tilde{U}_0)$. Conversely, if $\varphi(\tilde{U}) \in \Gamma_d(U_0)$, then $\dim \tilde{U} \cap \tilde{U}_0 \leq 1$. This implies $\tilde{U} \in \tilde{\Gamma}_d(\tilde{U}_0) \cup \tilde{\Gamma}_{d+1}(\tilde{U}_0)$. Since $\tilde{U} \in \tilde{X}_1$, we obtain $\tilde{U} \in \tilde{\Gamma}_{d+1}(\tilde{U}_0)$. Therefore, φ induces a bijection between $\tilde{\Gamma}_{d+1}(\tilde{U}_0)$ and $\Gamma_d(U_0)$. As φ is an isomorphism from $\tilde{\Lambda}$ to Λ, the restriction of φ to $\tilde{\Gamma}_{d+1}(\tilde{U}_0)$ is an isomorphism from $\tilde{\Delta}$ to Δ. ■

The graph Λ in Theorem 5.3 is known as the distance 1-or-2 graph of Γ, since two vertices are adjacent in Λ if and only if their distance in Γ is 1 or 2, by Proposition 3.6.

It is important to note, however, that the graph Δ is not the distance 1-or-2 graph of the subgraph induced on $\Gamma_d(U_0)$ by Γ. We shall determine which pair of vertices in $\Gamma_d(U_0)$ at distance 2 apart in Γ are at distance 2 in the subgraph induced on $\Gamma_d(U_0)$ by Γ.

Proposition 5.4 *Let Γ be the dual polar graph of type $B_d(q)$ and let U_0 be a vertex of Γ. Suppose $U_1, U_2 \in \Gamma_d(U_0)$ and $\dim U_1 \cap U_2 = d-2$. Then $\dim(U_1+U_2) \cap U_0 = 1$ or 2. Moreover, there exists a path of length 2 joining U_1 and U_2 in $\Gamma_d(U_0)$ if and only if $\dim U_0 \cap (U_1+U_2) = 1$.*

Proof. Since $2d = \dim(U_0+U_1) \le \dim(U_0+U_1+U_2) \le 2d+1$, we have

$$\begin{aligned}\dim U_0 \cap (U_1+U_2) &= \dim U_0 + \dim(U_1+U_2) - \dim(U_0+U_1+U_2)\\ &= 2d+2-\dim(U_0+U_1+U_2)\\ &= 1 \text{ or } 2.\end{aligned}$$

Suppose $\dim U_0 \cap (U_1+U_2) = 1$, say $U_0 \cap (U_1+U_2) = \langle u_0\rangle$. Since $U_1 \cap U_2$ and $U_1 \cap \langle u_0\rangle^\perp$ cannot cover U_1, we can find a vector $u_1 \in U_1$ such that $u_1 \notin U_2$, $u_1 \notin \langle u_0\rangle^\perp$. Since $\dim U_2 \cap \langle u_1\rangle^\perp = d-1 > d-2 = \dim U_1 \cap U_2$, we can find a vector $u_2 \in U_2 \cap \langle u_1\rangle^\perp$ such that $u_2 \notin U_1$. The subspace $U = \langle u_1, u_2\rangle \perp U_1 \cap U_2$ is a singular subspace adjacent to both U_1 and U_2. Since $U \subset U_1+U_2$, we have $U_0 \cap U \subset \langle u_0\rangle$. But we have $u_0 \notin \langle u_1\rangle^\perp \supset U$, so that $U_0 \cap U = 0$. Therefore, (U_1, U, U_2) is a path of length 2 in $\Gamma_d(U_0)$ joining U_1 and U_2.

Next suppose $\dim U_0 \cap (U_1+U_2) = 2$. Put $H = U_0+U_1+U_2$. Then $\dim H = 2d$, hence $H = U_0+U_1$, which is non-degenerate by Lemma 3.1. We can regard U_0, U_1, U_2 as vertices of the dual polar graph Σ of type $D_d(q)$ defined on H, and then $U_1, U_2 \in \Sigma_d(U_0)$. Suppose that there exists a path (U_1, U, U_2) of length 2 in $\Gamma_d(U_0)$. By Lemma 3.3 we have $U = U \cap U_1 + U \cap U_2 \subset U_1+U_2 \subset H$. This implies $U \in \Sigma_d(U_0)$. This is a contradiction since $\Sigma_d(U_0)$ has no edge by Theorem 4.5. ■

Both cases in Proposition 5.4 do occur. With the notation of the proof of Theorem 5.3, put

$$U_1 = \langle u_{d+1}, u_{d+2}, \ldots, u_{2d}\rangle \in \Gamma_d(U_0),$$

$$U_2 = \langle u_2+u_{d+1}, u_1-u_{d+2}, u_{d+3}, \ldots, u_{2d}\rangle \in \Gamma_d(U_0).$$

Then $\dim U_1 \cap U_2 = d-2$ and $(U_1+U_2)\cap U_0 = \langle u_1, u_2\rangle$. If we put

$$U_2' = \langle u_1-u_{d+1}+v, u_1+u_{d+1}+u_2-u_{d+2}, u_{d+3}, \ldots, u_{2d}\rangle \in \Gamma_d(U_0),$$

then $\dim U_1 \cap U_2' = d-2$ and $(U_1+U_2')\cap U_0 = \langle u_1+u_2\rangle$.

When q is a power of 2, the isomorphism between $\tilde{\Delta}$ and Δ exhibited in Theorem 5.3 gives rise to a mysterious nonlinear bijection between alternating matrices and symmetric matrices of size one less.

Lemma 5.5 *Let q be a power of 2 and $A = (a_{ij})$ be a symmetric $d \times d$ matrix with entries in $\mathrm{GF}(q)$. Let $\mathbf{a}$ be the row vector whose entries are the square roots of the diagonal entries of A: $\mathbf{a} = (\sqrt{a_{11}}, \sqrt{a_{22}}, \ldots, \sqrt{a_{dd}})$. Then the $d \times (d+1)$ matrix $(A\ {}^t\mathbf{a})$ has the same rank as A.*

Proof. Suppose that a vector $\mathbf{b} = (b_1, b_2, \ldots, b_d)$ is a left null vector of A: $\sum_{i=1}^{d} b_i a_{ij} = 0$ $(j = 1, 2, \ldots, d)$. Then we have

$$\begin{aligned}
(\sum_{i=1}^{d} b_i \sqrt{a_{ii}})^2 &= \sum_{i=1}^{d} b_i^2 a_{ii} \\
&= \sum_{i=1}^{d} b_i^2 a_{ii} + \sum_{i<j}^{d} b_i b_j a_{ij} + \sum_{i<j}^{d} b_i b_j a_{ij} \\
&= \sum_{i=1}^{d} b_i^2 a_{ii} + \sum_{i \neq j}^{d} b_i b_j a_{ij} \\
&= \sum_{j=1}^{d} b_j \sum_{i=1}^{d} b_i a_{ij} \\
&= 0.
\end{aligned}$$

This implies that $\mathbf{b}$ is also a left null vector of $(A\ {}^t\mathbf{a})$. Thus A and $(A\ {}^t\mathbf{a})$ has the same left null space, so we obtain $\mathrm{rank} A = \mathrm{rank}(A\ {}^t\mathbf{a})$. ■

Definition. The graph of symmetric bilinear form $\mathrm{Sym}(d, q)$ has

$$Y = \{A | A \text{ is an symmetric matrix with entries in } \mathrm{GF}(q)\}$$

as vertex set, two vertices A, B are adjacent whenever $\mathrm{rank}(A - B) = 1$.

Theorem 5.6 *Let Γ be the dual polar graph of type $B_d(q)$, U_0 a vertex of Γ. If q is a power of 2, then there exists an isomorphism φ from the graph $\mathrm{Sym}(d, q)$ to the subgraph induced on $\Gamma_d(U_0)$ by Γ. Moreover, $\dim \varphi(A) \cap \varphi(B) = d - \mathrm{rank}(A + B)$ holds for any vertices A, B of $\mathrm{Sym}(d, q)$.*

Proof. In view of Theorem 2.11 and the definition of dual polar space of type $B_d(q)$, we may assume that the quadratic form f is defined by

$$f(\sum_{i=1}^{2d+1} \xi_i u_i) = \sum_{i=1}^{d} \xi_i \xi_{d+i} + \xi_{2d+1}^2,$$

where $\{u_1, u_2, \ldots, u_{2d+1}\}$ is a basis of V. Also by Theorem 3.2 we may assume $U_0 = \langle u_1, u_2, \ldots, u_d \rangle$. Let Y be the set of vertices of $\mathrm{Sym}(d, q)$ and define a mapping φ from Y to $\Gamma_d(U_0)$ by

$$A = (a_{ij}) \mapsto \langle \sum_{i=1}^{d} a_{ij} u_i + u_{d+j} + \sqrt{a_{jj}} u_{2d+1} | j = 1, 2, \ldots, d \rangle.$$

Since

$$\begin{aligned}
f(\sum_{i=1}^{d} a_{ij} u_i + u_{d+j} + \beta_{jj} u_{2d+1}) &= \beta_{jj}^2 + B_f(\sum_{i=1}^{d} a_{ij} u_i, u_{d+j}) \\
&= \beta_{jj}^2 + a_{jj}, \qquad (5.4)
\end{aligned}$$

$$\begin{aligned} & B_f(\sum_{i=1}^d a_{ij}u_i + u_{d+j} + \beta_{jj}u_{2d+1}, \sum_{i=1}^d a_{ik}u_i + u_{d+k} + \beta_{kk}u_{2d+1}) \\ = \ & B_f(\sum_{i=1}^d a_{ij}u_i, u_{d+k}) + B_f(u_{d+j}, \sum_{i=1}^d a_{ik}u_i) \\ = \ & a_{kj} + a_{jk}, \end{aligned} \tag{5.5}$$

and (a_{ij}) is symmetric, we see that $\varphi(A)$ is singular. One checks easily $\dim \varphi(A) = d$ and $U_0 \cap \varphi(A) = 0$. Thus we have shown that φ is well-defined. Next we show that φ is injective. Suppose $\varphi((a_{ij})) = \varphi((b_{ij}))$. Then we have

$$\sum_{i=1}^d a_{ij}u_i + u_{d+j} + \sqrt{a_{jj}}u_{2d+1} = \sum_{k=1}^d \lambda_k(\sum_{i=1}^d b_{ik}u_i + u_{d+k} + \sqrt{b_{kk}}u_{2d+1})$$

for some $\lambda_k \in \mathrm{GF}(q)$. Comparing the coefficients of u_{d+k} for $k = 1, \ldots, d$, we find $\lambda_k = \delta_{jk}$ and $\sum_{i=1}^d a_{ij}u_i = \sum_{i=1}^d b_{ij}u_i$. This implies $a_{ij} = b_{ij}$, hence φ is injective. Next we show that φ is surjective. Suppose $U \in \Gamma_d(U_0)$. Let $\{v_1, \ldots, v_d\}$ be a basis of U and write

$$v_j = \sum_{i=1}^d b_{ij}u_i + \sum_{i=1}^d c_{ij}u_{d+i} + \gamma_j u_{2d+1} \quad (j = 1, 2, \ldots, d).$$

If the $d \times d$ matrix $C = (c_{ij})$ is singular, then there exists a nonzero vector $(\alpha_1, \ldots, \alpha_d) \in \mathrm{GF}(q)^d$ such that $\sum_{j=0}^d \alpha_j c_{ij} = 0$ for all $i = 1, \ldots, d$. But this implies $0 \neq \sum_{j=0}^d \alpha_j v_j \in f^{-1}(0) \cap (U_0 \perp \langle u_{2d+1}\rangle) = U_0$, which contradicts to $U \cap U_0 = 0$. Thus C is nonsingular. Put $A = (a_{ij}) = (b_{ij})C^{-1}$, $\beta_k = \sum_{j=1}^d (C^{-1})_{jk}\gamma_j$ $(k = 1, \ldots, d)$ and $w_k = \sum_{i=1}^d a_{ik}u_i + u_{d+k} + \beta_k u_{2d+1}$ $(k = 1, \ldots, d)$. Then

$$\begin{aligned} w_k &= \sum_{i=1}^d\sum_{j=1}^d b_{ij}(C^{-1})_{jk}u_i + \sum_{i=1}^d \delta_{ik}u_{d+i} + \sum_{j=1}^d (C^{-1})_{jk}\gamma_j u_{2d+1} \\ &= \sum_{j=1}^d (C^{-1})_{jk}\sum_{i=1}^d b_{ij}u_i + \sum_{i=1}^d\sum_{j=1}^d c_{ij}(C^{-1})_{jk}u_{d+i} + \sum_{j=1}^d (C^{-1})_{jk}\gamma_j u_{2d+1} \\ &= \sum_{j=1}^d (C^{-1})_{jk}v_j, \end{aligned}$$

so that $\{w_1, \ldots, w_d\}$ is a basis of U. Since U is singular, (5.5) implies that A is symmetric. Then the equality (5.4) implies $\varphi(A) = U$, proving the surjectivity. Finally we want to prove that φ preserves adjacency. Let $A, B \in Y$ and denote by $\mathbf{a}, \mathbf{b}$ the row vectors whose entries are the square roots of the diagonal entries of A, B, respectively. Then

$$\begin{aligned} \dim \varphi(A) \cap \varphi(B) &= 2d - \dim(\varphi(A) + \varphi(B)) \\ &= 2d - \mathrm{rank}\begin{pmatrix} A & B \\ I & I \\ \mathbf{a} & \mathbf{b} \end{pmatrix} \\ &= 2d - \mathrm{rank}\begin{pmatrix} A+B & B \\ \mathbf{a}+\mathbf{b} & \mathbf{b} \\ 0 & I \end{pmatrix} \end{aligned}$$

$$= \quad d - \operatorname{rank}\begin{pmatrix} A+B \\ \mathbf{a}+\mathbf{b} \end{pmatrix}$$
$$= \quad d - \operatorname{rank}(A+B)$$

by Lemma 5.5. This establishes the second part of the assertion, which also shows that φ is an isomorphism of the graphs $\mathrm{Sym}(d,q)$ and $\Gamma_d(U_0)$. ■

If one follows the proofs of Theorem 5.2, Theorem 5.3 and Theorem 5.6, it is not hard to construct a correspondence from $\mathrm{Alt}(d+1,q)$ to $\mathrm{Sym}(d,q)$ when q is a power of 2. We shall do this explicitly.

Let $\tilde{V}$ be a vector space of dimension $2d+2$ over $\mathrm{GF}(q)$, where q is a power of 2. Suppose that f is a quadratic form defined by

$$f(\sum_{i=1}^{2d+2} \xi_i u_i) = \sum_{i=1}^{d} \xi_i \xi_{d+i} + \xi_{2d+1}\xi_{2d+2},$$

where $\{u_1, u_2, \ldots, u_{2d+2}\}$ is a basis of $\tilde{V}$. Let $\tilde{U}_0 = \langle u_1, \ldots, u_d, u_{2d+1}\rangle$. Then an isomorphism from $\mathrm{Alt}(d+1,q)$ to the $(d+1)$-st subconstituent of $D_{d+1}(q)$ is given by $\varphi : A = (a_{ij}) \mapsto \langle v_j | j = 1, 2, \ldots, d+1\rangle$, where $v_j = \sum_{i=1}^{d} a_{ij}u_i + a_{d+1,j}u_{2d+1} + u_{d+j}$ $(j = 1, 2, \ldots, d)$, $v_{d+1} = \sum_{i=1}^{d} a_{i,d+1}u_i + u_{2d+2}$. Put $v = u_{2d+1} + u_{2d+2}$, $V = \langle v\rangle^{\perp}$. Then $f|_V$ is a non-degenerate quadratic form of Witt index d, and $\varphi(A) \cap V$ is a maximal singular subspace of V which intersects trivially with the maximal singular subspace $\langle u_1, u_2, \ldots, u_d\rangle$. Since $B_f(v_j, v) = a_{d+1,j}$ for $j = 1, 2, \ldots, d$ and $B_f(v_{d+1}, v) = 1$, we see

$$\varphi(A) \cap V = \langle v_j + a_{d+1,j}v_{d+1} | j = 1, 2, \ldots, d\rangle.$$

and

$$v_j + a_{d+1,j}v_{d+1} = \sum_{i=1}^{d}(a_{ij} + a_{d+1,i}a_{d+1,j})u_i + u_{d+j} + a_{d+1,j}v.$$

Under the correspondence given in Theorem 5.6, the subspace $\varphi(A) \cap V$ is mapped to the symmetric matrix $A_0 + {}^t\mathbf{a}\mathbf{a}$, where $A_0 = (a_{ij})_{0\le i,j\le d}$, ${}^t\mathbf{a} = (a_{d+1,1}, a_{d+1,2}, \ldots, a_{d+1,d})$.

The above argument gives the following theorem.

Theorem 5.7 *Let q be a power of 2. The graph $\mathrm{Alt}(d+1,q)$ is isomorphic to the "merged" symmetric bilinear forms graph, which has the same vertex set of $\mathrm{Sym}(d,q)$, and two vertices A, B are adjacent whenever $\mathrm{rank}(A+B) = 1$ or 2, under the mapping*

$$\psi : \begin{pmatrix} A_0 & {}^t\mathbf{a} \\ \mathbf{a} & 0 \end{pmatrix} \mapsto A_0 + {}^t\mathbf{a}\mathbf{a}, \tag{5.6}$$

where A_0 is a $d \times d$ alternating matrix.

This theorem can be proved without passing to dual polar graphs. See Appendix C. A proof for the case $q = 2$ can be found in [3].

Again we should note that the "merged" symmetric bilinear forms graph is not the distance 1-or-2 graph of the symmetric bilinear forms graph. This follows immediately from Proposition 5.4 and Theorem 5.6. Let q be a power of 2, $A, B \in \mathrm{Sym}(d,q)$ and suppose $\mathrm{rank}(A+B)=2$. Let us derive a condition when A and B are distance 2 apart in $\mathrm{Sym}(d,q)$. With the notation of Proposition 5.4 and Theorem 5.6, the distance between A and B is greater than 2 if and only if $\dim U_0 \cap (\varphi(A)+\varphi(B)) = 2$. Since $\dim(\varphi(A)+\varphi(B)) = d+2$, this is equivalent to $\dim(U_0+\varphi(A)+\varphi(B)) = 2d$. On the other hand,

$$\begin{aligned}\dim(U_0+\varphi(A)+\varphi(B)) &= \mathrm{rank}\begin{pmatrix} I & A & B \\ 0 & I & I \\ 0 & \mathbf{a} & \mathbf{b} \end{pmatrix} \\ &= d+\mathrm{rank}\begin{pmatrix} I & A+B \\ 0 & \mathbf{a}+\mathbf{b} \end{pmatrix} \\ &= 2d+\mathrm{rank}(\mathbf{a}+\mathbf{b}),\end{aligned}$$

where $\mathbf{a},\mathbf{b}$ are the row vectors whose entries are the square roots of the diagonal entries of A, B, respectively. Thus, the distance between A and B is greater than 2 if and only if $A+B$ is alternating.

Of course, one can argue without using the correspondence given in Theorem 5.6. Here we present a more straightforward way.

Lemma 5.8 *Let q be a power of 2 and $A=(a_{ij})$ be a symmetric matrix with entries in* $\mathrm{GF}(q)$. *Let* $\mathbf{a}$ *be the row vector whose entries are the square roots of the diagonal entries of A:* $\mathbf{a} = (\sqrt{a_{11}}, \sqrt{a_{22}}, \ldots, \sqrt{a_{dd}})$. *If A has rank 1, then* $A = {}^t\mathbf{a}\mathbf{a}$.

Proof. If A has rank 1, then Proposition 1.5 implies that A is not alternating. In particular, not all diagonal entries are 0. Suppose $a_{kk} \neq 0$. Since A has rank 1, every row vector of A is a scalar multiple of the k-th row. This implies $a_{ij} = a_{kj}a_{ik}/a_{kk}$ for any i, j. Since A is symmetric, putting $i=j$ gives $a_{ik} = \sqrt{a_{ii}a_{kk}}$. Thus

$$a_{ij} = \frac{a_{ik}a_{jk}}{a_{kk}} = \sqrt{a_{ii}a_{jj}}$$

for all i, j. This proves the desired formula $A = {}^t\mathbf{a}\mathbf{a}$. ∎

If A and B are distinct symmetric matrices of rank 1, then Lemma 5.8 implies that $A = {}^t\mathbf{a}\mathbf{a}$ and $B = {}^t\mathbf{b}\mathbf{b}$ for some vectors $\mathbf{a},\mathbf{b}$ with $\mathbf{a} \neq \mathbf{b}$. Then the diagonals of A and B are distinct, hence $A+B$ is not alternating. Conversely, if A is a non-alternating symmetric matrix of rank 2, then one can easily show that there exists a nonsingular matrix B such that

$${}^tBAB = \begin{pmatrix} 1 & 0 & \\ 0 & 1 & \\ & & \end{pmatrix},$$

thus A is a sum of two symmetric matrices of rank 1. To summarize:

Theorem 5.9 *Let q be a power of 2, A, B vertices of* $\mathrm{Sym}(d,q)$. *Then the distance between A and B is 2 if and only if* $\mathrm{rank}(A+B)=2$ *and $A+B$ is not alternating.*

Appendix

A Witt's extension theorem

Many of the results in sections 2,3 can be derived easily from the Witt's extension theorem. However, I have opted to exclude the Witt's extension theorem from the main text since its proof is rather complicated. In this section we let f be a non-degenerate quadratic form on a vector space V over an arbitrary field.

Lemma A.1 *If V is a hyperbolic plane, then the group of isometries of (V, f) acts transitively on the set of nonzero singular vectors.*

Proof. This is immediate from Proposition 1.8. ■

Lemma A.2 *Let U be a degenerate hyperplane of V. Assume that B_f is non-degenerate. Then any isometry $\sigma : U \longrightarrow V$ is extendable to V.*

Proof. Let $u \in \mathrm{Rad}\,(f|_U)$. Since B_f is non-degenerate, we have $\langle u \rangle = U$, and hence $\mathrm{Rad}\,(B_f|_U) = \mathrm{Rad}\,(f|_U) = \langle u \rangle$. Write $U = U_0 \perp \langle u \rangle$. Then $B_f|_{U_0}$ is non-degenerate, so $V = U_0 \perp U_0^\perp$. Also $V = \sigma(U_0) \perp \sigma(U_0)^\perp$. Note that we have $u \in U_0^\perp$, $\sigma(u) \in \sigma(U_0)^\perp$, and $f(u) = f(\sigma(u)) = 0$, so that $U_0^\perp$ and $\sigma(U_0)^\perp$ are hyperbolic planes. By Lemma A.1, there exists an isometry $\tau : U_0^\perp \longrightarrow \sigma(U_0)^\perp$ such that $\tau(u) = \sigma(u)$. Now $\sigma|_{U_0} \perp \tau$ is an extension of σ to V. ■

Lemma A.3 *If G is a group and A, B are subgroups of G such that $G = A \cup B$, then either $G = A$ or $G = B$.*

Proof. Suppose contrary. Then there exist elements $a \in A$, $b \in B$ such that $a \notin B$, $b \notin A$. Then the product $ab \notin A \cup B$, which is a contradiction. ■

Theorem A.4 (Witt's Extension Theorem) *Let f be a quadratic form on a vector space V such that B_f is non-degenerate. Suppose that U is a subspace of V and $\sigma : U \to V$ is an isometry. Then there exists an extension $\sigma^* : V \to V$ of σ.*

Proof. We prove by induction on $\dim U$. If $\dim U = 0$ then the assertion is trivially true by taking $\sigma^* = 1_V$. So let us assume $1 \leq \dim U \leq n-1$, where $n = \dim V$. If $\sigma = 1_U$, then again we can take $\sigma^* = 1_V$, so we assume $\sigma \neq 1_U$. Choose an arbitrary subspace U_0 of U with $\dim U_0 = \dim U - 1$. By induction there exists an isometry $\tau : V \to V$ such that $\tau|_{U_0} = \sigma|_{U_0}$. If there exists an extension $\tilde{\sigma}$ of $\tau^{-1} \circ \sigma$, then $\tau \circ \tilde{\sigma}$ is an extension of σ. Thus, without loss of generality we may assume $\sigma|_{U_0} = 1_{U_0}$.

Write $U = U_0 \oplus \langle a \rangle$, $W = U_0 \oplus \langle b \rangle$, where $b = \sigma(a)$. If there exists a vector $z \notin U \cup W$ such that $B_f(z, a) = B_f(z, b)$, then we may replace U, W, U_0 by $U \oplus \langle z \rangle$, $W \oplus \langle z \rangle$, $U_0 \oplus \langle z \rangle$, respectively, and extend σ to $U \oplus \langle z \rangle$ by defining $\sigma(z) = z$. Continuing this process until it is no longer possible, or we have $U = V$ in which case the proof is complete. Suppose

$U \neq V$. Then we must have $\langle a-b\rangle^{\perp} \subset U \cup W$. By Lemma A.3, we have either $\langle a-b\rangle^{\perp} \subset U$ or $\langle a-b\rangle^{\perp} \subset W$. Since U and W are proper subspaces and $\langle a-b\rangle^{\perp}$ is a hyperplane, we see $\langle a-b\rangle^{\perp} = U$ or W. In particular, $a \in \langle a-b\rangle^{\perp}$ or $b \in \langle a-b\rangle^{\perp}$. On the other hand, $f(a) = f(b)$ implies

$$B_f(a,a) = f(a) + f(b) = B_f(b,b),$$

and hence

$$B_f(a, a-b) = f(a-b) = B_f(b-a, b).$$

Therefore $f(a-b) = 0$. This implies $a - b \in \operatorname{Rad}(f|_U)$, that is, U is degenerate. Now σ is extendable to V by Lemma A.2. ∎

The non-degeneracy of B_f in the hypothesis of Theorem A.4 is necessary, as the following example indicates. Under an appropriate condition, the conclusion of Theorem A.4 holds even if B_f is degenerate. See Theorem A.6 and [4], 7.4 Theorem.

Example. Consider the quadratic form $f = x_1x_2 + x_3^2$ on $\mathrm{GF}(2)^3$. The mapping $\sigma : \langle e_3\rangle \to V$, $e_3 \mapsto e_1 + e_2$ is an isometry but it has no extension to V. Indeed, $\langle e_3\rangle$ is the radical of B_f which must be left invariant under any isometry of V.

Lemma A.5 *If U_1, U_2 are singular subspaces of V, then $(U_1 + U_2) \cap \operatorname{Rad} B_f = 0$.*

Proof. Let $v \in (U_1 + U_2) \cap \operatorname{Rad} B_f$, $v = u_1 + u_2$, $u_1 \in U_1$, $u_2 \in U_2$. Then $f(v) = f(u_1 + u_2) = B_f(u_1, u_2) = B_f(u_1, v) = 0$. Since f is non-degenerate, we see $v = 0$, that is, $(U_1 + U_2) \cap \operatorname{Rad} B_f = 0$. ∎

By the following theorem, the dimension of any maximal singular subspace is equal to the Witt index.

Theorem A.6 *Let f be a non-degenerate quadratic form on a vector space V over K. If U_1, U_2 are maximal singular subspaces of V, then there exists an isometry σ of V such that $\sigma(U_1) = U_2$. In particular,* $\dim U_1 = \dim U_2$.

Proof. Without loss of generality we may assume $\dim U_1 \leq \dim U_2$. Then any injection $\sigma : U_1 \longrightarrow U_2$ is an isometry. Suppose first that B_f is non-degenerate. By Witt's extension theorem, there exists an extension of σ to V, which we also denote by σ. Then $\sigma^{-1}(U_2)$ is a singular subspace containing U_1, hence by the maximality of U_1, we have $U_1 = \sigma^{-1}(U_2)$, in other words, $\sigma(U_1) = U_2$.

Next suppose that B_f is degenerate. By Lemma A.5, we have $(U_1+U_2) \cap \operatorname{Rad} B_f = 0$. This implies the existence of a hyperplane W containing $U_1 + U_2$ with $V = W \oplus \operatorname{Rad} B_f$. As $B_f|_W$ is non-degenerate, we can apply the first case to obtain an extension of σ to W. Extending σ further to V by defining $\sigma|_{\operatorname{Rad} B_f} = 1_{\operatorname{Rad} B_f}$, we obtain the desired isometry of V. ∎

Using the Witt's extension theorem, we can give an alternative proof of Theorem 3.2.

Proof of Theorem 3.2. By Lemma A.5, we have $(U_1+U_2) \cap \operatorname{Rad} B_f = (U_1'+U_2') \cap \operatorname{Rad} B_f = 0$. This implies that there exist hyperplanes W, W' complementary to $\operatorname{Rad} B_f$, containing $U_1 + U_2$, $U_1' + U_2'$, respectively. Now $f|_W$ and $f|_{W'}$ are non-degenerate, and have Witt index d, as W and W' contain singular d-dimensional subspaces. By Corollary 2.12 there exists an isometry $\tau : W' \longrightarrow W$. On the other hand, there exists an isometry $\sigma_0 : U_1 + U_2 \longrightarrow U_1' + U_2'$ satisfying $\sigma_0(U_1) = U_1'$ and $\sigma_0(U_2) = U_2'$ by Lemma 3.1. The composition $\tau \circ \sigma_0$ is an isometry $U_1 + U_2 \longrightarrow W$ which can be extended to an isometry $\rho : W \longrightarrow W$ by Witt's theorem. Now $\tau^{-1} \circ \rho : W \longrightarrow W'$ is an isometry extending σ_0. Finally the isometry σ defined by $\sigma|_W = \tau^{-1} \circ \rho$, $\sigma|_{\mathrm{Rad}\, B_f} = 1_{\mathrm{Rad}\, B_f}$ has the desired property. ■

B Transitivity without Witt's theorem

In this section we shall show that the orthogonal group acts transitively on the set of maximal singular subspaces, without using the Witt's extension theorem. The method used here works for an arbitrary base field. I would like to thank William Kantor for informing me of this approach.

Throughout this section, we assume that f is a non-degenerate quadratic form on a vector space V.

Lemma B.1 *The group of isometries of (V, f) acts transitively on the set of nonzero singular vectors.*

Proof. Let u, v be nonzero singular vectors. We want to show that there exists an isometry σ such that $\sigma(u) = v$.

Case 1. $B_f(u, v) \neq 0$. In this case $P = \langle u, v\rangle$ is a hyperbolic plane and $V = P \perp P^\perp$. By Lemma A.1 there exists an isometry σ of P such that $\sigma(u) = v$. Extending σ to V by defining $\sigma|_{P^\perp} = 1_{P^\perp}$, we obtain the desired isometry.

Case 2. $B_f(u, v) = 0$. We claim that there exists a singular vector w such that $B_f(u, w) \neq 0$, $B_f(v, w) \neq 0$. Then the proof reduces to Case 1. As for the claim, pick a vector $z \notin \langle u\rangle^\perp \cup \langle v\rangle^\perp$. This is possible by Lemma A.3. Then by Proposition 1.7 there exists a singular vector $w \in \langle u, z\rangle$ such that $B_f(u, w) = 1$. We also have $B_f(v, w) \neq 0$, since $\langle u, w\rangle = \langle u, z\rangle \not\subset \langle v\rangle^\perp$ and $u \in \langle v\rangle^\perp$. ∎

Theorem B.2 *The group of isometries of (V, f) acts transitively on the set of singular k-dimensional subspaces for any given k.*

Proof. We prove by induction on k. The case $k = 1$ has been established in Lemma B.1. Suppose $1 < k \leq d$, where d is the Witt index. By Proposition 2.4 we may write

$$V = \langle v_1, v_2\rangle \perp \cdots \perp \langle v_{2d-1}, v_{2d}\rangle \perp W,$$

where $\{v_{2i-1}, v_{2i}\}$ $(i = 1, \ldots, d)$ are hyperbolic pairs and W is a subspace containing no nonzero singular vectors. Let U be a singular subspace of dimension k. We want to construct an isometry σ of V such that $\sigma(U) = \langle v_1, v_3, \ldots, v_{2k-1}\rangle$. Pick a nonzero vector $u \in U$. By Lemma B.1, there exists an isometry τ of V such that $\tau(u) = v_1$. If we write $P = \langle v_1, v_2\rangle$, then $P^\perp \cap \tau(U) = \langle v_2\rangle^\perp \cap \tau(U)$ is a singular $(k-1)$-dimensional subspace of $P^\perp$. By induction, there exists an isometry ρ of $P^\perp$ such that $\rho(P^\perp \cap \tau(U)) = \langle v_3, \ldots, v_{2k-1}\rangle$. Since $\tau(U) = \langle v_1\rangle \perp P^\perp \cap \tau(U)$, we find $(1_P \perp \rho) \circ \tau(U) = \langle v_1, v_3, \ldots, v_{2k-1}\rangle$, that is, $\sigma = (1_P \perp \rho) \circ \tau$ is an isometry with the desired property. ∎

C Another proof of Theorem 5.7

Theorem 5.7 can be proved directly. It is easy to see that the mapping ψ defined in (5.6) is bijective. To show that ψ preserves adjacency, let

$$A = \begin{pmatrix} A_0 & {}^t\mathbf{a} \\ \mathbf{a} & 0 \end{pmatrix}, \quad B = \begin{pmatrix} B_0 & {}^t\mathbf{b} \\ \mathbf{b} & 0 \end{pmatrix}$$

be vertices of $\mathrm{Alt}(d+1,q)$, where A_0, B_0 are $d \times d$ alternating matrices. Then we have

$$\begin{aligned}
&\mathrm{rank}(A+B) \\
&= \mathrm{rank}\begin{pmatrix} A_0 + B_0 & {}^t(\mathbf{a}+\mathbf{b}) \\ \mathbf{a}+\mathbf{b} & 0 \end{pmatrix} \\
&= \mathrm{rank}\begin{pmatrix} A_0 + B_0 + {}^t(\mathbf{a}+\mathbf{b})(\mathbf{a}+\mathbf{b}) & {}^t(\mathbf{a}+\mathbf{b}) \\ \mathbf{a}+\mathbf{b} & 0 \end{pmatrix} \\
&= \mathrm{rank}\begin{pmatrix} \psi(A) + \psi(B) + {}^t(\mathbf{a}+\mathbf{b})\mathbf{b} + {}^t\mathbf{b}(\mathbf{a}+\mathbf{b}) & {}^t(\mathbf{a}+\mathbf{b}) \\ \mathbf{a}+\mathbf{b} & 0 \end{pmatrix} \\
&= \mathrm{rank}\begin{pmatrix} \psi(A) + \psi(B) & {}^t(\mathbf{a}+\mathbf{b}) \\ \mathbf{a}+\mathbf{b} & 0 \end{pmatrix}.
\end{aligned}$$

Since $\mathbf{a}+\mathbf{b}$ is the vector consisting of the square roots of the diagonal entries of $\psi(A) + \psi(B)$, we have, by Lemma 5.5,

$$\mathrm{rank}(A+B) = \mathrm{rank}(\psi(A)+\psi(B)) \quad \text{or} \quad \mathrm{rank}(\psi(A)+\psi(B)) + 1.$$

In particular, $\mathrm{rank}(A+B) = 2$ if and only if $\mathrm{rank}(\psi(A)+\psi(B)) = 1$ or 2. This shows that ψ is an isomorphism from $\mathrm{Alt}(d+1,q)$ to the "merged" symmetric bilinear forms graph.

D Notes

The example on page 5 may be a good exercise for students. During my lecture, I have left as exercises the proofs of Proposition 1.1, Proposition 1.5, Proposition 2.7, Lemma 3.3, Proposition 4.3, and the equalities (4.1), (4.2).

All, or part of materials in the first two sections can be found in many books, for example, [4], [6]. The books [1], [5] are excellent for beginning students, but they do not deal with quadratic forms in characteristic 2. All results in sections 3,4, and a part of section 5 can be found in [2]. It is more natural to identify the graph $\mathrm{Sym}(d, q)$ with the d-th subconstituent of the dual polar graph of type $C_d(q)$, than we did in Theorem 5.6. The detailed discussion in the latter part of section 5 of dual polar graphs and symmetric bilinear forms graphs has not been available in previously published work.

References

[1] E. Artin, Geometric Algebra, Interscience, New York, 1957.

[2] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-Regular Graphs, Springer, Berlin-Heidelberg 1989.

[3] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, $\mathbf{Z}_4$-Kerdock codes, orthogonal spreads, and extremal line-sets, preprint.

[4] J. Dieudonné, La géométrie des groupes classiques, Springer, Berlin, 1955.

[5] H. Nagao, "Groups and Designs" (in Japanese), Iwanami Shoten.

[6] D. E. Taylor,"The Geometry of the Classical Groups", Heldermann Verlag, Berlin, 1992.