18. Orthogonal groups

We will not give a full treatment of the orthogonal groups, as we do not have time, but we'll try and give a broad overview. Throughout this section V is an n-dimensional vector space over the field $k = \mathbb{F}_q$ and $Q : V \to \mathbb{F}_q$ is a non-degenerate quadratic form.

Recall first that we have the following possibilities for (V, Q). (Note that, in all cases, for $i = 1, \dots, r$, (v_i, w_i) are mutually orthogonal hyperbolic pairs, with $Q(v_i) = Q(w_i) = 0$.)

($\mathbf{O^+_{2r}}$) with basis $\{v_1, w_1, \dots, v_r, w_r\}$.

($\mathbf{O_{2r+1}}$) with basis $\{v_1, w_1, \dots, v_r, w_r, u\}$ where $\langle u\rangle$ is anisotropic and orthogonal to $\langle v_1, w_2, \dots, v_r, w_r\rangle$. We can prescribe, moreover, that $Q(u) = 1$ or, if q is odd, $Q(u)$ is 1 or a non-square.

($\mathbf{O^-_{2r+2}}$) with basis $\{v_1, w_1, \dots, v_r, w_r, u, u'\}$ where $\langle u, u'\rangle$ is anisotropic and orthogonal to $\langle v_1, w_2, \dots, v_r, w_r\rangle$. We can prescribe, moreover, that $Q(u) = 1$, $Q(u') = a$ and $x^2 + x + a$ is irreducible in $\mathbb{F}_q[x]$.

Note that, although there are two non-isomorphic spaces O_{2r+1}, the corresponding polar spaces, and hence the corresponding isometry (resp. similarly/ semisimilarity) groups are all isomorphic.

This remark allows us to make the following definitions. Note that, throughout,

$$\varepsilon \text{ is } \begin{cases} + \text{ or } -, & \text{if } n \text{ is even;} \\ \text{blank}, & \text{if } n \text{ is odd.} \end{cases}$$

- $\Gamma\mathrm{O}^\varepsilon_n(q)$ is the semisimilarity group of Q;
- $\mathrm{GO}^\varepsilon_n(q)$ is the similarity group of Q;
- $\mathrm{O}^\varepsilon_n(q)$ is the isometry group of Q;
- $\mathrm{SO}^\varepsilon_n(q)$ is the special isometry group of Q, i.e. it equals $\mathrm{O}^\varepsilon_n(q) \cap \mathrm{SL}_n(q)$.
- $\Omega^\varepsilon_n(q) = (\mathrm{O}^\epsilon_n(q))'$, a subgroup of $\mathrm{SO}^\varepsilon_n(q)$ of index 1 or 2.

For all of the listed groups X, there is a projective version $\mathrm{P}X = X/(X \cap K)$ where K is the set of scalar matrices.[46]

The groups we're primarily interested in are $\mathrm{P}\Omega^\varepsilon_n(q)$ as these are simple unless n and q are in a certain small range. Our treatment begins similarly to the other classical groups:

Lemma 18.1.

(1) *Let x^ε_n be the number of non-trivial singular vectors. Then*
   - $x^\varepsilon_{2m} = (q^m - \varepsilon 1)(q^{m-1} + \varepsilon 1)$;
   - $x_{2m+1} = q^{2m} - 1$.

(2) *The number of hyperbolic pairs is $x^\varepsilon_n \cdot q^{n-2}$.*

Proof. Clearly $x_1 = x_2^- = 0$. On the other hand, a space of type O_2^+ is a hyperbolic line, thus if (v, w) is a hyperbolic pair, then $Q(av + bw) = ab$ and so the singular vectors lie in $\langle v\rangle \cup \langle w\rangle$ and $x_2^+ = 2(q - 1)$.

Now for any $n \geq 3$, an orthogonal space admits a basis which is an orthogonal direct sum of a set of mutually orthgonal hyperbolic lines with one of the spaces already covered. Consider the different cases in turn.

($\mathbf{O^+_{2m}}$) with $Q(\sum a_i v_i + \sum b_i w_i) = \sum a_i b_i$. Then $Q(v) = 0$ iff either
   - $a_1 = 0$, b_1 is anything and the 'tail' of the vector in O^+_{2r-2} is singular. This gives $q(x^+_{2m-2} + 1) - 1$ possibilities. (The '+1' and the '−1' are there to account for zero vectors.)
   - $a_1 \neq 0$ and $b_1 = a_1^{-1} \sum_{i=2}^m b_i w_i$. This gives $(q - 1)q^{2m-2}$ possibilities.

   We conclude that $x^+_{2m} = (q - 1)q^{2m-2} + q(x^+_{2m-2} + 1) - 1$ and the result follows by induction.

($\mathbf{O_{2r+1}}$) Exactly the same reasoning as before implies that

$$x^-_{2m} = (q - 1)q^{2m-2} + q(x^+_{2m-2}1) - 1$$

and the result follows by induction.

($\mathbf{O^-_{2r+2}}$) This time we obtain that

$$x_{2m+1} = (q - 1)q^{2m-2} + q(x^+_{2m-1}1) - 1$$

and the result follows.

[46] Some authors label orthogonal groups slightly differently. I've chosen terminology that is consistent with [KL90] but, for instance, some people write $\mathrm{GO}^\varepsilon_n(q)$ for the isometry group of Q, rather than the similarity group.

To calculate the number of hyperbolic pairs (v,w), simply observe that the number of choices for the first entry v is x_n. To find w we choose any vector in the complement of $\ker(\beta_v)$ where $\beta_v : V \to k, w \mapsto \beta(v,w)$. Since β_v is a non-zero linear functional, its kernel has dimension $n-1$ and the number of vectors in the complement of the kernel is, therefore, $q^n - q^{n-1}$. Now we must restrict to those elements for which $\beta(v,w)=1$ and we obtain $\frac{1}{q-1}(q^n-q^{n-1})$ as required. □

We will use Lemma 18.1 to calculate the size of $O^\varepsilon_n(q)$ using induction on n. The base cases are treated in the following exercise.

(E18.1) *$O_1(q) = \{\pm I\}$ and $O^\varepsilon_2(q) \cong D_{2(q-\varepsilon 1)}$.*

Lemma 18.2.

- $|O^\varepsilon_{2m}(q)| = 2q^{m(m-1)}(q^m - \varepsilon 1)\prod_{i=1}^{m-1}(q^{2i}-1)$.
- $|O_{2m+1}(q)| = (2,q-1)q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$.

Proof. As in previous sections we use the fact (which follows from Witt's Lemma) that $\mathrm{Isom}(Q)$ acts regularly on the set of orthogonal bases. To count orthogonal bases we choose (x,y) to be a hyperbolic pair and invoke Lemma 18.1, before using induction to count the number of orthogonal bases in $\langle x,y\rangle^\perp$. The result follows, using (E18.1) for the base case. □

(E18.2*) *Prove that if $g \in \mathrm{O}^\varepsilon_n(q)$, then $\det(g) = \pm 1$. Prove that $-I \in \mathrm{O}^\varepsilon_n(q)$. Conclude that*

$$|\mathrm{SO}^\varepsilon_n(q)| = |\mathrm{PO}^\varepsilon_n(q)| = \frac{1}{(2,q-1)}|\mathrm{O}^\varepsilon_n(q)|.$$

Lemma 18.3.

(1) *If q is even, then $\Omega_{2m+1}(q) \cong \mathrm{Sp}_{2m}(q)$.*
(2) *If q is odd, then $\mathrm{P}\Omega_{2m+1}(q)$ and $\mathrm{PSp}_{2m+1}(q)$ have the same order. If, in addition $m>2$, then $\mathrm{P}\Omega_{2m+1}(q) \ncong \mathrm{PSp}_{2m+1}(q)$.*

Proof. Let Q be a non-degenerate quadratic form of type O_{2m+1} and assume that q is even. The polarization of Q, β_Q is alternating and, since the dimension is odd, it must be degenerate. However (E13.14) implies that $\mathrm{Rad}(\beta_Q)$ has dimension 1. Let $\mathrm{Rad}(\beta_Q) = \langle z\rangle$ and choose z so that $Q(z)=1$. Now the space $V/\langle z\rangle$ is non-degenerate and symplectic of order $2m$.

The action of $\mathrm{SO}_{2m+1}(q)$ on V induces an action by isometry on $V/\langle z\rangle$ and we obtain a homomorphism $\mathrm{SO}_{2m+1}(q) \to \mathrm{Sp}_{2m}(q)$. One can check that the kernel of this homomorphism is trivial, hence we obtain an embedding. However checking orders we see that the two groups have the same cardinality and the result follows.

Result (2) follows from the following exercise.

(E18.3) *Let q be odd. Show that $\mathrm{PSp}_{2m}(q)$ has $\lfloor \frac{m}{2} \rfloor + 1$ conjugacy classes of involutions, while $\mathrm{P}\Omega_{2m+1}(q)$ has m conjugacy classes of involutions.*

□

Some remarks about $\Omega_{2m+1}(q)$:

- Suppose that q is even. In light of Lemma 18.3 most authors tend not to study $\Omega_{2m+1}(q)$, opting instead to study the isomorphic group $\mathrm{Sp}_{2m}(q)$ (see, for instance, [KL90]).
- The proof of Lemma 18.3 implies that, if q is even, then $\Omega_{2m+1}(q) = \mathrm{SO}_{2m+1}(q)$, and that this group is simple, except when $(m,q) = (1,2)$ or $(2,2)$.
  In fact this is the only situation when $n<1$ and $\Omega^\epsilon_n(q)$ has index 1 in $\mathrm{SO}^\epsilon_n(q)$. In all other cases, provided $n>1$, $|\mathrm{SO}^\epsilon_n(q) : \Omega^\epsilon_n(q)| = 2$.
- Suppose that q is odd. (E18.2) implies that $\mathrm{SO}_{2m+1}(q)$ does not contain any scalar matrices and, in particular, we have that

$$\mathrm{PSO}_{2m+1}(q) = \mathrm{SO}_{2m+1}(q) \text{ and } \mathrm{P}\Omega_{2m+1}(q) = \Omega_{2m+1}(q).$$

The following couple of results show in addition that, when $n \leq 6$, $\mathrm{P}\Omega_n^\varepsilon(q)$ does not yield a new simple group. Indeed (E18.1) implies that already for $n \leq 2$.

Lemma 18.4. *If q is odd, then $\Omega_3(q) \cong \mathrm{PSL}_2(q)$.*

Proof. Let Ω be the set of homogeneous polynomials over $\mathbb{F}_q$ in variables x and y of degree 2, i.e.[47]

$$\Omega := \{rx^2 + sxy + ty^2 \mid r, s, t \in Fq\}.$$

Then $G = \mathrm{GL}_2(q)$ acts on Ω by substitution, i.e. given

$$g := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

we define

$$x^g = ax + by \text{ and } y^g = cx + dy$$

and observe that we have a well-defined action.

Indeed (by observing that Ω is a 3-dimensional vector space over $\mathbb{F}_q$) we can check that the group G acts on Ω as an object from $\mathbf{Vect}_{\mathbb{F}_q}$: we represent an element $f = rx^2 + sxy + ty^2$ by the vector $\begin{pmatrix} r & s & t \end{pmatrix}$ and observe that $f^g = \begin{pmatrix} r & s & t \end{pmatrix} \rho(g)$ where

$$\rho : \mathrm{GL}_2(q) \to \mathrm{GL}_3(q),\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad + bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}.$$

Clearly ρ is the associated homomorphism $G \to \mathrm{Aut}(\Omega)$, where $\mathrm{Aut}(\Omega) = \mathrm{GL}_3(q)$ is the automorphism group of Ω as an object from $\mathbf{Vect}_{\mathbb{F}_q}$.

Observe that $\ker(\rho) = \{\pm I\}$ and define a quadratic form on $V = (\mathbb{F}_q)^3$ via

$$Q\begin{pmatrix} r & s & t \end{pmatrix} = 4rt - s^2.$$

One can check that Q is non-degenerate and that, for $g \in G$,

$$Q(f^{\rho(g)}) = Q(f)(\det(g))^2.$$

This implies that $\mathrm{SL}_2(q)$ acts on (V, Q) as an object from $\mathbf{IVect}_{\mathbb{F}_q}$ and, by restricting the domain of ρ, we obtain

$$\rho : \mathrm{SL}_2(q) \to \mathrm{Aut}(V, Q) = \mathrm{Isom}(Q) = \mathrm{O}_3(q).$$

Now the first isomorphism theorem of groups, implies that

$$\mathrm{PSL}_2(q) \cong \mathrm{SL}_2(q)/\langle -I \rangle \cong \mathrm{Im}(\rho) \leq \mathrm{O}_3(q)$$

By checking orders we obtain that $\mathrm{Im}(\rho)$ is an index 4 subgroup of $\mathrm{O}_3(q)$. If $q > 3$, then the simplicity of $\mathrm{PSL}_2(q)$ can be used to prove that $\mathrm{Im}(\rho)$ is a normal subgroup of $\mathrm{O}_3(q)$; indeed it must be the derived subgroup of $\mathrm{O}_3(q)$ (since it is perfect and of index 4), and the result follows. For $q = 3$ we omit the proof. □

The proof of the following lemma is omitted. It is proved in a similar fashion to the last lemma.

Lemma 18.5.

(1) $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$.
(2) $\mathrm{P}\Omega_4^-(q) \cong \mathrm{PSL}_2(q^2)$.
(3) $\mathrm{P}\Omega_5(q) \cong \mathrm{PSp}_4(q)$.
(4) $\mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$.
(5) $\mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$.

[47] An equivalent formulation is to take Ω to be equal to $\mathrm{Sym}^2(V)$, the symmetric square of $V = \mathbb{F}_q^2$. Clearly $\mathrm{GL}_2(q)$ acts on V naturally via the homomorphism ρ defined below.

18.1. **Simplicity.** We conclude with a statement concerning the simplicity of $\mathrm{P}\Omega_n^\varepsilon(q)$. The last two lemmas imply the result for $n = 5$ and 6. Indeed they also imply that $\mathrm{P}\Omega_3(q)$ and $\mathrm{P}\Omega_4^-(q)$ are simple, but we do not include this in the statement.

Theorem 18.6. *If $n \geq 5$, then $\mathrm{P}\Omega_n^\varepsilon(q)$ is simple.*

The proof of this theorem is a little different to the previous cases we have studied, and we will not write it down. The following exercise highlights one major difference.

(E18.4*) *$SO_n^\varepsilon(q)$ contains a transvection if and only if q is even.*

It is worth mentioning a second major hurdle. We have defined $\Omega_n^\varepsilon(q)$ to be the derived subgroup of $O_n^\varepsilon(q)$, but in practice this definition is not adequate. We will finish by sketching a more explicit definition of $\Omega_n^\varepsilon(q)$.

Let $v \in V$ be a non-singular vector and define the *reflection in v* as the map

$$r_v : V \to V, x \mapsto x - \frac{\beta_Q(v,x)}{Q(v)}v.$$

(Observe that r_v satisfies the first condition for a map to be a transvection, since $r_v - I$ has rank 1, but it does not satisfy the second, since $(r_v - I)^2 \neq 0$.) One can check that $r_v \in \mathrm{Isom}(Q)$, that $r_v^2 = 1$, and that

$$\det(r_v) = \begin{cases} -1, & \text{if } q \text{ is odd;} \\ 1, & \text{if } q \text{ is even.} \end{cases}$$

Now the following result is [KL90, Prop 2.5.6].

Lemma 18.7. $\mathrm{Isom}(Q) = \langle r_v \mid Q(v) \neq 0 \rangle$, *provided* $\mathrm{Isom}(Q) \neq \mathrm{O}_4^+(2)$.

Now our definition is as follows:

- Suppose that q is even and that $\mathrm{Isom}(Q) \neq \mathrm{O}_4^+(2)$. We can assume that n is even by Lemma 18.3 and thus, by (E18.2), $\mathrm{O}_n^\varepsilon(q) = \mathrm{SO}_n^\varepsilon(q)$ and that, by Lemma 18.7, every element of $\mathrm{SO}_n^\varepsilon(q)$ can be written as a product of reflections. Now the subgroup of S consisting of products of an even number of reflections has index 2 in $\mathrm{SO}_n^\varepsilon(q)$ and this is the group $\Omega_n^\varepsilon(q)$. It is not a priori clear that this action yields an index 2 subgroup - the next exercise proves that it does when $\varepsilon = +$.

  (E18.5*) *Prove that this definition yields an index 2 subgroup when $\varepsilon = +$ by showing that, in the natural action of G on $\mathcal{U}_r$, the set of maximal totally singular subspaces, any reflection acts as an odd permutation on $\mathcal{U}_r$.*

- Suppose that q is odd and that $n \geq 2$. Consider the group $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ which has order 2.[48] Lemma 18.7 implies that every element of $\mathrm{SO}_n^\varepsilon(q)$ can be written as an even number of reflections $g = r_{v_1} \cdots r_{v_k}$, for some non-singular vectors v_i. Define the *spinor norm*,

$$\theta : \mathrm{SO}_n^\varepsilon(q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^2, \quad g \mapsto \prod_{i=1}^{k} \beta_Q(v_i, v_i) \pmod{(\mathbb{F}_q^*)^2}.$$

  It turns out that θ is a well-defined homomorphism, and that it is surjective. In particular $\ker(\theta)$ is an index 2 subgroup of $\mathrm{SO}_n^\varepsilon(q)$, and this is the subgroup $\Omega_n^\varepsilon(q)$.

  (E18.6) *Calculate the order of $|\Omega_n^\varepsilon(q)|$ when $(n, q, \varepsilon) \neq (4, 2, +)$.*

We do not give a definition of $\Omega_4^+(2)$. Those interested should consult [KL90, p. 30].

[48] We write $(\mathbb{F}_q^*)^2$ for the set of non-zero squares in $\mathbb{F}_q^*$. It is an index 2 subgroup of $\mathbb{F}_q^*$.