J. Group Theory **12** (2009), 171–180
DOI 10.1515/JGT.2008.069

Journal of Group Theory

Certain classical groups are not well-defined

John N. Bray, Derek F. Holt and Colva M. Roney-Dougal

(Communicated by C. W. Parker)

Abstract. In this article we show that the isomorphism type of certain semilinear classical groups may depend on the choice of form matrix, as well as the dimension and the field size. When there is more than one isomorphism type, we count them and present effective polynomial-time algorithms to determine whether two such groups are isomorphic.

1 Introduction

The main purpose of this article is to prove that certain commonly referred to classical groups are not always well-defined.

Throughout, p will denote a prime and $q = p^f$ a power of p. When discussing classical groups, we define $u = 2$ in the unitary case and $u = 1$ otherwise. In general, Φ will denote the map that replaces every element of a matrix with entries in $\mathbb{F}_{q^u}$ by its pth power.

Given a classical group of matrices over $\mathbb{F}_{q^u}$ that is normalized by the map Φ just defined, we also denote the induced automorphism of the classical group by Φ, and we let ϕ be the corresponding automorphism of the projective version of the classical group; that is, the group modulo scalars. The 'groups' that we are going to demonstrate are not always well-defined are often referred to as $\mathrm{P\Sigma U}_n(q)$, $\mathrm{\Sigma U}_n(q)$, $\mathrm{P\Sigma\Omega}^{\varepsilon}_n(q)$, $\mathrm{\Sigma\Omega}^{\varepsilon}_n(q)$, $\mathrm{P\Sigma O}^{\varepsilon}_n(q)$, $\mathrm{\Sigma O}^{\varepsilon}_n(q)$ and purportedly consist of $\mathrm{SU}_n(q)$, $\Omega^{\varepsilon}_n(q)$, $\mathrm{SO}^{\varepsilon}_n(q)$ or their projective variants, extended by Φ or ϕ respectively.

We will show that the isomorphism type of the group may depend on the choice of form matrix. For example, the two natural but distinct choices for unitary forms, namely those represented by the matrices I_n and $\mathrm{AntiDiag}(1, \ldots, 1)$, can give rise to non-isomorphic groups $\mathrm{\Sigma U}_n(q)$.

It was previously known that these 'groups' are not well-defined, but this knowledge was not widespread. For example, Magma [1] contains functions to produce certain of these groups. The notation $\mathrm{P\Sigma U}_3(5^2)$ (which, in our notation, would be written as $\mathrm{P\Sigma U}_3(5)$) is used in [3, Theorem 3.16(iv)] to denote the automorphism group of the

The third author would like to acknowledge the support of the Nuffield Foundation.

Hoffman–Singleton graph, which is the unique graph on 50 points of valency 7 and diameter 2. Fortunately there is only one isomorphism type in this particular case!

We determine for which n and q these groups are well-defined: our results are summarized below. When there is more than one isomorphism type of group satisfying the definition, we determine the number of isomorphism types, and it turns out that there are never more than two. We then present a polynomial-time algorithm to determine whether two such groups are isomorphic, given the corresponding classical forms.

By the *type* of a classical group we mean one of: unitary, symplectic, orthogonal in odd dimension, orthogonal of sign $+$, orthogonal of sign $-$. Recall that $u = 2$ for unitary groups and $u = 1$ otherwise. Let $\mathrm{M}_n(q^u)$ be the set of $n \times n$ matrices with entries in $\mathbb{F}_{q^u}$, and let $C_n(q, A)$ denote one of $\mathrm{SU}_n(q)$, $\mathrm{Sp}_n(q)$, $\Omega_n^\varepsilon(q)$ or $\mathrm{SO}_n^\varepsilon(q)$, fixing a non-degenerate form represented by the matrix $A \in \mathrm{M}_n(q^u)$. In the orthogonal cases, we choose A to represent a symmetric bilinear form in odd characteristic and a quadratic form in even characteristic. We assume throughout that $n > 2$ in the orthogonal case, and $n > 1$ otherwise, so that $C_n(q, A)$ is absolutely irreducible (see [7, Proposition 2.10.6]), and that all forms are non-degenerate.

Suppose that $C_n(q, A)$ is invariant under the map Φ as above. We can think of $C_n(q, A)$ and Φ as lying within the group $\Gamma\mathrm{L}_n(q^u)$ of semilinear transformations of $\mathbb{F}_{q^u}^n$, and we denote the subgroup of $\Gamma\mathrm{L}_n(q^u)$ that they generate by $\langle C_n(q, A), \Phi \rangle$. This is also isomorphic to the semidirect product $C_n(q, A) : \langle \Phi \rangle$ of $C_n(q, A)$ by its cyclic group of automorphisms generated by Φ.

For the special linear group, given n and q there is a unique copy of $\mathrm{SL}_n(q)$ inside $\mathrm{GL}_n(q)$, and hence a unique group $\langle \mathrm{SL}_n(q), \Phi \rangle$ up to isomorphism. We denote this group by $\Sigma\mathrm{L}_n(q)$.

We shall show the following.

(i) When n is even and p is odd, there are two isomorphism classes of groups $\langle \mathrm{SU}_n(q), \Phi \rangle$ and $\langle \mathrm{U}_n(q), \phi \rangle$, so the notation $\Sigma\mathrm{U}_n(q)$, $\mathrm{P}\Sigma\mathrm{U}_n(q)$ is ambiguous.

(ii) When n and f are both even, there are two isomorphism classes of groups $\langle \Omega_n^+(q), \Phi \rangle$ and $\langle \mathrm{P}\Omega_n^+(q), \phi \rangle$, so the notation $\mathrm{P}\Sigma\Omega_n^+(q)$, $\Sigma\Omega_n^+(q)$ is ambiguous.

(iii) When n and f are both even and p is odd, there are two isomorphism classes of groups $\langle \mathrm{SO}_n^+(q), \Phi \rangle$ and $\langle \mathrm{PSO}_n^+(q), \phi \rangle$, so the notation $\mathrm{P}\Sigma\mathrm{O}_n^+(q)$, $\Sigma\mathrm{O}_n^+(q)$ is ambiguous.

(iv) When n and f are even, there is no choice of a bilinear or quadratic orthogonal form of $-$ type for which $C_n(q, A)$ is invariant under Φ, so there is no natural or canonical way of defining $\mathrm{P}\Sigma\Omega_n^-(q)$, $\Sigma\Omega_n^-(q)$, $\mathrm{P}\Sigma\mathrm{O}_n^-(q)$, $\Sigma\mathrm{O}_n^-(q)$.

(v) In all other cases where $C_n(q, A)$ is invariant under Φ, there is a unique isomorphism class of groups $\langle C_n(q, A), \Phi \rangle$, and similarly for the projective variants. This applies in particular to the symplectic groups.

Of course, when $C_n(q, A)$ is not invariant under Φ field automorphisms do exist, but they are defined as the composite of the map Φ and conjugation by an element of $\mathrm{GL}_n(q)$. Note also that in cases (ii) and (iii), the two isomorphism classes result

from form matrices in $\mathrm{M}_n(p)$ that are of different signs when regarded as form matrices over $\mathbb{F}_p$.

2 Preliminary results and notation

Let Σ be the map from $\mathrm{M}_n(q^u)$ to itself which sends each entry of a matrix to its qth power. Note that Σ is non-trivial only when the case is unitary. If A is the matrix of a unitary form then $A^\Sigma = A^{\mathrm{T}}$, so if A and λA both represent unitary forms then $\lambda \in \mathbb{F}_q^\times$. If A is the matrix of a symplectic or symmetric bilinear form, then all non-zero scalar multiples of A represent symplectic or symmetric bilinear forms, respectively. We will discuss quadratic forms in Section 4.

In parts (2) and (3) of the following lemma, if $\lambda = 1$ then x is an *isometry*, otherwise x is a *similarity*.

Lemma 1. *Let $G = C_n(q, A)$ and $H = C_n(q, B)$ be absolutely irreducible, isomorphic and of the same type, with q odd if the type is orthogonal. Then*

(1) *$G = C_n(q, \lambda A)$ for all $\lambda \in \mathbb{F}_q^\times$.*

(2) *There exists $x \in \mathrm{GL}_n(q^u)$ such that $H^x = G$. Such an x may be chosen to satisfy $xAx^{\mathrm{T}\Sigma} = B$ unless the type is orthogonal of odd dimension and the determinant of AB is non-square, in which case x may be chosen to satisfy $xAx^{\mathrm{T}} = \lambda B$ for any non-square λ.*

(3) *Let $x \in \mathrm{GL}_n(q^u)$. Then $H^x = G$ if and only if $xAx^{\mathrm{T}\Sigma} = \lambda B$ for some $\lambda \in \mathbb{F}_q^\times$.*

Proof. (1) Let $\lambda \in \mathbb{F}_q^\times$ and $g \in G$. Then $g\lambda A g^{\mathrm{T}\Sigma} = \lambda g A g^{\mathrm{T}\Sigma} = \lambda A$.

(2) It is proved in [7, Propositions 2.3.1, 2.4.1, 2.5.4] that all such forms are isometric, with the exception of the orthogonal forms in odd dimension where there are two isometry classes but one similarity class. The two classes are distinguished by whether the determinant of the form matrix is a square. Hence such an x exists in all cases.

(3) First assume that $x^{-1}Hx = G$. Then for all $h \in H$ there exists $g \in G$ with $h = xgx^{-1}$ such that

$$hxAx^{\mathrm{T}\Sigma}h^{\mathrm{T}\Sigma} = xgx^{-1}xAx^{\mathrm{T}\Sigma}(xgx^{-1})^{\mathrm{T}\Sigma} = xAx^{\mathrm{T}\Sigma},$$

so H preserves the form with matrix $xAx^{\mathrm{T}\Sigma}$. Since a form matrix represents an isomorphism between two modules which, by assumption, are absolutely irreducible, we must have $xAx^{\mathrm{T}\Sigma} = \lambda B$ for some $\lambda \in \mathbb{F}_{q^u}^\times$. In the unitary case, since A and B are unitary forms, $\lambda \in \mathbb{F}_q$.

Now assume that $xAx^{\mathrm{T}\Sigma} = \lambda B$, and let $h \in H$. Then

$$\begin{aligned} x^{-1}hxA(x^{-1}hx)^{\mathrm{T}\Sigma} &= x^{-1}hx \cdot x^{-1}\lambda B(x^{-1})^{\mathrm{T}\Sigma} \cdot x^{\mathrm{T}\Sigma}h^{\mathrm{T}\Sigma}(x^{-1})^{\mathrm{T}\Sigma} \\ &= \lambda x^{-1}hBh^{\mathrm{T}\Sigma}(x^{-1})^{\mathrm{T}\Sigma} \\ &= x^{-1}\lambda B(x^{-1})^{\mathrm{T}\Sigma} = A. \end{aligned}$$

Thus H^x fixes A and, since G and H are of the same type, $H^x = G$. □

In the following lemma, and for the remainder of the paper, we abbreviate $(x^{-1})^{\Phi}$ by $x^{-\Phi}$.

Lemma 2. *Let $G = C_n(q, A)$ and $H = C_n(q, B)$ with G and H absolutely irreducible, isomorphic and of the same type, with q odd if the type is orthogonal. Then*

(1) *G^{Φ} preserves a classical form of the same type as A with matrix A^{Φ}.*

(2) *For all $x \in \mathrm{GL}_n(q^u)$, if $G^x = H$ then $\langle G, \Phi\rangle^x = \langle H, \Phi x^{-\Phi} x\rangle$. Furthermore, if $A, B \in \mathrm{M}_n(p)$ and $xBx^{\Sigma \mathrm{T}} = A$ then $(x^{-\Phi}x)B(x^{-\Phi}x)^{\Sigma \mathrm{T}} = B$.*

(3) *$\Phi \in \mathrm{N}_{\Sigma \mathrm{L}_n(q^u)}(G)$ if and only if $A = \lambda A'$ for some $A' \in \mathrm{M}_n(p)$.*

Proof. (1) Let $g \in G$. Then $g^{\Phi}A^{\Phi}g^{\mathrm{T}\Sigma\Phi} = (gAg^{\mathrm{T}\Sigma})^{\Phi} = A^{\Phi}$. Since Φ commutes with transposition, negation and Σ, the matrix A^{Φ} represents a form of the same type as A.

(2) These are straightforward calculations. Firstly

$$\Phi^x = x^{-1}\Phi x = \Phi\Phi^{-1}x^{-1}\Phi x = \Phi x^{-\Phi}x,$$

and secondly

$$x^{-\Phi}xBx^{\Sigma \mathrm{T}}x^{-\Phi\Sigma \mathrm{T}} = (x^{-1}Ax^{-\Sigma \mathrm{T}})^{\Phi} = B^{\Phi} = B.$$

(3) By Lemma 1 (3), for Φ to normalize G we require $A^{\Phi} = \lambda A$ for some $\lambda \in \mathbb{F}_q^{\times}$. If a, b are any two non-zero entries of A, then since $a^p = \lambda a$ and $b^p = \lambda b$ it follows that $a^{p-1} = b^{p-1}$. Hence a and b differ by a $(p-1)$st root of unity, that is, by an element of $\mathbb{F}_p$. □

Therefore Φ normalizes $C_n(q, A)$ only when $A = \lambda A'$ with $A' \in \mathrm{M}_n(p)$, in which case $C_n(q, A) = C_n(q, A')$. For other matrices A, consider the generators of the group of field automorphisms in the normalizer of $C_n(q, A)$ in $\Sigma \mathrm{L}_n(q)$. They have the form $\Phi z \in \Sigma \mathrm{L}_n(q)$, where $zAz^{\mathrm{T}\Sigma} = \lambda A^{\Phi}$ for some $\lambda \in \mathbb{F}_q$. A suitable z of determinant 1 may not exist, since $\mathrm{SL}_n(q)$ generally contains more than one conjugacy class of each classical group, and these classes are permuted by the diagonal and field automorphisms. In particular if $\det(A)^{1-p} \notin \{\lambda^n : \lambda \in \mathbb{F}_{q^u}^{\times}\}$ then no such z exists. So we shall restrict attention to $A \in \mathrm{M}_n(p)$, and take z to be the identity.

The following is used to determine whether two groups of the form $\langle C_n(q, A), \Phi\rangle$ are isomorphic.

Lemma 3. *Let S be a non-abelian simple group and let $A, B \leqslant \mathrm{Out}(S)$. Then the inverse images of A and B in $\mathrm{Aut}(S)$ are isomorphic if and only if A is conjugate in $\mathrm{Out}(S)$ to B.*

2.1 Symplectic groups. We briefly examine the symplectic groups, and prove that $\mathrm{P}\Sigma \mathrm{Sp}_n(q)$ and $\Sigma \mathrm{p}_n(q)$ are well-defined.

Theorem 4. *Let n be even and let $G = \mathrm{Sp}_n(q, A)$ and $H = \mathrm{Sp}_n(q, B)$ where $A, B \in \mathrm{M}_n(p)$. Then $\langle G, \Phi\rangle \cong \langle H, \Phi\rangle$, and hence their projective images are also isomorphic.*

Proof. By Lemma 1 applied to $\mathrm{Sp}_n(p, A)$ and $\mathrm{Sp}_n(p, B)$ there exists $x \in \mathrm{GL}_n(p)$ with $xAx^{\mathrm{T}} = B$; but then Lemma 1(3) implies $H^x = G$. Now $x^\Phi = x$ and so $\langle H, \Phi\rangle^x = \langle G, \Phi\rangle$. □

3 Unitary groups

In this section we show that, even when we restrict to those unitary forms that can be written over $\mathbb{F}_p$, there can be more than one isomorphism class of groups $\langle \mathrm{U}_n(q, A), \phi\rangle$.

Let $m = (q+1, n)$. The outer automorphism group of $\mathrm{U}_n(p^f)$ has presentation $\langle \phi, \delta \mid \phi^{2f} = 1, \delta^m = 1, \delta^\phi = \delta^p\rangle$. With respect to the identity form ϕ is as before and δ extends $\mathrm{U}_n(q)$ to $\mathrm{PGU}_n(q)$. Let Δ be a corresponding matrix, extending $\mathrm{SU}_n(q)$ to $\mathrm{GU}_n(q)$. Note that $\det(\Delta)$ can be taken to be any primitive $(q+1)$st root of unity. Each element of the outer automorphism group can be written as $\phi^i\delta^j$ for $0 \leqslant i \leqslant 2f-1$ and $0 \leqslant j \leqslant m-1$.

Lemma 5. *If q is odd and n is even then the sets $\{\phi\delta^{2i} : 0 \leqslant i \leqslant (m/2-1)\}$ and $\{\phi\delta^{2i+1} : 0 \leqslant i \leqslant (m/2-1)\}$ are conjugacy classes in $\mathrm{Out}(\mathrm{U}_n(q))$. Otherwise $\{\phi\delta^i : 0 \leqslant i \leqslant m-1\}$ is one class. Furthermore, if there are two such conjugacy classes then the cyclic groups generated by elements from distinct classes are not conjugate as subgroups of $\mathrm{Out}(\mathrm{U}_n(q))$.*

Proof. Note that

$$(\phi\delta^i)^\delta = \delta^{-1}\phi\delta^{i+1} = \phi\phi^{-1}\delta^{-1}\phi\delta^{i+1} = \phi\delta^{i+1-p},$$

and $(\phi\delta^i)^\phi = \phi\delta^{ip}$. Therefore the conjugacy class of $\phi\delta^i$ contains

$$S_i := \{\phi\delta^{i+j(1-p)} : 0 \leqslant j \leqslant m-1\}.$$

The size of the set S_i is independent of i, and the number of such sets S_i is $(m, p-1) = (n, q+1, p-1)$. Since $p-1$ divides $q-1$, the greatest common divisor of $p-1$ and $q+1$ is 2 if p is odd and 1 if $p = 2$. Hence the number of such conjugacy classes is at most 2 if p is odd and n is even, and is 1 otherwise.

If p is odd and n is even, then $A_i := \{\phi\delta^{ip^j} : 0 \leqslant j \leqslant 2f\} \subseteq S_i$. Since the conjugacy class of $\phi\delta^i$ is the union of A_i and S_i, there are indeed two conjugacy classes. The final statement is clear. □

In the following theorem, ω denotes the exponent in the theoretical complexity of matrix multiplication. (The best known bounds are currently that $2 \leqslant \omega \leqslant 2.236$.)

Theorem 6. *Let n be even and q be odd. Let $\mathscr{S}$ be the set of all groups $G = \langle \mathrm{SU}_n(q, A), \Phi \rangle$ that preserve a non-degenerate unitary form with matrix $A \in \mathrm{M}_n(p)$. Then $\mathscr{S}$ contains two isomorphism classes of groups, and the same is true for projective versions. Given the corresponding form matrices, in $\mathrm{O}(n^\omega + \log p)$ finite field operations one can determine whether two such groups are isomorphic.*

Proof. Let $G = \mathrm{SU}_n(q, A)$ and $H = \mathrm{SU}_n(q, B)$ with $A, B \in \mathrm{M}_n(p)$ non-degenerate. By Lemma 1, there exists $x \in \mathrm{GL}_n(q^2)$ such that $B = xAx^{\mathrm{T}\Sigma}$ and $H^x = G$. Denoting $\det(x)$ by $\mu \in \mathbb{F}_{q^2}^\times$ we see that $\det(B)/\det(A) = \det(x)^{q+1}$, and so $v := \mu^{q+1} \in \mathbb{F}_p^\times$. By Lemma 2, $\langle H, \Phi \rangle^x = \langle G, \Phi x^{-\Phi} x \rangle$ with $x^{-\Phi} x \in \mathrm{GU}_n(q, A)$. Hence $x^{-\Phi} x$ is equal (modulo G) to a power of Δ.

If $\langle H, \Phi \rangle^x \cong \langle G, \Phi \rangle$ then by Lemmas 3 and 5, $x^{-\Phi} x$ corresponds to an even power of δ, so $\det(x^{-\Phi} x) = \mu^{1-p}$ is a square in $K_q := \{x \in \mathbb{F}_{q^2} : x^{q+1} = 1\}$. Now $(\mu^{(1-p)/2})^{q+1} = v^{(1-p)/2}$, which is equal to 1 if $v \in \mathbb{F}_p^{\times 2}$ and equal to -1 otherwise. Therefore μ is a non-square in K_q whenever $\det(B)/\det(A) \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$. Now letting $\langle \alpha \rangle = \mathbb{F}_p^\times$, and setting $A = \mathrm{Diag}(\alpha, 1, \ldots, 1)$, $B = \mathrm{I}_n$ shows that μ can be non-square, and hence that there are two isomorphism types of groups consisting of $\mathrm{U}_n(q)$ extended by a field automorphism.

Given $A, B \in \mathrm{M}_n(p)$, we calculate $\xi = \det(A)\det(B)$ in $\mathrm{O}(n^\omega)$ field operations [2] and determine whether $\xi \in \mathbb{F}_p^{\times 2}$ in $\mathrm{O}(\log p)$ field operations [5, Theorem 8.12]. □

Proposition 7. *For qn odd or q even, let $G = \mathrm{SU}_n(q, A)$ and $H = \mathrm{SU}_n(q, B)$ with $A, B \in \mathrm{M}_n(p)$. Then $\langle G, \Phi \rangle \cong \langle H, \Phi \rangle$, and hence their projective images are also isomorphic.*

Proof. Fix $x \in \mathrm{GL}_n(q^2)$ such that $xAx^{\mathrm{T}} = B$ and $H^x = G$. Then

$$\langle H, \Phi \rangle^x = \langle G, \Phi x^{-\Phi} x \rangle,$$

where $x^{-\Phi} x$ corresponds projectively to δ^i for some i. Thus $\Phi x^{-\Phi} x$ lies in the same conjugacy class of $\mathrm{Aut}(G)$ as Φ by Lemma 5, and so $\langle H, \Phi \rangle \cong \langle G, \Phi \rangle$ by Lemma 3. □

4 Orthogonal groups

The *discriminant* of a bilinear form over a field of odd characteristic is square if the determinant of the corresponding matrix is a square, and is non-square otherwise.

In odd dimension we assume that q is odd (for irreducibility). There are two isometry types of orthogonal group, differentiated by discriminant. Since the form matrices for the two isometry types can be taken to be A and λA for λ a non-square, the corresponding groups are the same.

In even dimension there are two similarity types of orthogonal group, denoted by $+$ and $-$. When q is odd the discriminant of the form is square if either the type is $+$ and $(q-1)n/4$ is even, or the type is $-$ and $(q-1)n/4$ is odd; otherwise for odd q the discriminant is non-square [7, Proposition 2.5.10]. Note, therefore, that if f is even

then a form over $\mathbb{F}_q$ with symmetric bilinear form matrix $A \in \mathrm{M}_n(p)$ can have a different sign when considered as a form over $\mathbb{F}_p$.

Lemma 8. (1) *If f and n are even, then all symmetric bilinear or quadratic form matrices in $\mathrm{M}_n(p)$ are of $+$ type as forms over $\mathbb{F}_q$. If f is odd, then forms represented by matrices in $\mathrm{M}_n(p)$ have the same types as forms over $\mathbb{F}_p$ and over $\mathbb{F}_q$.*

(2) *In $+$ type there exist form matrices that are fixed by Φ for all q.*

(3) *In $-$ type there exist form matrices that are fixed by Φ if and only if f is odd.*

Proof. The first statement of (1) is proved in [7, p. 40]. Any isometry between forms in $\mathrm{GL}_n(p)$ is an isometry in $\mathrm{GL}_n(q)$, so forms of the same type over $\mathbb{F}_p$ are also of the same type over $\mathbb{F}_q$.

Standard bases for quadratic forms are described in [7, Proposition 2.5.3]. The corresponding $+$ type matrices have entries 0 or 1, which proves (2). (In fact, after a reordering of the basis the quadratic form matrix is $\mathrm{AntiDiag}(1, \ldots, 1, 0, \ldots, 0)$, with half of the entries 1.) This shows that forms of $+$ type over $\mathbb{F}_p$ are also of $+$ type over $\mathbb{F}_q$.

The quadratic or bilinear form for the $\mathbb{F}_p$-basis given in [7, Proposition 2.5.3 (ii)] is still of $-$ type when viewed as a matrix over any odd degree field extension, because the irreducible quadratic used in its definition remains irreducible. Hence all form matrices of $-$ type over $\mathbb{F}_p$ are of $-$ type over $\mathbb{F}_q$, which completes the proof of (1). Then (3) follows immediately from (1). □

Thus in $-$ type if f is even then Φ can never fix the form. In this instance $\mathrm{Out}(\Omega_n^-(q))$ is isomorphic to $\mathrm{C}_2 \times \mathrm{C}_{2f}$ and hence does not contain an element of order f that generates the field automorphisms. We shall not consider this case any further.

Let q be even, and let A be a matrix of a non-degenerate quadratic form over $\mathbb{F}_q$. For $A, B \in \mathrm{M}_n(q)$, we write $A \equiv B$ if $A_{ii} = B_{ii}$ for $1 \leqslant i \leqslant n$ and $A + A^{\mathrm{T}} = B + B^{\mathrm{T}}$. Note that $A + A^{\mathrm{T}}$ is the matrix of the corresponding symplectic form, and that $x \in \mathrm{GL}_n(q)$ preserves the quadratic form if and only if $xAx^{\mathrm{T}} \equiv A$. Lemmas 1 and 2 still apply, but with the modification that there exists $x \in \mathrm{GL}_n(q)$ such that $B \equiv xAx^{\mathrm{T}}$ and $H^x = G$ (note that for Lemma 1 (3) with $(n, q, \pm) = (4, 2, +)$ we calculate this directly, as the proof strategy does not apply).

Proposition 9. *Let $G = \Omega_n^e(q, A)$ and $H = \Omega_n^e(q, B)$, where the quadratic or bilinear form matrices $A, B \in \mathrm{M}_n(p)$ have the same type when considered as form matrices over $\mathbb{F}_p$. Then $\langle G, \Phi \rangle \cong \langle H, \Phi \rangle$. The same statement is true for $\mathrm{SO}_n^e(q)$, and also for projective versions.*

Proof. If n is odd and A and B have different discriminants over $\mathbb{F}_p$ then, since $H = \Omega_n(q, \mu B)$ where $\mu \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$, we may replace B by μB. So we assume without loss of generality that the discriminants of A and B are equal. Then since A and B

have the same type and discriminant over $\mathbb{F}_p$, by Lemmas 1 and 2 there is an isometry $x \in \mathrm{GL}_n(p)$ such that $\langle H, \Phi\rangle^x = \langle G, \Phi x^{-\Phi} x\rangle$. Since $x^\Phi = x$ the groups are isomorphic. □

Since there are only two isometry types of forms over $\mathbb{F}_p$, we have the following result:

Corollary 10. *There are at most two isomorphism types of groups $\langle G, \Phi\rangle$ arising from groups $G = \Omega_n^\varepsilon(q, A), \mathrm{SO}_n^\varepsilon(q, A)$ or their projective variants, for form matrices $A \in \mathrm{M}_n(p)$.*

Proposition 11. *If f or n is odd, then there is a unique isomorphism type of groups $\langle G, \Phi\rangle$ for $G = \Omega_n^\varepsilon(q, A)$, $\mathrm{SO}_n^\varepsilon(q, A)$ or their projective variants, for form matrices $A \in \mathrm{M}_n(p)$.*

Proof. Let $G = \Omega_n^\varepsilon(q, A)$ and $H = \Omega_n^\varepsilon(q, B)$, where $A, B \in \mathrm{M}_n(p)$. If n is odd then A and B have the same type over $\mathbb{F}_p$, and so the result follows from Proposition 9.

If f is odd then, by Lemma 8 (1), the fact that A and B have the same type over $\mathbb{F}_q$ implies that they have the same type over $\mathbb{F}_p$ and again the result follows from Proposition 9. □

Proposition 12. *For f and n both even, there are two isomorphism types of groups $\langle G, \Phi\rangle$ for $G = \Omega_n^+(q, A), \mathrm{P}\Omega_n^+(q, A)$, with form matrices $A \in \mathrm{M}_n(p)$. If q is odd, then the same is true for $G = \mathrm{SO}_n^+(q, A), \mathrm{PSO}_n^+(q, A)$.*

If $A, B \in \mathrm{M}_n(p)$ are of + type then in $\mathrm{O}(n^\omega + \log p)$ (for p odd) or $\mathrm{O}(n^3)$ (for $p = 2$) field operations, we may determine whether $\langle \Omega_n^+(q, A), \Phi\rangle \cong \langle \Omega_n^+(q, B), \Phi\rangle$, and similarly for other types of G.

Proof. Let $G = \Omega_n^+(q, A)$ and $H = \Omega_n^+(q, B)$, with $A, B \in \mathrm{M}_n(p)$. Suppose first that $p \neq 2$. There exists $x \in \mathrm{GL}_n(q)$ such that $\langle H, \Phi\rangle^x = \langle G, \Phi x^{-\Phi} x\rangle$ and $x^{-\Phi} x \in \mathrm{GO}_n^+(q, A)$.

For odd q the group $\mathrm{Out}(G)$ has a normal subgroup $N \cong \mathrm{D}_8$ corresponding to $\mathrm{N}_{\mathrm{GL}_n(q)}(G)$, and $\mathrm{Out}(G)/N \cong \mathrm{C}_f$ and is generated by the image of a field automorphism ϕ; see [7, Proposition 2.7.3 (i)]. The centre of N corresponds to an automorphism induced by elements of $\mathrm{SO}_n^+(q)$, and ϕ centralizes N modulo its centre. So if $g \in N \backslash \mathrm{Z}(N)$ then $\langle \phi\rangle$ is not conjugate to $\langle \phi g\rangle$ in $\mathrm{Out}(N)$.

Let $\alpha \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$, and let $A = \mathrm{I}_n$ and $B = \mathrm{Diag}(\alpha, 1, \ldots, 1)$. Since f is even, α has a square root $\mu \in \mathbb{F}_q^\times$, and $x = \mathrm{Diag}(\mu, 1, \ldots, 1)$ satisfies $xAx^{\mathrm{T}} = B$. Then $\det(x^{-\Phi} x) = \mu^{1-p} \neq 1$ since $\mu \notin \mathbb{F}_p$. Hence $x^{-\Phi} x \notin \mathrm{SO}_n^+(q, A)$ and so, by the discussion in the preceding paragraph, ϕ is not conjugate in $\mathrm{Out}(G)$ to ϕg, where g is the element of $\mathrm{Out}(G)$ induced by $x^{-\Phi} x$. So by Lemma 3 the groups $\langle H, \Phi\rangle$ and $\langle G, \Phi\rangle$ are not isomorphic, and the result follows from Corollary 10. The same argument applies with G and H replaced by $\mathrm{SO}_n^+(q, A)$ and $\mathrm{SO}_n^+(q, B)$.

In order to determine whether two such groups are isomorphic, we calculate $\zeta := \det(A)\det(B)$ in $\mathrm{O}(n^\omega)$ field operations [2], then check whether $\zeta \in \mathbb{F}_p^{\times 2}$ in $\mathrm{O}(\log p)$ field operations [5, Theorem 8.12].

Next let q be even, and recall the equivalence on form matrices described before Proposition 9. From [7, Proposition 2.7.3(i)] we have $\mathrm{Out}(G) = \langle r \rangle \times \langle \phi \rangle$, where $|r| = 2$ and r is induced by elements of $\mathrm{SO}_n^+(q)\backslash\Omega_n^+(q)$. To complete the proof, we find form matrices $A, B \in \mathrm{M}_n(p)$ and $x \in \mathrm{GL}_n(q)$ such that $xAx^{\mathrm{T}} \equiv B$ and $x^{-\Phi}x \in \mathrm{SO}_n^+(q, A)\backslash\Omega_n^+(q, A)$.

Let P_n denote the upper triangular matrix $\mathrm{AntiDiag}(1, \ldots, 1, 0, \ldots, 0)$ with $n/2$ entries equal to 1. Then P_n represents a quadratic form of $+$ type over $\mathbb{F}_2$ by [7, Proposition 2.5.3], and hence also over $\mathbb{F}_{2^f}$ for any f. The polynomial $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, so the 2×2 matrix

$$M_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

represents a form of $-$ type over $\mathbb{F}_2$. Hence, for n even, $A := P_2 \oplus P_{n-2}$ and $B := M_2 \oplus P_{n-2}$ are of opposite types over $\mathbb{F}_2$, but since f is even, they are both of $+$ type over $\mathbb{F}_q$ by Lemma 8. Let v be an element of multiplicative order 3 in $\mathbb{F}_q$ (note that v exists since f is even), and let

$$x = \begin{pmatrix} 1 & 1 \\ v & v^2 \end{pmatrix} \oplus \mathrm{I}_{n-2}.$$

The reader can check that $xAx^{\mathrm{T}} \equiv B$ and that $x^{-\Phi}x = \mathrm{AntiDiag}(1, 1) \oplus \mathrm{I}_{n-2}$. The spinor norm of $g \in \mathrm{M}_n(2^f)$ is equal to the parity of the rank of $g + \mathrm{I}_n$ (see [4]), and so $x^{-\Phi}x$ has spinor norm 1.

To determine whether two such groups are isomorphic we first find an isometry x between the quadratic forms over $\mathbb{F}_4$ in $\mathrm{O}(n^3)$ field operations [6, Proposition 3.4], then calculate the rank of $x^{-\Phi}x$ in $\mathrm{O}(n^\omega)$ field operations [2]. □

Bibliography

[1] W. Bosma and J. J. Cannon, eds. *Handbook of Magma functions*. Edition 2.13 (2006).

[2] P. Bürgisser, M. Clausen and M. A. Shokrollahi. *Algebraic complexity theory* (Springer-Verlag, 1990).

[3] P. J. Cameron. *Permutation groups*. London Math. Soc. Student Texts 45 (Cambridge University Press, 1999).

[4] R. H. Dye. A geometric characterisation of the special orthogonal groups and the Dickson invariant. *J. London Math. Soc.* (2) **15** (1977), 472–476.

[5] K. O. Geddes, S. R. Czapor and G. Labahn. *Algorithms for computer algebra* (Kluwer Academic Publishers, 1992).

[6] D. F. Holt and C. M. Roney-Dougal. Constructing maximal subgroups of classical groups. *LMS J. Comput. Math.* **8** (2005), 46–79.

[7] P. B. Kleidman and M. W. Liebeck. *The subgroup structure of the finite classical groups*. London Math. Soc. Lecture Note Ser. 129 (Cambridge University Press, 1990).

Received 21 December, 2007

John N. Bray, School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, U.K.
E-mail: j.n.bray@qmul.ac.uk

Derek F. Holt, Mathematics Institute, University of Warwick, Coventry CV4 7AL, U.K.
E-mail: d.f.holt@warwick.ac.uk

Colva M. Roney-Dougal, School of Mathematics and Statistics, North Haugh, St Andrews, Fife KY16 9SS, U.K.
E-mail: colva@mcs.st-and.ac.uk