Appendix 2 Clifford algebras and Lie triple systems

Section 1 Preliminaries

Good general references for this section are [LM, chapter 1] and [FH, pp. 299-315]. We are especially indebted to D. Shapiro [S2] who explained the ideas behind the proofs of Propositions 2.6 through 2.8 and the first three assertions of the main result in section 3.

Let V be a finite dimensional real inner product space, and let $C\ell(V)$ denote the Clifford algebra determined by V according to the multiplication rule

(1) $xy + yx = -2 < x,y >$ for all $x,y \in V$

The algebra $C\ell(V)$ becomes a Lie algebra with the bracket operation given by

(2) $[a, b] = (1/2) \{ab - ba\}$ for all $a,b \in C\ell(V)$

In particular

$[x, y] = xy + < x, y >$ for all $x,y \in V$

A representation of $C\ell(V)$ on a finite dimensional real vector space U is an algebra homomorphism $j : C\ell(V) \to End(U)$ such that

(3) $j(x)\, j(y) + j(y)\, j(x) = -2 < x, y > Id$ for all $x,y \in V$

Note that j is almost a Lie algebra homomorphism. Specifically,

(4) $j([a, b]) = (1/2)\, [\, j(a), j(b)] = (1/2)\ \{j(a)\, j(b) - j(b)\, j(a)\}$ for all $a,b \in C\ell(V)$

Hence $\psi = (1/2)\, j : C\ell(V) \to End(V)$ is a Lie algebra homomorphism.

Clifford algebras satisfy the following universal mapping property (cf. Proposition 1.1 of [LM]) :

(5) Let $\{V, < , >\}$ be a finite dimensional real inner product space, and let $\sigma : V \to \mathfrak{A}$ be an $\mathbb{R}$-linear map into an associative $\mathbb{R}$-algebra $\mathfrak{A}$ with unit 1 such that $\sigma(v)\cdot\sigma(v) = -|v|^2\, 1$ for all $v \in V$. Then σ extends uniquely to an $\mathbb{R}$-algebra homomorphism $\sigma : C\ell(V) \to \mathfrak{A}$.

If $\alpha : V \to C\ell(V)$ is the $\mathbb{R}$-linear map such that $\alpha(v) = -v$ for all $v \in V$, then clearly $\alpha(v)\cdot\alpha(v) = v\cdot v = -|v|^2\, 1$ for all $v \in V$. Hence by (5) we obtain

(6) For any finite dimensional real inner product space V there is an involutive automorphism $\alpha : C\ell(V) \to C\ell(V)$ such that $\alpha(v) = -v$ for all $v \in V$.

Section 2

We describe briefly the classification of Clifford algebras $C\ell(V)$ and the irreducible $C\ell(V)$-modules up to equivalence. For further details see, for example, [LM, sections 1.4 and 1.5].

Classification of Clifford algebras and their modules

For an integer $p \geq 1$ let $C\ell(p)$ denote the Clifford algebra determined by $V = \mathbb{R}^p$, where < , > denotes the standard dot product. For a field K and an integer n let K(n) denote the algebra of n x n matrices with elements in K. It is well known that for each integer r, $C\ell(p)$ is isomorphic as an algebra to $K(2^k)$ or $K(2^k) \oplus K(2^k)$, where $K = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$ and k is an integer that depends on p. More specifically, one obtains the next result by induction and the information in [LM, section 1.4].

Proposition 2.1

$C\ell(8k) \cong \mathbb{R}(2^{4k})$	$C\ell(8k+1) \cong \mathbb{C}(2^{4k})$	$C\ell(8k+2) \cong \mathbb{H}(2^{4k})$
$C\ell(8k+3) \cong \mathbb{H}(2^{4k}) \oplus \mathbb{H}(2^{4k})$	$C\ell(8k+4) \cong \mathbb{H}(2^{4k+1})$	$C\ell(8k+5) \cong \mathbb{C}(2^{4k+2})$
$C\ell(8k+6) \cong \mathbb{R}(2^{4k+3})$	$C\ell(8k+7) \cong \mathbb{R}(2^{4k+3}) \oplus \mathbb{R}(2^{4k+3})$	

Relationship to the Hurwitz problem (cf. [S1])

Let K be a field with characteristic $\neq 2$, and let K^n denote the K-vector space of n-tuples $(x_1, x_2, \ldots, x_n)$, $x_i \in K$ for all i. Define a square norm $|\ |^2$ on K^n by $|(x_1, x_2, \ldots, x_n)|^2 = \sum_{i=1}^{n} x_i^2$. A triple of positive integers (r,s,n) is <u>admissible</u> if there exists a bilinear map $f : K^r \times K^s \to K^n$ such that $|f(x,y)|^2 = |x|^2 |y|^2$ for all $(x,y) \in K^r \times K^s$. Hurwitz showed that (n,n,n) is admissible $\Leftrightarrow$ n = 1,2,4 or 8. More generally, an elementary argument (cf. [S1, pp.237-238]) shows

(2.2) For $r \geq 2$ the triple (r,n,n) is admissible relative to f $\Leftrightarrow$ there exist n x n skew symmetric matrices $\{A_1, A_2, \ldots A_{r-1}\}$ such that $A_i^2 = -\mathrm{Id}$ for all i and $A_i A_j + A_j A_i = 0$ for all $i \neq j$, $1 \leq i,j \leq r-1$.

In the case that $K = \mathbb{R}$ assertion (2.2) says

(2.3) (r,n,n) is admissible for $r \geq 2 \Leftrightarrow C\ell(r-1)$ has a representation on $\mathbb{R}^n$.

Determining the set of admissible triples (r,n,n) involves the Hurwitz-Radon function $\rho : \mathbb{Z}^+ \to \mathbb{Z}^+$ defined as follows. Given a positive integer n write $n = 2^m u$, where u is odd, and define

$\rho(n) = 2m+1$ if $m \equiv 0 \pmod 4$

$\rho(n) = 2m$ if $m \equiv 1 \pmod 4$ or $m \equiv 2 \pmod 4$

$\rho(n) = 2m+2$ if $m \equiv 3 \pmod 4$

One now has

Theorem 2.4

For any field K of characteristic $\neq 2$ the triple (r,n,n) is admissible $\Leftrightarrow r \leq \rho(n)$. See [S1] for a discussion of this result with references to proofs in the literature. We use the classification of real Clifford modules to give a proof below for the case $K = \mathbb{R}$.

For $r = \rho(n)$ the literature contains several constructions of skew symmetric matrices $\{A_1, A_2, \dots A_{r-1}\}$ satisfying the conditions of (2.2) and having the additional property that each entry of each matrix A_i is 0, 1 or -1. See the references cited in [S1, p. 238].

Remark

The original Hurwitz problem follows easily from Theorem 2.4. If (n,n,n) is admissible, then $\rho(n) \geq n = 2^m u$, where u is odd. If $m \geq 4$, then $\rho(n) \leq 2m+2 < 2^m \leq n \leq \rho(n)$. Hence $m \leq 3$, and it is now easy to see that n= 1, 2, 4 or 8 are the only solutions.

Classification of irreducible Clifford modules

Proposition 2.5

1) The number of equivalence classes of irreducible finite dimensional real representations $\sigma : C\ell(m) \to End(U)$ are :

a) 1 if $m \neq 4k+3$.

b) 2 if $m = 4k+3$.

2) The dimension of an irreducible finite dimensional real representation $\sigma : C\ell(m) \to End(U)$ is an integer d(m) that depends only on m.

Proof

This is an immediate consequence of Proposition 2.1 and the next well known result (cf. Lemma 5.6 of [LM, chapter 1]). See also Proposition 2 in the discussion of two sided ideals in Clifford algebras at the end of this appendix.

Lemma 2.5

Let $K = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$. Then

a) The natural algebra representation ρ of K(n) on the vector space K^n is the only irreducible real representation of K(n) up to equivalence.

b) The algebra $K(n) \oplus K(n)$ has exactly two irreducible representations ρ_1 and ρ_2 up to equivalence. These are given by $\rho_1(\varphi_1, \varphi_2) = \rho(\varphi_1)$ and $\rho_2(\varphi_1, \varphi_2) = \rho(\varphi_2)$.

Proof of Theorem 2.4

For each positive integer p let d(p) denote the $\mathbb{R}$-dimension of an irreducible $C\ell(p)$-module. Any $C\ell(p)$-module U is a direct sum of irreducible $C\ell(p)$-modules, and it follows immediately that $C\ell(p)$ has a representation on $\mathbb{R}^n \Leftrightarrow$ d(p) divides n. From Propositions 2.1 and 2.5 it is routine to calculate the following :

$d(8k) = 2^{4k}$ $\quad d(8k+1) = 2^{4k+1}$ $\quad d(8k+2) = d(8k+3) = 2^{4k+2}$

$d(8k+a) = 2^{4k+3}$ $\quad$ for $4 \leq a \leq 7$

Hence d(p) divides $n = 2^m u$, where u is odd $\Leftrightarrow$

$m \geq 4k$ $\quad p = 8k$

$m \geq 4k+1$ $\quad p = 8k+1$

$m \geq 4k+2$ $\quad$ $p = 8k+2$ and $8k+3$

$m \geq 4k+3$ $\quad$ $p = 8k+4, 8k+5, 8k+6$ and $8k+7$

It is now a routine exercise using the definition of the Hurwitz-Radon function ρ to show $p+1 \leq \rho(n) \Leftrightarrow d(p)$ divides n. The proof is now completed by (2.3) if one sets $p = r-1$. □

Clifford algebras of dimension 4k+3

We investigate further the exceptional case of 1b) in Proposition 2.5. The relationship between the two equivalence classes of irreducible representations of $C\ell(4k+3)$ is restated in Proposition 2.7 in a form that will be more useful to us than that of Lemma 2.5.

Proposition 2.6

Let $\alpha : C\ell(m) \to C\ell(m)$ denote the involutive automorphism such that $\alpha(v) = -v$ for all $v \in \mathbb{R}^m$. Let $m = 4k+3$ for some integer $k \geq 0$. Then there exists an element z of the center of $C\ell(m)$, unique up to sign, such that $z \notin \mathbb{R}$ and $z^2 = 1$. Moreover,

1) $C\ell(m) = A_1 \oplus A_2$, where $A_1 = \{\xi \in C\ell(m) : z\xi = -\xi\}$ and $A_2 = \{\xi \in C\ell(m) : z\xi = \xi\}$.

2) A_1 and A_2 are two sided ideals of $C\ell(m)$ such that $\alpha(A_1) = A_2$ and $\alpha(A_2) = A_1$.

3) $a_1a_2 = a_2a_1 = 0$ for all $a_1 \in A_1$ and $a_2 \in A_2$.

4) A_1 and A_2 are algebras isomorphic to $C\ell(m-1)$. Moreover, both A_1 and A_2 have no proper two sided ideals.

Proposition 2.7

Let $m = 4k+3$ and let $\rho : C\ell(m) \to \mathrm{End}(U)$ be an irreducible representation on a finite dimensional real vector space U. Let $\alpha : C\ell(m) \to C\ell(m)$ denote the involutive automorphism such that $\alpha(v) = -v$ for all $v \in \mathbb{R}^m$. Then

1) $\rho' = \rho \circ \alpha : C\ell(m) \to \mathrm{End}(U)$ is an irreducible representation that is not equivalent to ρ.

2) $C\ell(m) = \mathrm{Ker}(\rho) \oplus \mathrm{Ker}(\rho')$. Moreover, $\{\mathrm{Ker}(\rho), \mathrm{Ker}(\rho')\} = \{A_1, A_2\}$, where A_1 and A_2 are the two sided ideals of $C\ell(m)$ defined in Proposition 2.6.

Remarks

1) The classification of Clifford algebras in Proposition 2.1 is used in only a few places in these two results. In Proposition 2.6 it is used only to prove the uniqueness of z and the second statement of 4). In Proposition 2.7 it is used only in the proof of 2).

2) For an alternative approach to Propositions 2.6 and 2.7 see the appendix below, " Two sided ideals in Clifford algebras ".

We need a few preliminary results before proving Proposition 2.6.

Lemma 2.6a

Let $\{e_1, e_2, \dots e_m\}$ be an orthonormal basis of $\mathbb{R}^m$, and let $z = e_1 \cdot e_2 \cdot \dots \cdot e_m$. If $m = 2n+1$, then

a) z lies in the center of $C\ell(m)$ and $z \notin \mathbb{R}$.

b) $z^2 = 1$ if $n = 2k+1$ $(m = 4k+3)$

$z^2 = -1$ if $n = 2k$ $(m = 4k+1)$

Proof of Lemma 2.6a

Using the relation (1) from section 1 it is easy to see that z commutes with each of the generators $\{e_1, e_2, \dots e_m\}$ for $C\ell(m)$ if m is odd, and hence a) holds. By applying $(2n) + (2n-1) + \dots + 1 = n(2n+1)$ interchanges of the form $e_i e_j \to e_j e_i$ the element z^2 can be brought to the form $(e_1{}^2)(e_2{}^2) \dots (e_m{}^2) = -1$. Hence $z^2 = (-1)(-1)^{(2n+1)n} = (-1)^{n+1}$. Assertion b) now follows.$\square$

An immediate consequence of the result above is

Lemma 2.6b

Let $m = 4k+3$ and let $z = z = e_1 \cdot e_2 \cdot \dots \cdot e_m$ be the element of Lemma 1. Let $e = (1/2)(1-z)$ and $e' = (1/2)(1+z)$. Then $e^2 = e$, $(e')^2 = e'$, $ze = -e$, $ze' = e'$ and $ee' = e'e = 0$.

Proof of Proposition 2.6

Let $z = e_1 \cdot e_2 \cdot \dots \cdot e_m$. Then z lies in the center of $C\ell(m)$, $z^2 = 1$ and $z \notin \mathbb{R}$ by Lemma 2.6a. We postpone the uniqueness of z, up to sign, until the end of the proof.

Let $B_1 = e\, C\ell(m)$ and $B_2 = e'\, C\ell(m)$, where e and e' are the central idempotents defined in Lemma 2.6b. Note that $C\ell(m) = B_1 + B_2$ since $e + e' = 1$. By Lemma 2.6b it follows that $B_1 \subseteq A_1$ and $B_2 \subseteq A_2$, and hence $B_1 \cap B_2 \subseteq A_1 \cap A_2 = \{0\}$. We conclude that $B_1 = A_1$ and $B_2 = A_2$ since $C\ell(m) = B_1 \oplus B_2 \subseteq A_1 \oplus A_2 \subseteq C\ell(m)$. This proves 1).

It follows from 1) and the fact that z is central that A_1 and A_2 are two sided ideals of $C\ell(m)$. By the definitions of z and α it follows that $\alpha(z) = -z$. From Lemma 2.6b it follows that $\alpha(e) = e'$ and $\alpha(e') = e$, which completes the proof of 2).

If $a_1 = e\,\xi$ and $a_2 = e'\,\xi'$ are arbitrary elements of A_1 and A_2, where ξ and ξ' are elements of $C\ell(m)$, then by Lemma 2.6b, $a_1\, a_2 = e\, e'\, \xi\, \xi' = 0$ and $a_2\, a_1 = e'\, e\, \xi'\, \xi = 0$.

It remains to prove the uniqueness of z and 4). Let z' be a central element of $C\ell(m)$, $m = 4k+3$, such that $(z')^2 = 1$ and $z' \notin \mathbb{R}$. Write $z' = a_1 + a_2$, where $a_1 \in A_1$ and

$a_2 \in A_2$. It follows easily from Lemma 2.6b that a_1 and a_2 are central elements of $C\ell(m)$. Moreover $e + e' = 1 = (z')^2 = (a_1)^2 + (a_2)^2$ by 3). By 1) we conclude that $e = (a_1)^2$ and $e' = (a_2)^2$. The elements $a_1 - e$ and $a_1 + e$ lie in the center of A_1, and $(a_1 - e)(a_1 + e) = 0$. Assume for the moment that 4) has been proved. Then A_1 and A_2 are isomorphic to $C\ell(4k+2)$, which by Proposition 2.1 is algebra isomorphic to the matrix algebra K(n), where $K = \mathbb{R}$ or $\mathbb{H}$. Hence the centers of A_1 and A_2 are fields isomorphic to $\mathbb{R}$ (cf. [J, p. 229]). It follows that either $a_1 - e = 0$ or $a_1 + e = 0$. A similar argument shows that $(a_2 - e')(a_2 + e') = 0$ and either $a_2 - e' = 0$ or $a_2 + e' = 0$. Since $z' \notin \mathbb{R}$ and $e + e' = 1$ it follows that either $z' = e - e' = -z$ or $z' = e' - e = z$.

We prove 4). Define $\varphi : \mathbb{R}^{m-1} \to A_1 = e\, C\ell(m)$ by $\varphi(v) = ev$ for all $v \in \mathbb{R}^{m-1} = \{v = (v_1, v_2, \ldots, v_m) \in \mathbb{R}^m : v_m = 0\}$. Note that A_1 is an associative algebra with unit e by Lemma 2.6b. Moreover, φ is an $\mathbb{R}$-linear map such that $\varphi(v)\cdot\varphi(v) = ev^2 = -|v|^2 e$ for all $v \in \mathbb{R}^{m-1}$. Hence φ extends uniquely to an $\mathbb{R}$-algebra homomorphism $\varphi : C\ell(m-1) \to A_1$ by the universal mapping property of Clifford algebras. Note that $-ze_m = e_1 e_2 \ldots e_{m-1}$. Since $ez = -e$ it follows that $e\, e_m = e(-z)e_m = (e\, e_1)(e\, e_2) \ldots (e\, e_{m-1}) \in \varphi(C\ell(m-1))$. We conclude that $\varphi : C\ell(m-1) \to A_1$ is surjective since $\varphi(C\ell(m-1))$ contains the algebra generators $\{(e\, e_1), (e\, e_2), \ldots (e\, e_m)\}$ of A_1. It follows that φ is an algebra isomorphism since $C\ell(m-1)$ and A_1 both have dimension 2^{m-1} over $\mathbb{R}$. By 2) $A_2 = \alpha(A_1)$ is isomorphic to A_1 and hence also to $C\ell(m-1)$. Finally, by Proposition 2.1 $C\ell(m-1) = C\ell(4k+2)$ is algebra isomorphic to K(n), where $K = \mathbb{R}$ or $\mathbb{H}$. It is well known that K(n) has no proper two sided ideals (cf. [J, pp.227-228]). This completes the proof of 4) and also of Proposition 2.6.□

Before proving Proposition 2.7 we need a preliminary result.

Lemma 2.7

Let $m = 4k+3$ and let $\rho : C\ell(m) \to \mathrm{End}(U)$ be an irreducible representation on a finite dimensional real vector space. Let $\{e_1, e_2, \ldots e_m\}$ be an orthonormal basis of $\mathbb{R}^m$, and let $z = e_1 \cdot e_2 \cdot \ldots \cdot e_m$. Then either $\rho(z) = \mathrm{Id}$ or $\rho(z) = -\mathrm{Id}$.

Proof of Lemma 2.7

By Lemma 2.6a, $\rho(z)^2 = \rho(z^2) = \mathrm{Id}$, and hence $U = U_1 \oplus U_{-1}$, where $U_1 = \{u \in U : \rho(z)u = u\}$ and $U_{-1} = \{u \in U : \rho(z)u = -u\}$. By a) of lemma 2.6a, $\rho(z)$ commutes with $\rho(C\ell(m))$, and hence $\rho(C\ell(m))$ leaves invariant both U_1 and U_{-1}. It follows that either $U = U_1$ or $U = U_{-1}$ by the irreducibility of ρ.□

Proof of Proposition 2.7

1) Let $\{e_1, e_2, \ldots e_m\}$ be an orthonormal basis of $\mathbb{R}^m$. Since $\alpha(e_i) = -e_i$ for all i and $\alpha(z) = -z$ it follows that $\rho'(e_i) = -\rho(e_i)$ for all i and $\rho'(z) = -\rho(z)$. Hence ρ' is also an irreducible representation of $C\ell(m)$ on U since any subspace W invariant under $\{\rho'(e_1),$

$\rho'(e_2)$, ...$\rho'(e_m)$} is also invariant under {$\rho(e_1)$, $\rho(e_2)$, ...$\rho(e_m)$}. By lemma 2.7 either a) $\rho(z) = Id$ and $\rho'(z) = - Id$ or b) $\rho(z) = - Id$ and $\rho'(z) = Id$. Recall that $e = (1/2)(1-z)$ and $e' = (1/2)(1+z)$. If a) holds, then Ker (ρ) contains e but not e', and Ker (ρ') contains e' but not e. Hence Ker (ρ) ≠ Ker (ρ'). A similar argument shows that Ker (ρ) ≠ Ker (ρ') in case b). If there existed an invertible linear map $T : U \to U$ such that $T \circ \rho(\xi) = \rho'(\xi) \circ T$ for all elements ξ of $C\ell(m)$, then it would follow that Ker (ρ) = Ker (ρ'). Hence ρ and ρ' are inequivalent representations of $C\ell(m)$ on U when $m = 4k+3$.

2) Since $A_1 = e\, C\ell(m)$ and $A_2 = e'\, C\ell(m)$, using the notation of Proposition 2.6, it follows that a) Ker (ρ) $\supseteq A_1$ and Ker (ρ') $\supseteq A_2$ if $\rho(z) = Id$ or b) Ker (ρ) $\supseteq A_2$ and Ker (ρ') $\supseteq A_1$ if $\rho(z) = - Id$. It suffices to prove that Ker (ρ) $\cap$ Ker (ρ') = {0}.

We consider only case a) since the proof in case b) is similar. Note that $\mathfrak{B}$ = Ker (ρ) $\cap$ Ker (ρ') is a 2-sided ideal of $C\ell(m)$ that is invariant under α since $\rho' = \rho \circ \alpha$. If $a = a_1 + a_2$ is a nonzero element of $\mathfrak{B}$, where $a_1 \in A_1$ and $a_2 \in A_2$, then we may assume that $a_1 \neq 0$, replacing a by $\alpha(a)$ if necessary. Hence $a_1 = ea_1 = ea$ is a nonzero element of $\mathfrak{B} \cap A_1$ since $e\, A_2 = e\, e'\, C\ell(m) = 0$ by lemma 2.6b. Since A_1 has no proper two sided ideals by 4) of Proposition 1 it follows that $A_1 = \mathfrak{B} \cap A_1 \subseteq \mathfrak{B} \subseteq$ Ker (ρ'). Hence Ker (ρ') $\supseteq A_1 \oplus A_2 = C\ell(m)$, a contradiction that shows $\mathfrak{B}$ = Ker (ρ) $\cap$ Ker (ρ') = {0}.□

$\mathbb{Z}$-structures for Clifford modules

The next result will be used in proving the existence of lattices for simply connected , 2-step nilpotent Lie groups N that arise from representations of Clifford algebras.

Proposition 2.8

For an integer $m \geq 2$ let $\sigma : C\ell(m) \to End(U)$ be any finite dimensional real representation. Let < , > be the standard inner product on $\mathbb{R}^m$, and let {e_1, e_2, ... e_m} be any orthonormal basis of $\mathbb{R}^m$. Then there exists an inner product < , >* on U such that $j(v) \in \mathfrak{so}(U, <,>^*)$ for every $v \in \mathbb{R}^m$, and an orthonormal basis {u_1, u_2, ... u_N} of U such that each element $\sigma(e_k)$ of End(U) has an N x N matrix A_i relative to {u_1, u_2, ... u_N} satisfying the following properties :

(1) A_i is a skew symmetric matrix such that $A_i^2 = - Id$ for $1 \leq i \leq m$.

(2) $A_i A_j = - A_j A_i$ for all $1 \leq i \neq j \leq m$.

(3) Each entry of A_i is 0, 1 or -1.

Proof

It suffices to prove this in the case that U is an irreducible $C\ell(m)$-module. We first prove that there exists some representation $\Sigma : C\ell(m) \to End(U)$ with the properties listed above, and we then deduce the result for all representations σ from Propositions 2.5 and 2.7.

Lemma 2.8

For an integer $m \geq 2$ let $< , >$ and $< , >'$ denote the standard inner products on $\mathbb{R}^m$ and $\mathbb{R}^{d(m)}$ respectively, where d(m) is the dimension of an irreducible $C\ell(m)$ module U. Let $\mathfrak{B} = \{e_1, e_2, \ldots, e_m\}$ and $\mathfrak{B}' = \{e'_1, e'_2, \ldots, e'_{d(m)}\}$ be orthonormal bases of $\mathbb{R}^m$ and $\mathbb{R}^{d(m)}$ respectively. Then there exists an irreducible representation $\Sigma : C\ell(m) \to \mathrm{End}(\mathbb{R}^{d(m)})$ such that if A_i is the matrix of $\Sigma(e_i)$ relative to $\mathfrak{B}'$ for $1 \leq i \leq m$, then the matrices $\{A_i\}$ satisfy the properties (1), (2) and (3) above.

Proof of lemma 2.8

Given an integer $m \geq 2$ we set $n = d(m)$. By the discussion above in the proof of Theorem 2.4 it is easy to check that one has $m+1 \leq \rho(n)$ in each of the cases $m = 8k+a$, $0 \leq a \leq 7$, where ρ denotes the Hurwitz-Radon function. By (2.2), Theorem 2.4 and the discussion following Theorem 2.4 there exist n x n matrices $\{A_1, A_2, \ldots, A_m\}$ that satisfy the properties (1), (2) and (3) above. Let $\sigma : \mathbb{R}^m \to \mathrm{End}(\mathbb{R}^n)$ be the $\mathbb{R}$-linear map such that $\sigma(e_i)$ is the element of $\mathrm{End}(\mathbb{R}^n)$ whose matrix is A_i relative to the basis $\mathfrak{B}'$ for $\mathbb{R}^n$, $1 \leq i \leq m$. It follows from (1), (2) and (3) that $\sigma(v)^2 = -|v|^2\,\mathrm{Id}$ for all $v \in \mathbb{R}^m$. Hence σ extends to an $\mathbb{R}$-algebra homomorphism $\sigma : C\ell(m) \to \mathrm{End}(\mathbb{R}^n)$ by the universal mapping property (5) of section 1. Since $n = d(m)$ it follows that the representation σ is irreducible. □

Proof of Proposition 2.8

Let $\sigma : C\ell(m) \to \mathrm{End}(U)$ be as in the statement of the Proposition, and assume furthermore that U is an irreducible $C\ell(m)$-module. Without loss of generality we may assume that $U = \mathbb{R}^n$, where $n = d(m)$. Let $\mathfrak{B} = \{e_1, e_2, \ldots e_m\}$ be any orthonormal basis of $\mathbb{R}^m$, and let $\mathfrak{B}' = \{e'_1, e'_2, \ldots, e'_n\}$ be an orthonormal basis of $\mathbb{R}^n$ relative to the standard inner product $< , >'$ on $\mathbb{R}^n$. Let $\Sigma : C\ell(m) \to \mathrm{End}(\mathbb{R}^n)$ be an irreducible representation that satisfies the conditions of lemma 2.8.

If $m \neq 4k+3$, then by Proposition 2.5 there exists an invertible linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ such that $T \circ \Sigma(\xi) = \sigma(\xi) \circ T$ for all $\xi \in \mathbb{R}^m$. If A_i is the matrix of $\Sigma(e_i)$ relative to $\{e'_1, e'_2, \ldots e'_n\}$, then A_i is also the matrix of $\sigma(e_i)$ relative to $\{u_1, u_2, \ldots u_n\}$, where $u_i = T(e'_i)$ for $1 \leq i \leq n$. By the statement of lemma 2.8 the matrices $\{A_i\}$ satisfy the conditions (1), (2) and (3) of the proposition. If $< , >^*$ is the inner product on $U = \mathbb{R}^n$ that makes $\{u_1, u_2, \ldots u_n\}$ an orthonormal basis of U, then $\sigma(v) \in \mathit{so}(U, < , >^*)$ for all $v \in \mathbb{R}^m$ since $\sigma(e_i) \in \mathit{so}(U, < , >^*)$ for $1 \leq i \leq m$ by (1), (2) and (3).

If $m = 4k+3$, then there are two irreducible representations of $C\ell(m)$, up to equivalence, by Proposition 2.5. By Proposition 2.7 the representation $\Sigma' : C\ell(m) \to \mathrm{End}(U)$ given by $\Sigma' = \Sigma \circ \alpha$, where α is the canonical involution of $C\ell(m)$, represents the other equivalence class of representations of $C\ell(m)$ on $\mathbb{R}^m$. Hence there exists an invertible linear map $T : \mathbb{R}^n \to \mathbb{R}^n$, $n = d(m)$, that intertwines the given represention σ and either Σ or Σ' as in the previous paragraph. By the definition of α it follows that $\Sigma'(e_i) = -\Sigma(e_i)$ for $1 \le i \le m$, and hence $\Sigma'(e_i)$ has matrix $A'_i = -A_i$ relative to the basis $\mathfrak{B}' = \{e'_1, e'_2, \ldots, e'_n\}$. It follows immediately that the matrices $\{A'_i\}$ satisfy (1), (2) and (3) since the matrices $\{A_i\}$ have this property. If $u_i = T(e'_i)$ for $1 \le i \le n$ and if $< , >^*$ is the inner product on U that makes $\{u_1, u_2, \ldots u_n\}$ an orthonormal basis, then we complete the proof as in the previous paragraph.□

Section 3 Clifford algebras and Lie triple systems

If V is a finite dimensional real inner product space, and $j : C\ell(V) \to End(U)$ is a representation, then by the discussion in section (2.2) of the main text there exists an inner product $< , >$ on U such that $j(C\ell(V)) \subseteq so(U, < , >)$. The main result in this section is that if dim V = n ≠ 3, then W = j(V) is a Lie triple system in $so(U, < , >)$ and $W \oplus [W, W]$ is an orthogonal direct sum, relative to the canonical trace form inner product on $so(U, < , >)$, that is isomorphic as a Lie algebra to $so(n+1)$. If dim V = n = 3, then there are two possibilities that are described in the main result below.

Proposition 3

Let V be a finite dimensional real inner product space, and let $C\ell(V)$ denote the Clifford algebra determined by V. Let $j : C\ell(V) \to End(U)$ denote a nonzero representation of $C\ell(V)$ on a finite dimensional real vector space U. Then

1) $V \oplus [V,V]$ is a Lie subalgebra of $C\ell(V)$ that is Lie algebra isomorphic to $so(n+1)$, where n = dim V.

2) If n = 2 or n ≥ 4, then $j : V \oplus [V,V] \to End(U)$ is injective and its image is the Lie subalgebra $j(V) \oplus [j(V), j(V)]$ of End(U), which is isomorphic to $so(n+1)$.

3) If n = 3, then either

a) $j : V \oplus [V,V] \to End(U)$ is injective with image $j(V) \oplus [j(V), j(V)]$

or

b) $j(V \oplus [V,V]) = j(V) = [j(V), j(V)]$ is a Lie subalgebra of End(U) that is Lie algebra isomorphic to $so(3)$.

4) j(V) is a Lie triple system in $so(U, < , >)$ relative to a suitable inner product $< , >$ on U. Moreover, if n = 2 or n ≥ 4, then j(V) and ([j(V), j(V)]) are orthogonal in $so(U, < , >)$ relative to the inner product $<< , >>$ given by $<< A, B >> = -\,\mathrm{trace}(AB)$ for elements A,B in $so(U, < , >)$.

Example the quaternion representation of $C\ell(\mathbb{R}^3)$

Before proving the Proposition we illustrate the case 3b) by describing a representation $j : C\ell(\mathbb{R}^3) \to End(\mathbb{R}^4)$ that is not injective on the Lie subalgebra

$\mathbb{R}^3 \oplus [\mathbb{R}^3, \mathbb{R}^3]$.

Identify $\mathbb{R}^4$ with the quaternions $\mathbb{H} = \{a + bI + cJ + dK$, with $a,b,c, d \in \mathbb{R}\}$, where the multiplication on $\mathbb{H}$ is given by $I^2 = J^2 = K^2 = -1$; $IJ = -JI = K$; $JK = -KJ = I$ and $KI = -IK = J$. Let $\mathbb{R}^3$ be given the standard inner product $< , >$, and let $\{e_1, e_2, e_3\}$ be the standard basis of $\mathbb{R}^3$, which is orthonormal relative to $< , >$. Imbed $\mathbb{H} \approx \mathbb{R}^4$ as a subalgebra of End $(\mathbb{H}) \approx$ End $(\mathbb{R}^4)$ by the map $a \to L_a$, where L_a denotes left multiplication by $a \in \mathbb{H}$. Let $\varphi : \mathbb{R}^3 \to \mathbb{H}$ be the linear map given by $\varphi(a) = a_1 I + a_2 J + a_3 K$ for $a = (a_1, a_2, a_3) \in \mathbb{R}^3$. If $j : \mathbb{R}^3 \to$ End $(\mathbb{H})$ is the map given by $j(a) = L_{\varphi(a)}$, then it follows routinely that $j(a)\, j(b) + j(b)\, j(a) = -2 < a, b >$ Id. Hence j extends to a representation of $C\ell(\mathbb{R}^3)$ on End $(\mathbb{H}) \approx$ End $(\mathbb{R}^4)$. It is easy to see that $j : \mathbb{R}^3 \oplus [\mathbb{R}^3, \mathbb{R}^3] \to$ End $(\mathbb{H})$ is not injective. For example, $j([e_1, e_2]) = j(e_1 e_2) = j(e_1)\, j(e_2) = L_I \circ L_J = L_K = j(e_3)$.□

Proof of Proposition 3

Lemma 1

Let $\{V, < , >\}$ be a finite dimensional real inner product space. Let $\varphi : \Lambda^2(V) \to$ *so*$(V , < , >)$ be the linear map such that $\varphi(a \wedge b)\,(v) = < a, v > b - < b, v > a$ for all $a,b,v \in V$. Then

1) φ is a linear isomorphism of vector spaces.

2) Let Lie algebra structures be defined on $\Lambda^2(V)$ by $[a \wedge b, c \wedge d] = - < b,c > a \wedge d + < b,d > a \wedge c + < a,d > c \wedge b - < a,c > d \wedge b$ for all $a,b,c,d \in V$ and on *so*$(V , < , >)$ by $[A, B] = AB - BA$ for all $A,B \in$ *so*$(V , < , >)$. Then φ is a Lie algebra isomorphism.

3) Let inner products be defined on Λ^2(V by $< a \wedge b,\ c \wedge d > = \det \begin{bmatrix} < a\ c > & < a\ d > \\ < b\ c > & < b\ d > \end{bmatrix}$ and on *so*$(V , < , >)$ by $< A, B > = -$ trace AB. Then

a) $< \varphi(x \wedge y)\, v, w > = < x \wedge y, v \wedge w >$ for all $x,y,v,w \in V$.

b) $< \varphi(\xi), \varphi(\eta) > = 2 < \xi, \eta >$ for all $\xi, \eta \in \Lambda^2(V)$

Remark

If $T : V \times V \to U$ is an alternating bilinear map for real vector spaces V, U, then there exists a linear map $\hat{T} : \Lambda^2(V) \to U$ such that $\hat{T}(v \wedge w) = T(v, w)$ for all $v,w \in V$. In particular, the map $T : V \times V \to$ *so*$(V , < , >)$ given by $T(a,b)\,(v) = < a,v > b - < b,v > a$ for $a,b, v \in V$ is alternating and bilinear, which guarantees the existence of the map $\hat{T} = \varphi: \Lambda^2(V) \to$ *so*$(V , < , >)$ of the Lemma.

Proof of Lemma 1

Let $\mathcal{B} = \{e_1, ... , e_n\}$ be an orthonormal basis of V. The map $\varphi : \Lambda^2(V) \to$

$\mathfrak{so}(V, \langle\ ,\ \rangle)$ is surjective since $\varphi(e_i \wedge e_j)$ is the element of $\mathfrak{so}(V, \langle\ ,\ \rangle)$ whose matrix relative to $\mathcal{B}$ has -1 in position (i,j), 1 in position (j,i) and zeros elsewhere. Therefore φ is a linear isomorphism since $\dim \Lambda^2(V) = \dim \mathfrak{so}(V, \langle\ ,\ \rangle) = (1/2)\, n(n-1)$. This proves 1). The assertions in 2) and 3) follow routinely from the definitions, and we omit the details.

The next result contains a proof of 1) of Proposition 3.

Lemma 2

Let $\{V, \langle\ ,\ \rangle\}$ be a finite dimensional real inner product space, and let $C\ell(V)$ denote the Clifford algebra determined by $\{V, \langle\ ,\ \rangle\}$. Let $V' = \mathbb{R} \oplus V \subseteq C\ell(V)$. Then

a) $[V, V]$ is a Lie subalgebra of $C\ell(V)$ isomorphic as a Lie algebra to $\Lambda^2(V)$. Moreover, $[V, V] = \mathbb{R}$–span $\{ab : a,b \in V\}$.

b) $[V, [V, V]] \subseteq V$.

c) $V \oplus [V, V]$ is a Lie subalgebra of $C\ell(V)$ isomorphic as a Lie algebra to $\Lambda^2(V')$.

d) $V \oplus [V, V]$ is isomorphic as a Lie algebra to $\mathfrak{so}(n+1)$, $n = \dim V$.

Proof of Lemma 2

Let $\mathcal{B} = \{e_1, \ldots , e_n\}$ be an orthonormal basis of V.

a) The vector space $[V, V]$ is spanned by $\{[e_i, e_j] = e_i e_j ,\ 1 \le i,j \le n\}$. The fact that $[V, V]$ is a Lie subalgebra of $C\ell(V)$ follows immediately from the next observation, whose proof is a routine consequence of (1) and (2) of section 1.

Sublemma

Let a,b,c and d be elements of V. Then $[ab, cd] = - \langle b, c \rangle ad + \langle b, d \rangle ac - \langle a, c \rangle db + \langle a, d \rangle cb$.

To identify $[V, V]$ with $\Lambda^2(V)$ we consider the alternating bilinear map $T : V \times V \to [V, V]$ given by $T(v,w) = [v, w]$ for all $v,w \in V$. Let $\hat{T} : \Lambda^2(V) \to [V, V]$ be the linear map such that $\hat{T}(v \wedge w) = [v, w]$ for all $v,w \in V$. The map $\hat{T}$ is surjective since $\hat{T}(e_i \wedge e_j) = [e_i, e_j]$ for $1 \le i,j \le n$. Hence $\hat{T}$ is a linear isomorphism since $\dim \Lambda^2(V) = \dim [V, V] = (1/2)\, n(n-1)$.

We show that $\hat{T}$ is a Lie algebra isomorphism, using the bracket operation for $\Lambda^2(V)$ defined in 2) of Lemma 1. Let a,b,c and d be any elements of V. By (1) and (2) of section 1 and the sublemma above we obtain $\hat{T}([a \wedge b, c \wedge d]) = - \langle b, c \rangle [a, d] + \langle b, d \rangle [a, c] + \langle a, d \rangle [c, b] - \langle a, c \rangle [d, b] = - \langle b, c \rangle ad + \langle b, d \rangle ac + \langle a, d \rangle cb - \langle a, c \rangle db = [ab + \langle a, b \rangle, cd + \langle c, d \rangle] = [\hat{T}(a \wedge b), \hat{T}(c \wedge d)]$.

The final assertion of a) is an immediate consequence of the fact that $[V, V] = \mathbb{R}$–span $\{[e_i, e_j] : 1 \le i,j \le n\} = \mathbb{R}$–span $\{e_i e_j : 1 \le i,j \le n\}$.

b) It suffices to show that $[e_i, [e_j, e_k]] \in V$ for all i,j,k with $j \neq k$. Since $[e_j, e_k] = e_j e_k$ if $j \neq k$ it follows from (1) of section 1 that $[e_i, [e_j, e_k]] = 0$ if i,j,k are all distinct and $[e_i, [e_i, e_k]] = -e_k$ if $i \neq k$.

c) It follows immediately from a) and b) that $V \oplus [V,V]$ is a Lie subalgebra of $C\ell(V)$. It remains to show that $V \oplus [V,V]$ is isomorphic to $\Lambda^2(V')$.

If we let $e_o = 1$, then $\{e_o, e_1, \ldots, e_n\}$ is a basis of $V' = \mathbb{R} \oplus V$. Since $\mathbb{R}$ is the center of $C\ell(V)$ it follows that $[V', V'] = [V, V]$ since $[(r,v), (s,w)] = [v, w]$ for all elements $(r,v), (s,w) \in \mathbb{R} \oplus V$. By the remark following lemma 1 there exists a linear map $\hat{S} : \Lambda^2(V') \to V \oplus [V, V]$ such that $\hat{S}((r, v) \wedge (s, w)) = (rw - sv) + [v, w]$ for all elements $(r,v), (s,w) \in V' = \mathbb{R} \oplus V$. Note that $\hat{S}$ is surjective ; Im $(\hat{S})$ contains $[V, V]$ since $\hat{S}(v \wedge w) = [v, w]$ for all $v,w \in V$, and Im $(\hat{S})$ contains V since $\hat{S}((r,0) \wedge (0, v)) = rv$ for all $r \in \mathbb{R}$ and $v \in V$. Therefore $\hat{S}$ is a linear isomorphism since $\dim \Lambda^2(V') = \dim (V \oplus [V, V]) = (1/2)\, n(n+1)$.

Equip $\Lambda^2(V')$ with the Lie bracket defined in 2) of Lemma 1. To show that $\hat{S} : \Lambda^2(V') \to V \oplus [V, V]$ is a Lie algebra isomorphism it suffices to show that $\hat{S}([e_i \wedge e_j, e_k \wedge e_\ell]) = [\hat{S}(e_i \wedge e_j), \hat{S}(e_k \wedge e_\ell)]$ for $0 \leq i,j,k,\ell \leq n$. The verification of this assertion follows routinely although tediously from the definitions of $\hat{S}$ and the bracket operation in $\Lambda^2(V')$.

d) This assertion follows immediately from c) and Lemma 1.

Proof of 2) of Proposition 3

If $n = 2$ or $n \geq 4$, then $V \oplus [V, V] \approx so(n+1)$ is a simple Lie algebra. By (4) of section 1, $\psi = (1/2)\, j : C\ell(V) \to \text{End}(V)$ is a Lie algebra homomorphism. If we restrict ψ and j to the Lie subalgebra $V \oplus [V, V]$, then Ker (j) = Ker $(\psi) = \{0\}$ since Ker (ψ) is an ideal of $V \oplus [V, V]$. Hence we obtain a Lie algebra isomorphism $\psi : V \oplus [V, V] \to \psi(V \oplus [V, V]) = \psi(V) \oplus [\psi(V), \psi(V)] = j(V) \oplus [j(V), j(V)]$. □

Proof of 3) of Proposition 3

If $n = 3$, then $V \oplus [V, V] \approx so(4)$ by d) of Lemma 2. It is known that $so(4) \approx so(3) \oplus so(3)$, and more precisely, $so(4)$ is the Lie algebra direct sum of its two simple ideals, both of which are isomorphic to $so(3)$ (cf. [H, Corollary 6.3, p.132]). Hence $j : V \oplus [V, V] \to \text{End}(U)$ is either injective or has nontrivial kernel isomorphic to $so(3)$.

To complete the proof of 3) it suffices to show that if Ker (j) is isomorphic to $so(3)$, then $j(V) = j([V, V]) = [j(V), j(V)] = j(V \oplus [V, V])$. It follows from (4) of section 1 and c) of Lemma 2 that $j(V \oplus [V, V])$ is a subalgebra of End (U).

We show first that $j : [V, V] \to \text{End}(U)$ is injective. It then follows that $j([V, V]) = [j(V), j(V)]$ has dimension 3 since $[V, V] \approx so(3)$ by Lemma 1 and a) of Lemma 2. Since $so(3)$ is simple it would follow that $j([V, V]) = \{0\}$ if j is not injective on [V, V], and hence

$[V, V] \subseteq \mathrm{Ker}(j)$, $j : V \oplus [V, V] \to \mathrm{End}(U)$. Equality must then hold since both $[V, V]$ and $\mathrm{Ker}(j)$ have dimension 3, but this would contradict the fact that $[V, V]$ is not an ideal of $V \oplus [V, V]$. Note, for example, that $[e_i, [e_i, e_j]] = [e_i, e_i e_j] = - e_j$ for $i \neq j$.

Next, we observe that $j(V) = j(V \oplus [V, V])$. Clearly $j(V) \subseteq j(V \oplus [V, V])$ and equality follows since both spaces have dimension 3. The space $j(V)$ has dimension 3 since $j : V \to \mathrm{End}(U)$ is injective by the definition of a representation of a Clifford algebra (cf. (3) of section 1). The space $j(V \oplus [V, V)$ has dimension 3 since $V \oplus [V, V] \approx \mathit{so}(4)$ has dimension 6, and $\mathrm{Ker}(j) \approx \mathit{so}(3)$ has dimension 3.

Finally, $[j(V), j(V)] = j([V, V]) \subseteq j(V \oplus [V, V]) = j(V)$, and equality holds since both $j(V)$ and $j([V, V])$ have dimension 3 by the discussion above.

Proof of 4) of Proposition 3

From (4) of Section 1 and b) of lemma 2 it follows immediately that $[j(V), [j(V), j(V)]] = j([V, [V, V]]) \subseteq j(V)$. By the discussion in section (2.2) of the main text there exists an inner product $< , >$ on U such that $j(V) \subseteq \mathit{so}(U, < , >)$.

We conclude by showing that if $n = 2$ or $n \geq 4$, then $j(V)$ and $([j(V), j(V)])$ are orthogonal in $\mathit{so}(U, < , >)$ relative to the inner product $<< , >>$ in $\mathit{so}(U, < , >)$ given by $<< A, B >> = - \mathrm{trace}(AB)$ for elements A, B of $\mathit{so}(U, < , >)$. We actually prove somewhat more than this. We treat only the case $n \geq 4$ and omit the proof for the simpler case $n = 2$.

Fix an orthonormal basis $\{e_1, e_2, \dots ,e_n\}$ for V, where $n \geq 4$, and let $E_i = j(e_i) \in \mathit{so}(U, < , >)$ for $1 \leq i \leq n$. The orthogonality of $j(V)$ and $j([V, V])$ follows from 2) of the next result.

Lemma

Let $\mathcal{B}_1 = \{E_i : 1 \leq i \leq n\}$, $\mathcal{B}_2 = \{E_i E_j : 1 \leq i < j \leq n\}$ and $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Then $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}$ are orthogonal bases of $j(V)$, $([j(V), j(V)])$ and $j(V) \oplus [j(V), j(V)]$ respectively relative to the inner product $<< , >>$ on $\mathit{so}(U, < , >)$. Moreover, $X^2 = - \mathrm{Id}$ and $<< X, X >> = n$ for every element X of $\mathcal{B}$.

Proof of the lemma

The lemma is an immediate consequence of the following assertions :

1) $<< E_i, E_j >> = n\, \delta_{ij}$ for $1 \leq i,j \leq n$.

2) $<< E_i, E_j E_k >> = 0$ for all $1 \leq i,j,k \leq n$.

3) a) $(E_i E_j)^2 = - \mathrm{Id}$ if $i \neq j$.

   b) $<< E_i E_j, E_k E_\ell >> = n$ if $i = k$ and $j = \ell$.

   c) $<< E_i E_j, E_k E_\ell >> = 0$ if $\{i,j\} \neq \{k,\ell\}$.

To prove these assertions we use repeatedly the facts

(*) $E_i^2 = -\,\mathrm{Id}$ for all i and $E_i E_j + E_j E_i = 0$ if $i \neq j$.

1) This assertion is an immediate consequence of the definition of $\langle\langle\ ,\ \rangle\rangle$, (*) and the fact that $E_i E_j$ is skew symmetric if $i \neq j$.

2) If $i = j$ or $i = k$, then $E_i E_j E_k = -E_k$ or E_j respectively by (*). Hence in this case $\langle\langle E_i, E_j E_k \rangle\rangle = -\,\mathrm{trace}\,(E_i E_j E_k) = 0$ since E_r is skew symmetric for all r.

We now assume that i,j and k are all distinct and define $T = E_i E_j E_k$. From (*) it is easy to verify the following :

a) If $\ell \notin \{i,j,k\}$, then $TE_\ell = -E_\ell T$.

b) T is symmetric relative to $\langle\ ,\ \rangle$ on U and $T^2 = \mathrm{Id}$.

From b) it follows that T has eigenvalues $\lambda = 1$ and -1 and $U = U_1 \oplus U_{-1}$, where U_1 denotes the eigenspace for $\lambda = 1$ and U_{-1} denotes the eigenspace for $\lambda = -1$. We need to show that trace (T) = 0, and since trace (T) = $\dim U_1 - \dim U_{-1}$ it suffices to show that $\dim U_1 = \dim U_{-1}$. Since $n \geq 4$ we can find an integer ℓ with $\ell \notin \{i,j,k\}$. From a) it follows that $E_\ell(U_1) = U_{-1}$ and $E_\ell(U_{-1}) = U_1$. Since E_ℓ is nonsingular we conclude that $\dim U_1 = \dim U_{-1}$.

3) Assertion b) follows from a) and the definition of $\langle\langle\ ,\ \rangle\rangle$. Assertion a) is an immediate consequence of (*). We prove c). If the integers i,j,k and ℓ are not all distinct, then $E_i E_j E_k E_\ell = E_r E_s$ for some integers r and s. Since $E_r E_s$ is skew symmetric it follows that $\langle\langle E_i E_j, E_k E_\ell \rangle\rangle = -\,\mathrm{trace}\,(E_i E_j E_k E_\ell) = 0$.

Suppose now that the integers i,j,k and ℓ are all distinct. Define $T = E_i E_j E_k$ and $S = E_i E_j E_k E_\ell = TE_\ell$. From a) and b) in the proof of 2) and (*) it is easy to show that $TS = -ST = E_\ell$, $S^2 = \mathrm{Id}$ and S is symmetric relative to $\langle\ ,\ \rangle$ on U. As in the proof of 2) we write $U = W_1 \oplus W_{-1}$, where W_1 denotes the S-eigenspace for $\lambda = 1$ and W_{-1} denotes the S-eigenspace for $\lambda = -1$. Since $TS = -ST$ it follows that $T(W_1) = W_{-1}$ and $T(W_{-1}) = W_1$. Therefore $\dim W_1 = \dim W_{-1}$ since T is nonsingular. We conclude that $\langle\langle E_i E_j, E_k E_\ell \rangle\rangle = -\,\mathrm{trace}\,(S) = -\{\dim W_1 - \dim W_{-1}\} = 0$ if the integers i,j,k and ℓ are all distinct. □

Appendix Two sided ideals in Clifford algebras

We begin by determining the centers of the Clifford algebras $C\ell(m)$.

Proposition 1

If $\mathfrak{Z}_m$ denotes the center of the Clifford algebra $C\ell(m)$, then one has the following:

1) If $m = 4k$, then $\mathfrak{Z}_m$ is a field isomorphic to $\mathbb{R}$.

2) If $m = 4k+1$, then $\mathfrak{Z}_m$ is a field isomorphic to $\mathbb{C}$.

3) If $m = 4k+2$, then $\mathfrak{Z}_m$ is a field isomorphic to $\mathbb{R}$.

4) If $m = 4k+3$, then $\mathfrak{Z}_m = \{a+bz : a,b \in \mathbb{R}\}$, where $z \in \mathfrak{Z}_m - \mathbb{R}$ is an element such that $z^2 = 1$. The element z is uniquely determined up to sign.

The main result may now be stated.

Proposition 2

1) If $m \neq 4k+3$, then $C\ell(m)$ contains no proper two sided ideals.

2) The algebra $C\ell(4k+3)$ contains exactly two proper two sided ideals A_1 and A_2 that are both isomorphic to $C\ell(4k+2)$. Moreover,

a) Let $z \in \mathfrak{Z}_m - \mathbb{R}$ an element such that $z^2 = 1$ and define $e = (1/2)(1-z)$ and $e' = (1/2)(1+z)$. Then $A_1 = e\, C\ell(4k+3)$ and $A_2 = e'\, C\ell(4k+3)$, relabeling if necessary.

b) $\alpha(A_2) = A_1$ and $\alpha(A_1) = A_2$, where α is the main involution of $C\ell(4k+3)$.

c) $C\ell(4k+3) = A_1 \oplus A_2$ and $A_1 A_2 = A_2 A_1 = \{0\}$.

A useful application of the main result is

Proposition 3

Let $m = 4k+3$ and let $\rho : C\ell(m) \rightarrow \mathrm{End}(U)$ be an irreducible representation on a finite dimensional real vector space. Let $\alpha : C\ell(m) \rightarrow C\ell(m)$ denote the involutive automorphism such that $\alpha(v) = -v$ for all $v \in \mathbb{R}^m$. Then

1) $\rho' = \rho \circ \alpha : C\ell(m) \rightarrow \mathrm{End}(U)$ is an irreducible representation that is not equivalent to ρ.

2) $C\ell(m) = \mathrm{Ker}(\rho) \oplus \mathrm{Ker}(\rho')$. Moreover, $\{\mathrm{Ker}(\rho), \mathrm{Ker}(\rho')\} = \{A_1, A_2\}$, where A_1 and A_2 are the two sided ideals of $C\ell(m)$ defined in Proposition 2.

Lemma 1a

If $C\ell(m)_{even}$ denotes the subalgebra of even elements of $C\ell(m)$, then $\mathfrak{Z}_m \cap C\ell(m)_{even} = \mathbb{R}$.

Proof

Let $\{e_1, e_2, \dots, e_m\}$ be an orthonormal basis of $\mathbb{R}^m$, and let $\mathfrak{B}$ be the corresponding basis of $C\ell(m)$; that is, $\mathfrak{B} = \{1, e_{i_1} e_{i_2} \dots e_{i_k}, 1 \leq i_1 < i_2 < \dots < i_k, 1 \leq k \leq m\}$. Let x be an element of $\mathfrak{Z}_m \cap C\ell(m)_{even}$ and write $x = \sum_{i=0}^{N} a_i \sigma_i$, where $a_i \in \mathbb{R}$, $\sigma_i \in \mathfrak{B}$, $\sigma_o = 1$ and σ_i is the product of an even number of the generators $\{e_1, e_2, \dots, e_m\}$ for all $i \geq 1$.

For an integer k with $1 \le k \le m$ we define $A_k = \{i : 1 \le i \le N$ and e_k is a factor of $\sigma_i\}$ and $B_k = \{i : 1 \le i \le N$ and e_k is not a factor of $\sigma_i\}$. It is easy to see, by induction on the number of factors of σ_i, that

$$e_k\, \sigma_i\, e_k^{-1} = -\,\sigma_i \qquad \text{if } i \in A_k$$
$$e_k\, \sigma_i\, e_k^{-1} = \sigma_i \qquad \text{if } i \in B_k$$

Hence $e_k\, x - x\, e_k = 2e_k(\sum_{i \in A_k} a_i\, \sigma_i)$ for all k. It follows that $e_k\, x = x\, e_k$ for all $k \Leftrightarrow a_k = 0$ for all $k \ge 1$. Hence $x = a_o \in \mathbb{R}$.□

Lemma 1b

Let $\{e_1, e_2, \ldots ,e_m\}$ be an orthonormal basis of $\mathbb{R}^m$, and let $z = e_1\, e_2 \ldots e_m$.

1) If $m = 4k$, then $z\, e_i = -\, e_i\, z$ for all i and $z^2 = 1$.

2) If $m = 4k+1$, then $z \in \mathfrak{Z}_m$ and $z^2 = -\,1$.

3) If $m = 4k+2$, then $z\, e_i = -\, e_i\, z$ for all i and $z^2 = -\,1$.

4) If $m = 4k+3$, then $z \in \mathfrak{Z}_m$ and $z^2 = 1$.

Proof

Note that $z \in \mathfrak{Z}_m \Leftrightarrow z\, e_i = e_i\, z$ for all i. The stated relations between $z\, e_i$ and $e_i\, z$ follow by induction on m if one writes $z = z'\, e_m$, where $z' = e_1\, e_2 \ldots e_{m-1}$. If one applies $m(m-1)/2 = (m-1) + (m-2) + \ldots + 1$ interchanges of the form $e_i\, e_j \to e_j\, e_i$ to the element z^2, then one obtains the element $e_1^{\,2}\, e_2^{\,2} \ldots e_m^{\,2} = (-1)^m$. Hence $z^2 = (-1)^{\{m+m(m-1)/2\}} = (-1)^{m(m+1)/2}$, and we obtain the stated values for z^2 in cases 1) through 4).□

Proof of Proposition 1

Let α be the main involution of $C\ell(m)$ defined by $\alpha(v) = -\,v$ for all $v \in \mathbb{R}^m$, and recall that $C\ell(m) = C\ell(m)_{even} \oplus v\, C\ell(m)_{even}$ for every nonzero element v of $\mathbb{R}^m$. Let ξ be an arbitrary element of $\mathfrak{Z}_m$, and write $\xi = a + b\, e_1$ for suitable elements a,b in $C\ell(m)_{even}$. Then $a = (1/2)\, \{\xi+\alpha(\xi)\} \in \mathfrak{Z}_m \cap C\ell(m)_{even} = \mathbb{R}$ by Lemma 1a, and furthermore $b\, e_1 = \xi - a \in \mathfrak{Z}_m$.

In cases 1) and 3) it suffices to prove that $b = 0$. If $z = e_1\, e_2 \ldots e_m$, then by Lemma 1b, $z\,(b\, e_1) = (b\, e_1)\, z = -b\,(z\, e_1)$, which implies that $zb = -\, bz$ since $e_1^{\,2} = -1$. However, Lemma 1b also implies that z commutes with even elements in cases 1) and 3), and hence $zb = bz$. It follows that $bz = 0$ and $b = 0$ since z is invertible.

We now consider cases 2) and 4) where m is odd. In this case, z is an odd element of $\mathfrak{Z}_m$, $\alpha(z) = -\, z$ and $C\ell(m) = C\ell(m)_{even} \oplus z\, C\ell(m)_{even}$. Clearly $\mathfrak{Z}_m \supseteq \{a + bz : a,b \in \mathbb{R}\}$, and we assert that equality holds. Let ξ be any element of $\mathfrak{Z}_m$, and and write $\xi = x + zy$, where x,y are elements of $C\ell(m)_{even}$. Then $x = (1/2)\, \{\xi+\alpha(\xi)\}$ and

$y = \pm(1/2)\{\alpha(\xi) - \xi\}z$ are elements of $\mathfrak{Z}_m \cap C\ell(m)_{even} = \mathbb{R}$ by Lemma 1a, which proves that $\xi \in \{a + bz : a,b \in \mathbb{R}\}$.

In case 2) it is easy to see that $\mathfrak{Z}_m = \{a + bz : a,b \in \mathbb{R}\}$ is a field isomorphic to $\mathbb{C}$ since $z^2 = -1$ by Lemma 1b. In case 4) it is also easy to see that $\mathfrak{Z}_m = \{a + bz : a,b \in \mathbb{R}\}$ is not a field since $z^2 = 1$, which implies that (1-z) and (1+z) are nonzero central elements whose product is zero. In case 4) it is also easy to check that if ξ is any element of $\mathfrak{Z}_m - \mathbb{R}$ such that $\xi^2 = 1$, then $\xi = z$ or $\xi = -z$.□

Proof of Proposition 2

The map $L : C\ell(m) \to End_{\mathbb{R}}(C\ell(m))$ given by L(x) = left multiplication by x is a representation of $C\ell(m)$. All representations $\rho : C\ell(m) \to End(U)$ are completely reducible since $\rho(C\ell(m)) \subseteq so(U, < , >)$ for a suitable inner product < , > on U. Hence we may write $C\ell(m) = L_1 \oplus L_2 \oplus ... \oplus L_N$, where the $\{L_i\}$ are irreducible $C\ell(m)$ - submodules or equivalently , left ideals of $C\ell(m)$ that contain no proper left ideals of $C\ell(m)$. Hence $C\ell(m)$ is a semisimple ring, and by standard theory (cf. Theorems 2 and 4 of [L, pp.447-448]) we can write $C\ell(m) = R_1 \oplus R_2 \oplus ... \oplus R_p$, where each R_i is a ring with no proper two sided ideal and $R_i R_j = R_j R_i = 0$ if $i \neq j$. The number p and the factors $\{R_1, R_2, ... , R_p\}$ are uniquely determined up to isomorphism and order. Note that if we write $1 = e_1 + e_2 + ... + e_p$, then each e_i is a central element of $C\ell(m)$ such that $e_i^2 = e_i$ and $e_i e_j = e_j e_i = 0$ if $i \neq j$. If $p \geq 2$, then the center of $C\ell(m)$ would not be a field, and it follows that p = 1 if $m \neq 4k+3$ by Proposition 1.

We prove 2). Let m = 4k+3. By the discussion above the center $\mathfrak{Z}_m$ contains the p-dimensional subspace spanned by $\{e_1, e_2, ... , e_p\}$. Hence p = 1 or 2 by 4) of Proposition 1. We show that p = 2.

By 4) of Proposition 1 there exists an element $z \in \mathfrak{Z}_m - \mathbb{R}$ such that $z^2 = 1$. Define e = (1/2)(1-z) and e' = (1/2)(1+z). The elements e and e' are nonzero and central, and they satisfy the properties $e^2 = e$, $e'^2 = e'$, 1 = e + e' and ee' = e'e = 0. If $B_1 = e\, C\ell(4k+3)$ and $B_2 = e'\, C\ell(4k+3)$, then B_1 and B_2 are two sided ideals of $C\ell(4k+3)$ since the elements e and e' are central. Moreover $C\ell(4k+3) = B_1 \oplus B_2$ since 1 = e + e'. Hence p = 2 and $R_i = B_i$ for i = 1, 2, using the notation above.

To prove a) it suffices to show that B_1 and B_2 are the only proper two sided ideals of $C\ell(m)$. If B is a two sided ideal of $C\ell(m)$, then $B \cdot B_i \subseteq B \cap B_i$ for i = 1,2, and hence $B \cdot B_i$ is a nonzero ideal of B_i if $B \cdot B_i \neq 0$. Since $B_1 = R_1$ and $B_2 = R_2$ contain no proper two sided ideals it follows that $B \cdot B_i \supseteq B_i$ if $B \cdot B_i \neq 0$, and we conclude that $B = B_1$ or $B = B_2$ if B is proper.

Assertion 2c) follows from a) and the properties of e and e' listed above. Now let α be the main involution of $C\ell(4k+3)$, which has the property that $\alpha v = -v$ for all v in

$\mathbb{R}^m$. It follows that $\alpha(z) = -z$ by the definition of z in Lemma 1b and the fact that m is odd. Hence $\alpha(e) = e'$ and $\alpha(e') = e$, which proves 2b).

To complete the proof of Proposition 2 it remains only to prove that both A_1 and A_2 are isomorphic as algebras to $C\ell(4k+2)$. Define $\varphi : \mathbb{R}^{4k+2} \to A_1$ by $\varphi(v) = ev$ for all $v \in \mathbb{R}^{4k+2} = \{v = (v_1, v_2, \ldots, v_{4k+3}) \in \mathbb{R}^{4k+3} : v_{4k+3} = 0\}$. Note that A_1 is an associative algebra with unit e. Moreover, φ is an $\mathbb{R}$-linear map such that $\varphi(v)\cdot\varphi(v) = ev^2 = -|v|^2 e$ for all $v \in \mathbb{R}^{4k+2}$. Hence φ extends uniquely to an $\mathbb{R}$-algebra homomorphism $\varphi : C\ell(4k+2) \to A_1$ by the universal mapping property of Clifford algebras. Since $z = e_1 e_2 \ldots e_{4k+3}$ by lemma 1b it follows that $-ze_{4k+3} = e_1 e_2 \ldots e_{4k+2}$. Since $ez = -e$ it follows that $e\,e_{4k+3} = e(-z)e_{4k+3} = (e\,e_1)(e\,e_2) \ldots (e\,e_{4k+2}) \in \varphi(C\ell(4k+2))$. We conclude that $\varphi : C\ell(4k+2) \to A_1$ is surjective since $\varphi(C\ell(4k+2))$ contains the algebra generators $\{(e\,e_1), (e\,e_2), \ldots (e\,e_{4k+3})\}$ of A_1. It follows that φ is an algebra isomorphism since $C\ell(4k+2)$ and A_1 both have dimension 2^{4k+2} over $\mathbb{R}$. By 2b) $A_2 = \alpha(A_1)$ is isomorphic to A_1 and hence also to $C\ell(4k+2)$. This completes the proof of Proposition 2. □

Before proving Proposition 3 we need a preliminary result.

Lemma 3

Let $m = 4k+3$ and let $\rho : C\ell(m) \to \mathrm{End}(U)$ be an irreducible representation on a finite dimensional real vector space. Let $\{e_1, e_2, \ldots e_m\}$ be an orthonormal basis of $\mathbb{R}^m$, and let $z = e_1 \cdot e_2 \cdot \ldots \cdot e_m$. Then either $\rho(z) = \mathrm{Id}$ or $\rho(z) = -\mathrm{Id}$.

Proof of Lemma 3

By Lemma 1 , $\rho(z)^2 = \rho(z^2) = \mathrm{Id}$, and hence $U = U_1 \oplus U_{-1}$, where $U_1 = \{u \in U : \rho(z)u = u\}$ and $U_{-1} = \{u \in U : \rho(z)u = -u\}$. Since z is central by case 4) of lemma 1b , $\rho(z)$ commutes with $\rho(C\ell(m))$, and hence $\rho(C\ell(m))$ leaves invariant both U_1 and U_{-1}. It follows that either $U = U_1$ or $U = U_{-1}$ by the irreducibility of ρ. □

Proof of Proposition 3

1) Let $\{e_1, e_2, \ldots e_m\}$ be an orthonormal basis of $\mathbb{R}^m$. Since $\alpha(e_i) = -e_i$ for all i and $\alpha(z) = -z$ it follows that $\rho'(e_i) = -\rho(e_i)$ for all i and $\rho'(z) = -\rho(z)$. Hence ρ' is also an irreducible representation of $C\ell(m)$ on U since any subspace W invariant under $\{\rho'(e_1), \rho'(e_2), \ldots\rho'(e_m)\}$ is also invariant under $\{\rho(e_1), \rho(e_2), \ldots\rho(e_m)\}$. By lemma 3 either a) $\rho(z) = \mathrm{Id}$ and $\rho'(z) = -\mathrm{Id}$ or b) $\rho(z) = -\mathrm{Id}$ and $\rho'(z) = \mathrm{Id}$. Recall that $e = (1/2)(1-z)$ and $e' = (1/2)(1+z)$. If a) holds, then Ker (ρ) contains e but not e', and Ker (ρ') contains e' but not e. Hence Ker $(\rho) \neq$ Ker (ρ'). A similar argument shows that Ker $(\rho) \neq$ Ker (ρ') in case b). If there existed an invertible linear map $T : U \to U$ such that $T \circ \rho(\xi) = \rho'(\xi) \circ T$ for all elements ξ of $C\ell(m)$, then it would follow that Ker (ρ) = Ker (ρ'). Hence ρ and ρ' are inequivalent representations of $C\ell(m)$ on U when $m = 4k+3$.

2) Recall that A_1 and A_2 are the only proper two sided ideals of $C\ell(4k+3)$ by the proof of 2a) of Proposition 2. Clearly Ker (ρ) and Ker (ρ') are proper two sided ideals of $C\ell(4k+3)$ that are distinct by 1). Hence assertion 2) of Proposition 3 now follows immediately from assertions 2a) and 2c) of Proposition 2. □

References

[FH] W. Fulton and J. Harris, Representation Theory, a First Course, Springer, 1991, New York.

[H] S. Helgason, Differential Geometry, Lie Groups and Symmetric Spaces, Academic Press, 1978, New York.

[J] N. Jacobson, Lectures in Abstract Algebra, vol. II, Van Nostrand, 1953, New York.

[L] S. Lang, Algebra, Addison-Wesley, 1965, Reading.

[LM] H. B. Lawson and M.-L. Michelsohn, Spin Geometry, Princeton University Press, 1989, Princeton.

[S1] D. Shapiro, " Products of sums of squares ", Expo. Math. 2 (1984), 235-261.

[S2] -------, private communications.