Commentationes Mathematicae Universitatis Carolinae

Jimmie Lawson

Clifford algebras, Möbius transformations, Vahlen matrices, and B-loops

Commentationes Mathematicae Universitatis Carolinae, Vol. 51 (2010), No. 2, 319--331

Persistent URL: http://dml.cz/dmlcz/140109

Comment.Math.Univ.Carolin. 51,2 (2010) 319–347

Clifford algebras, Möbius transformations, Vahlen matrices, and B-loops

Jimmie Lawson

Abstract. In this paper we show that well-known relationships connecting the Clifford algebra on negative euclidean space, Vahlen matrices, and Möbius transformations extend to connections with the Möbius loop or gyrogroup on the open unit ball B in n-dimensional euclidean space $\mathbb{R}^n$. One notable achievement is a compact, convenient formula for the Möbius loop operation $a * b = (a+b)(1-ab)^{-1}$, where the operations on the right are those arising from the Clifford algebra (a formula comparable to $(w+z)(1+\overline{w}z)^{-1}$ for the Möbius loop multiplication in the unit complex disk).

Keywords: Bruck loop, Clifford algebra, gyrogroup, Möbius transformations, Vahlen matrices, involutive group

Classification: 20N05, 51B10, 15A66

1. Introduction

There is a standard Möbius addition on the complex unit disk given by

$$w \oplus z = \frac{w+z}{1+\overline{w}z}$$

giving it the structure of a uniquely 2-divisible Bruck loop, or (in the gyrogroup language) a uniquely 2-divisible gyrocommutative gyrogroup. This generalizes to a loop resp. gyrogroup structure on the unit open ball of $\mathbb{R}^n$, which A. Ungar has studied in some detail [11].

There is an approach to Möbius geometry via the Clifford algebra of negative euclidean space and Vahlen matrices (which induce Möbius transformations as "fractional transformations"). Via this approach the general Möbius geometry exhibits rather striking analogies to the Möbius geometry of the extended complex plane via fractional transformations. The goal of this paper is to embed the Möbius loop on the unit ball of euclidean space into this framework. Again the Möbius loop has notable analogies to the basic one on the unit ball of the complex plane, in particular with respect to the basic formula we derive for the Möbius loop operation.

Much of the paper consists of quick summaries of the theory and results that we need concerning Clifford algebras, Vahlen matrices, Möbius geometry, involutive groups, and, of course, loop theory. In this sense most of the material is not original. The originality comes from the bringing together of the various threads to recast the Möbius loop in the framework of Clifford algebras.

2. Clifford algebras

We recall some basic facts about Clifford algebras. We consider the category of algebras (= associative algebras with a multiplicative identity 1) over a fixed field $\mathbb{F}$, always assumed not to be of characteristic 2, with morphisms identity preserving algebra homomorphisms.

Definition 2.1. Let V be a vector space over $\mathbb{F}$ equipped with a nondegenerate symmetric bilinear form $Q : V \times V \to \mathbb{F}$. The algebra $\mathcal{C}_Q$ is a *Clifford algebra* for (V, Q) if

(1) it contains V and $\mathbb{F} = \mathbb{F} \cdot 1$ as distinct subspaces;
(2) (the Clifford condition) for all $x, y \in V \subseteq \mathcal{C}_Q$, $xy + yx = 2Q(x, y)$;
(3) V generates $\mathcal{C}_Q$ as an algebra over $\mathbb{F}$;
(4) $\mathcal{C}_Q$ is the universal algebra over V (or $\mathcal{C}_Q$ is freely generated by V) subject to the relations $xy + yx = 2Q(x, y)$.

A linear map $\phi : V \to A$, A an algebra, is called a *Clifford map* if it *preserves the form* Q, i.e., if for all $x, y \in V$, $\phi(x)\phi(y) + \phi(y)\phi(x) = 2Q(x, y) \cdot 1_A$. In more detail, the universal property (4) means that given any Clifford map $\phi : V \to A$, there exists a unique algebra morphism $\tilde{\phi} : \mathcal{C}_Q \to A$ that extends ϕ.

Note in particular in $\mathcal{C}_Q$ that $x^2 = Q(x)$, where $Q(x) := Q(x, x)$ is the associated quadratic form. The members of V viewed as members of the larger $\mathcal{C}_Q$ are called *vectors*. Note also that by considering the reverse operation on any algebra A, any Clifford map from $V \to A$ can also be uniquely extended to an antihomomorphism from $\mathcal{C}_Q$ to A.

For any Clifford algebra, there are three basic involutions, one an automorphism and the other two antiautormorphisms. The linear map on V defined by $x \mapsto -x$ preserves the quadratic form Q and so by the universal property of Clifford algebras extends uniquely to an involutive algebra automorphism on C_Q called the *grade involution* and denoted by $x \mapsto \hat{x}$, and also extends uniquely to an involutive antiautomorphism on C_Q, called *Clifford conjugation* and denoted $x \mapsto \overline{x}$. The identity map on V also extends uniquely to an involutive antiautomorphism on C_Q, denoted $x \mapsto x^*$. Since for products of vectors, $(x_1 \cdots x_n)^* = x_n \cdots x_1$, this involution is called *reversion*. Since $\hat{v}^* = \overline{v}$ for $v \in V$ and V generates C_Q, it follows that $\hat{x}^* = \overline{x}$ for all $x \in C_Q$.

2.1 Bases and dimension. If the dimension of V is n and $\{e_1, \ldots, e_n\}$ is a basis of V, then the set

$$\{e_I := e_{i_1} e_{i_2} \cdots e_{i_k} : 1 \le i_1 < \ldots < i_k \le n,\ I{=}\{i_1, \ldots, i_k\}{\subseteq}\{1, \ldots, n\},\ 0 \le k \le n\}$$

is a basis for $\mathcal{C}_Q$. The empty product ($k = 0$) is defined as the multiplicative identity element, $e_\emptyset = 1$. Since V comes equipped with a nondegenerate symmetric bilinear form, the basis for V may be chosen to be an orthogonal basis, one consisting of orthogonal vectors. The fundamental Clifford identity implies that for an orthogonal basis $e_i e_j = -e_j e_i$ for $i \neq j$ which simplifies manipulation of orthogonal basis vectors. Given a product of distinct orthogonal basis vectors, one can put them into standard increasing ordering by including an overall sign corresponding to the number of flips needed to correctly order them (i.e. the signature of the ordering permutation). For each value of k there are $\binom{n}{k}$ basis elements spanning the *subspace of grade* k members of $\mathcal{C}_Q$, so the total dimension of $\mathcal{C}_Q$ is 2^n. The subspace of grade k is independent of the orthogonal base chosen and gives a $\mathbb{Z}$-grading of $\mathcal{C}_Q$ (as a vector space, not an algebra), with nonzero values for grades 0 through n. The grade 0 subspace is equal to $\mathbb{F}$, the grade 1 subspace is V, the vectors, and the elements of grade 2 are called bivectors. The sum of the subspaces of even grade form a subalgebra of $\mathcal{C}_Q$.

One can easily extend the quadratic form Q on V to a quadratic form on all of $\mathcal{C}_Q$ by choosing an orthogonal basis of V and requiring that distinct elements of the corresponding basis of $\mathcal{C}_Q$ are orthogonal to one another and that $Q(e_I) = Q(e_{i_1} e_{i_2} \cdots e_{i_k}) = Q(e_{i_1})Q(e_{i_2}) \cdots Q(e_{i_k})$. We then have

$$\begin{aligned} Q(a) &= Q(\sum_I a_I e_I) = \sum_I a_I^2 Q(e_I) \quad \text{for} \quad a = \sum_I a_I e_I \in \mathcal{C}_Q, \\ 2\langle a, b\rangle &= Q(a+b) - Q(a) - Q(b) \quad \text{for} \quad a, b \in \mathcal{C}_Q. \end{aligned}$$

The quadratic form defined in this way is actually independent of the orthogonal basis chosen. One can show

$$Q(v_1 v_2 \cdots v_k) = Q(v_1)Q(v_2)\cdots Q(v_k) \quad \text{for} \quad v_1, \ldots, v_k \in V, \tag{2.1}$$

an identity which is not valid for arbitrary elements of $\mathcal{C}_Q$. We also note that each of the three basic involutions multiplies each of the basis element e_I by ± 1, and hence each of them preserves Q and the bilinear form.

2.2 The Clifford group. We continue the assumption that $\dim(V) = n$. We note that an element $x \in V$ is invertible in $\mathcal{C}_Q$ if and only if $Q(x) \neq 0$. In the latter case, one deduces from $xx = Q(x)$ that $x^{-1} = (1/Q(x))x$. The *Clifford group* Γ_Q of $\mathcal{C}_Q$, also called the *Lipschitz group* since it was first considered by Lipschitz, is the subgroup of invertible elements consisting of products of invertible elements of V. It has an alternative characterization as

$$\Gamma_Q = \{s \in \mathcal{C}_Q : sx\hat{s}^{-1} \in V \quad \text{for all} \quad x \in V\}.$$

The action $s.x = sx\hat{s}^{-1}$ defines a linear action, called *twisted conjugation* of Γ_Q not only on V, but on the entire Clifford algebra $\mathcal{C}_Q$ (although twisted conjugation is not an algebra automorphism). When restricting twisted conjugation to V, we have, using the fact that the grade involution preserves Q and equation (2.1),

$$Q(sx\hat{s}^{-1}) = Q(s)Q(x)Q(\widehat{s^{-1}}) = Q(x)Q(s)Q(s^{-1}) = Q(x)Q(1 = ss^{-1}) = Q(x).$$

Thus twisted conjugation preserves Q, and so gives a homomorphism from the Clifford group to the orthogonal group preserving Q. The Clifford group contains all elements s of V of nonzero norm, and these act on V by the corresponding reflections that take v to $sv(-s)^{-1} = v - 2Q(v,s)s/Q(s)$.

Writing $s \in \Gamma_Q$ as a product $v_1 \cdots v_k$ of invertible members of V, we have from equation (2.1) that

$$ss^* = (v_1 \cdots v_k)(v_k \cdots v_1) = \prod_{i=1}^{k} Q(v_i) = Q(s) \in \mathbb{F},$$

and thus that $s^{-1} = (1/Q(s))s^*$. Similarly $s^*s = Q(s)$, so $ss^* = s^*s$. The *pin group* Pin_Q is a subgroup of Γ_Q consisting of those $s \in \Gamma_Q$ that can be written as finite products of vectors $s = v_1 \cdots v_k$ where $Q(v_i) = \pm 1$ for $1 \leq i \leq k$. Members of the *spin group* Spin_Q can be characterized as being written as such products where the number of factors is even, i.e., Spin_Q is the intersection of Pin_Q and the subalgebra of even elements. Since for $c, d, x \in V$,

$$cdx\hat{d}^{-1}\hat{c}^{-1} = cdx(-d^{-1})(-c^{-1}) = cdxd^{-1}c^{-1},$$

we conclude that for members of Spin_Q acting by twisted conjugation is equal to acting by conjugation, and that the action is the composition of an even number of twisted conjugations, which are equal to reflections, by members of V. It follows that members of Spin_Q acting by conjugation on V give rise to members of the special orthogonal group $\mathrm{SO}(Q)$.

2.3 Negative euclidean space. Our primary interest is in the Clifford algebra $\mathcal{C}_n$ for negative euclidean space: $\mathbb{R}^n$ equipped with the bilinear form $Q(x,y) = -\langle x, y\rangle$, where $\langle \cdot, \cdot \rangle$ is the usual euclidean inner product. If one chooses an orthonormal basis $\{e_1, \ldots, e_n\}$, one has in addition to the usual $e_ie_j = -e_je_i$ for $i \neq j$ that $e_ie_i = -\langle e_i, e_i\rangle = -1$. More generally for $v \in V$, we have $v^2 = -\langle v, v\rangle = -|v|^2$, and so $v^{-1} = -v/|v|^2 = \overline{v}/|v|^2$ for $v \neq 0$.

We list some elementary useful properties related of $\mathcal{C}_n$. Proofs may be found in [1] and [13], but in many cases reduce to general facts about Q stated previously.

Proposition 2.2. *Let $a, b \in \mathcal{C}_n$.*

(i) *If $a \in \Gamma_n$ or $b \in \Gamma_n$, then $|ab| = |a|\,|b|$.*
(ii) *If $a \in \Gamma_n$, then $|a|^2 = a\overline{a} = \overline{a}a$.*
(iii) *If $a \in \mathrm{Spin}_n$, i.e., is a product of an even number of non-zero vectors, then the conjugation map $I_a : \mathbb{R}^n \to \mathbb{R}^n$ given by $I_a(v) = ava^{-1}$ is in $\mathrm{SO}(n, \mathbb{R})$.*

Assertion (iii) follows from the remarks of the preceding subsection since a linear map of $\mathbb{R}^n$ preserves Q if and only if it preserves $\langle \cdot, \cdot \rangle$, and thus $\mathrm{SO}(Q) = \mathrm{SO}(n, \mathbb{R})$.

Remark 2.3. For $a, b \in \mathbb{R}^n$, $a \neq 0$, $ab \neq 1$,

$$k := 1 - ab = -\frac{a}{|a|^2}(a + |a|^2 b)$$

is the product of two nonzero members of V and hence the inner automorphism $x \mapsto kxk^{-1}$ is a rotation of $\mathbb{R}^n$.

3. Möbius transformations and Vahlen matrices

Möbius transformations of $\mathbb{R}^n$ are important for a variety of reasons, one being that they are precisely the conformal maps.

Definition 3.1. Let $\hat{\mathbb{R}}^n$ denote $\mathbb{R}^n$ with a point attached at infinity. The *Möbius transformations* of $\mathbb{R}^n$ consist of all Möbius transformations on $\hat{\mathbb{R}}^n$, that is, the group of transformations (under composition) generated by rigid motions, scalar multiplication by positive scalars, and inversion through spheres, where rigid motions and scalar multiplication leave the point at infinity fixed and inversion through a sphere carries the center of the sphere and the point at infinity to each other.

3.1 Möbius transformations of the unit ball. We consider the subgroup $G(B)$ consisting of all Möbius transformations that carry the open unit ball $B := \{x \in \mathbb{R}^n : |x| < 1\}$ onto itself. These include of course all members of the orthogonal group. It is known that $G(B)$ can be generated by $\mathrm{O}(n, \mathbb{R})$ and a special class of Möbius transformations called *Möbius translations*. These have a compact and straightforward description by means of the Clifford algebra $\mathcal{C}_n$. For $a \in B$, we define the Möbius translation τ_a by a by the rule

$$\tau_a(x) = (x + a)(-ax + 1)^{-1}.$$

We calculate in $\mathcal{C}_n$ for $a, b \in B$:

$$\begin{aligned} \tau_a(b) &= (a + b)(1 - ab)^{-1} \\ &= (a + b)(1 - ba)(1 - ba)^{-1}(1 - ab)^{-1} \\ &= (a + b)(1 - ba)\big((1 - ab)(1 - ba)\big)^{-1}. \end{aligned}$$

Multiplying the first two factors, we obtain

$$\begin{aligned} (a + b)(1 - ba) &= a + b - aba + |b|^2 a \\ &= a + b - a(-ab - 2\langle a, b\rangle) + |b|^2 a \\ &= a + b - |a|^2 b + 2\langle a, b\rangle a + |b|^2 a \\ &= (1 + 2\langle a, b\rangle + |b|^2)a + (1 - |a|^2)b. \end{aligned}$$

Multiplying the second two factors (without the inverse), we obtain

$$\begin{aligned} (1 - ab)(1 - ba) &= 1 - ab - ba + |a|^2|b|^2 \\ &= 1 + 2\langle a, b\rangle + |a|^2|b|^2. \end{aligned}$$

Since the last line is a scalar, we have

$$\tau_a(b) = \frac{(1+2\langle a,b\rangle + |b|^2)a + (1-|a|^2)b}{1+2\langle a,b\rangle + |a|^2|b|^2}. \tag{3.2}$$

Note that equation (3.2) agrees with the known euclidean space formulation for Möbius translations (see, for example, [11, Section 3.5]), and is a Möbius transformation that carries B to B for $a \in B$.

3.2 Vahlen matrices. Members of Γ_n may be used to define the Vahlen matrices, which form a group under matrix multiplication [12], [1].

Definition 3.2. A matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is called a *Vahlen matrix* if

(i) $a, b, c, d \in \Gamma_n \cup \{0\}$;
(ii) $ab^*, cd^*, c^*a, d^*b \in \mathbb{R}^n$;
(iii) the pseudodeterminant $\Delta := ad^* - bc^*$ is real and nonzero.

The *Vahlen matrix group* is the group of all Vahlen matrices under matrix multiplication.

The following theorem connects Vahlen matrices with Möbius transformations [12], [1], [13].

Theorem 3.3. *A matrix $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with entries from $\mathcal{C}_n$ induces a bijective map $\Phi_M(x) := (ax+b)(cx+d)^{-1}$ on $\hat{\mathbb{R}}^n$ that is a Möbius transformation if and only if M is a Vahlen matrix. The map $M \mapsto \Phi_M$ is a surjective homomorphism from the Vahlen group to the group of Möbius transformations, and has kernel the group of scalar matrices $\left[\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right]$, $\lambda \in \mathbb{R}\setminus\{0\}$. Hence two Vahlen matrices induce the same Möbius transformation if and only if one is a nonzero scalar multiple of the other.*

Observe that the Vahlen matrix $\left[\begin{smallmatrix} 1 & a \\ -a & 1 \end{smallmatrix}\right]$ induces the Möbius translation $\tau_a(x) = (x+a)(1-ax)^{-1}$ and that

$$\begin{bmatrix} 1 & a \\ -a & 1 \end{bmatrix} \begin{bmatrix} 1 & -a \\ a & 1 \end{bmatrix} = \begin{bmatrix} 1+|a|^2 & 0 \\ 0 & 1+|a|^2 \end{bmatrix}.$$

The Vahlen matrix on the right induces the identity map on $\hat{\mathbb{R}}^n$, since it is a scalar times the identity (see Theorem 3.3). Since composition of Möbius maps corresponds with multiplication of the inducing Vahlen matrices, we conclude that $\tau_a \circ \tau_{-a}$ is the identity map, i.e., $\tau_{-a} = (\tau_a)^{-1}$.

Let $g \in G(B)$, set $a = g(0) \in B$. Then $\tau_{-a}g$ is a Möbius transformation preserving B and carrying 0 to 0, hence by a standard result of Möbius geometry it is an orthogonal map θ. Hence $g = \tau_a(\tau_{-a}g) = \tau_a\theta$, and we conclude that every Möbius transformation preserving B can be factored into factors of a Möbius translation and an orthogonal map.

4. Twisted subgroups, involutive groups, and B-loops

In this section we cover more-or-less familiar ground to loop theorists, but it is perhaps worthwhile to quickly review it in a context that applies to the current setting.

4.1 B-loops. We recall certain basic definitions and elementary properties from loop theory. A pair $(B,*)$ consisting of a set B and a binary operation $*$ is a *loop* if it has an identity and the equations $a*x=b$ and $y*a=b$ have unique solutions in B for all $a,b\in B$. A *left Bol loop* is a loop satisfying the Bol-identity (I), and a *Bruck loop* or K*-loop* is a left Bol loop satisfying item (II):

(I) (Bol-identity) $x\circ(y\circ(x\circ z))=(x\circ(y\circ x))\circ z$,

(II) (Automorphic inverse property) $(a\circ b)^{-1}=a^{-1}\circ b^{-1}$.

An equivalent definition of a Bruck loop is to replace item (II) by the following [6, Theorem 6.8]:

(II′) $(a\circ b)\circ(a\circ b)=a\circ((b\circ b)\circ a)$.

It is a standard result that a K-loop (indeed a left Bol loop) is power associative (integer powers of any element associate) and every element has a unique two-sided inverse (indeed, this in necessary for (II) to make sense), which together imply that every element is contained in a cyclic subgroup. Furthermore, a K-loop is *left power alternative*: $x^m\circ(x^n\circ y)=x^{m+n}\circ y$ for all integers m,n. The K-loop is *uniquely* 2*-divisible* if every element has a unique square root. Such loops are sometimes referred to as B*-loops*, a terminology we adopt. Alternatively, B-loops are 2-divisible K-loops with no elements of order 2 ([5] or [9]).

The term B-loop arose in the work of Glaubermann ([3] and [4]). He studied Bruck loops that were finite of odd order. Since each cyclic subgroup $\langle x\rangle$ partitions the Bruck loop in cosets $\langle x\rangle\circ y$ of equal cardinality, one has a Lagrange theorem for cyclic subgroups. Therefore each cyclic subgroup has odd order and hence is uniquely 2-divisible.

4.2 Twisted subgroups. Recall that a subset X of a group G is a *twisted subgroup* if $e\in G$ and $x,y\in G$ implies $x^{-1},xyx\in G$. The twisted subgroup X is *uniquely* 2*-divisible* if every element of X has a unique square root in X. The following result may be found in [10, 3.9] or [6, Theorem 6.14]. For a converse, namely that every B-loop arises in such a manner, see [6, Theorem 6.15].

Proposition 4.1. *A uniquely 2-divisible twisted subgroup X of a group G is a B-loop with respect to the operation $a\otimes b=a^{1/2}ba^{1/2}$. Furthermore, integer powers of elements in X formed in G and in $(X,\otimes)$ agree.*

Corollary 4.2. *A uniquely 2-divisible twisted subgroup X of a group G is a B-loop with respect to the operation $a*b=(ab^2a)^{1/2}$.*

PROOF: The algebraic systems $(X,*)$ and $(X,\odot)$ are isomorphic, the isomorphism being given by $D:(P,*)\to(P,\odot)$, $D(x)=x^2$:

$$D(a*b)=D((ab^2a)^{1/2})=ab^2a=a^2\odot b^2=D(a)\odot D(b).$$

The bijectiveness follows from the unique 2-divisibility of the twisted subgroup X. Thus $(X, *)$ is a B-loop, since it is isomorphic to one. $\square$

4.3 Involutive groups. We turn now to the setting of an involutive group G, a group equipped with an involutive automorphism τ. We set $g^* = \tau(g^{-1}) = (\tau(g))^{-1}$ and note that $g \mapsto g^* : G \to G$ is an involutive antiautomorphism. Let

$$G^\tau := \{x \in G : \tau(x) = x\}, \qquad P_G := \{xx^* : x \in G\} \subseteq G_\tau := \{g \in G : g = g^*\}.$$

(That $(xx^*)^* = x^{**}x^* = xx^*$ shows $P_G \subseteq G_\tau$.)

We recall some basic terminology. Let G be a group with subgroup H. A subset L of G is said to be a *transversal of* G/H or *transversal to* H if the identity $e \in L$ and L intersects each coset gH of H in precisely one point. Thus the map $g \mapsto gH : G \to G/H$ has a cross-section, namely the map that picks the member of L out of each coset. One sees readily that a subset L containing e is a transversal to H if and only if the map $(x, h) \mapsto xh$ from $L \times H$ to G is a bijection. In the case of an involutive group (G, τ), if $L \subseteq \{g \in G : g = g^*\}$, then the map $(x, k) \mapsto xk : L \times G^\tau \to G$ is called a *polar map*. Hence $e \in L \subseteq G_\tau$ is transversal to G^τ if and only if the polar map is a bijection. If it is a bijection, then the pair (L, G^τ) is called a *polar decomposition* for (G, τ).

Lemma 4.3. *Let (G, τ) be an involutive group. Then $P = \{gg^* : g \in G\}$ is a twisted subgroup invariant under the action of G^τ by conjugation, or more generally under the action of G by congruence transformations $x \mapsto gxg^*$.*

Proof: For $g, h \in G$, $h(gg^*)h^* = (hg)(hg)^*$, and hence P is invariant under all congruence transformations. Since $h^* = h^{-1}$ for $h \in G^\tau$, these congruence transformations reduce to conjugations. For $g, h \in G$, we have

$$gg^*(hh^*)^{-1}gg^* = (gg^*(h^{-1})^*)(gg^*(h^{-1})^*)^*,$$

so P is a twisted subgroup. $\square$

Most, if not all, of the equivalences below may be found in the literature and are more or less familiar to researchers in loop theory.

Proposition 4.4. *Let (G, τ) be an involutive group, $P = \{gg^* | g \in G\}$. The following are equivalent:*

(1) *P is a uniquely 2-divisible twisted subgroup;*
(2) *P is transversal to G^τ, i.e., the map $(x, g) \mapsto xg : P \times G^\tau \to G$ is bijective;*
(3) *every element $g \in G$ has a unique polar decomposition $g = xk \in PG^\tau$, $x \in P$, $k \in G^\tau$, where $x = (gg^*)^{1/2}$.*

Proof: (1) $\Rightarrow$ (3): If $g = x_1k_1 = x_2k_2 \in PG^\tau$, then $gg^* = (x_1)^2 = (x_2)^2$. Hence $x_1 = x_2$, and then $k_1 = k_2$. Thus factorizations, when they exist, are unique.

For $g \in G$, set $x := (gg^*)^{1/2} \in P$. Choose $k \in G$ so that $g = xk$. We are finished if we show that $k \in G^\tau$. We have

$$kk^* = (x^{-1}g)(x^{-1}g)^* = (gg^*)^{-1/2}gg^*(gg^*)^{-1/2} = e,$$

and thus $k^* = k^{-1}$, i.e., $k \in G^\tau$.

(3) $\Rightarrow$ (2): Immediate.

(2) $\Rightarrow$ (1): By Lemma 4.3, P is a twisted subgroup. For $gg^* \in P$, let $g = xk \in PG^\tau$. Then $gg^* = xk(xk)^* = x^2$, so $x \in P$ is a square root of gg^*. If $y \in P$ were another, then one verifies that $y(y^{-1}g)$ would give another decomposition of g, since

$$y^{-1}g = y^{-1}gg^*(g^*)^{-1} = y^{-1}y^2\tau(g) = y\tau(g) = \tau(y^{-1}g).$$

□

4.4 Loops from transversals. Let $G = BH$, where H is a subgroup of G and B is transversal to H. Let $b_1, b_2 \in B$ be any two elements of B, and let

$$b_1b_2 = (b_1 * b_2)h(b_1, b_2) \in BH \tag{4.3}$$

be the unique decomposition of the element $b_1b_2 \in G$, where $b_1 * b_2 \in B$ and $h(b_1, b_2) \in H$, determining (i) a binary operation $*$ in B, called the *transversal operation* of B induced by G, and (ii) a map $h : B \times B \to H$, called the *transversal map*. Then as an algebraic structure $(B, *)$ is a left loop, that is, it has an identity, namely the identity e of the group, and there is a unique solution of the equation $a * x = b$ for all $a, b \in B$ (see, for example, [6, Theorem 2.7]). The various types of left loops and loops that arise as one imposes various additional properties on the transversal B have been quite intensively studied.

Things become quite nice in the case that we considered in the previous subsection.

Theorem 4.5. *Let (G, τ) be an involutive group, $K = G^\tau$ the fixed point subgroup, and $P = \{xx^* : x \in G\}$ satisfy any of the three equivalent conditions of Proposition 4.4. Then for $b_1, b_2 \in P$,*

$$b_1b_2 = (b_1 * b_2)h(b_1, b_2) \in PK,$$

where $(b_1 * b_2) = (b_1b_2^2b_1)^{1/2}$. Furthermore, $(P, *)$ is a B-loop.

Proof: That $(b_1 * b_2) = (b_1b_2^2b_1)^{1/2}$ follows from Proposition 4.4(3). That $(P, *)$ is a B-loop then follows from Proposition 4.4(1) and Corollary 4.2. □

Let $a, b \in L$, a loop. An important role is played in loop theory by the *precession map* $\gamma_{a,b} : L \to L$, which is the unique function satisfying for all $c \in L$ the equation:

$$a * (b * c) = (a * b) * \gamma_{a,b}c.$$

Proposition 4.6. *Let (G, τ) be an involutive group, $K = G^\tau$ the fixed point subgroup, and $P = \{xx^* : x \in G\}$ satisfy any of the three equivalent conditions of Proposition 4.4, and let $(P, *)$ be the B-loop defined in Theorem 4.5. Then the precession map $\gamma_{a,b}$ is given by conjugation by $h(a, b)$, i.e., $c^{h(a,b)} := h(a, b)ch(a, b)^{-1} = \gamma_{a,b}c$ for all $c \in P$.*

Proof: We note for some $h_1, h_2 \in K$

$$a(bc) = a(b * c)h_1 = a * (b * c)h_2 h_1$$

and for some $h_3 \in K$

$$(ab)c = (a * b)h(a,b)c = (a * b)c^{h(a,b)}h(a,b)^{-1} = (a * b) * c^{h(a,b)}h_3 h(a,b)^{-1}.$$

By uniqueness of the polar decomposition, we have $a*(b*c) = (a*b)*c^{h(a,b)}$. From the defining equation for $\gamma_{a,b}$, we conclude for all $c \in P$ that $c^{h(a,b)} = \gamma_{a,b}c$. □

5. The Möbius loop

In this section we obtain the major result of the paper, Theorem 5.2, an analog for euclidean space of Möbius loop on the complex unit disk.

Let B be the open unit ball in $\mathbb{R}^n \subseteq \hat{\mathbb{R}}^n$, and let $G(B)$ be the group of all Möbius transformations that carry B onto B. Define $j : B \to B$ by $j(x) = -x$ and define the involution σ on $G(B)$ by $\sigma(g) = jgj$.

Theorem 5.1. *For the involutive group $(G(B), \sigma)$, we have $G(B)^\sigma = G(B)_0$ (the isotropy group at 0) is the orthogonal group $\mathrm{O}(n)$ and $P := \{gg^* : g \in G\} = \{\tau_a : a \in B\}$ is a uniquely 2-divisible twisted subgroup. Hence $(x, h) \mapsto xh$ from $P \times \mathrm{O}(n)$ to $G(B)$ is a bijection.*

Proof: Since $\theta(-x) = -\theta(x)$ for an orthogonal map θ, it follows directly that $j\theta j = \theta$, i.e., $\theta \in G(B)^\sigma \subseteq G(B)_0$. Conversely from the theory of Möbius geometry, any Möbius transformation in $G(B)$ fixing 0 must be an orthogonal map. Therefore $\mathrm{O}(n) = G(B)^\sigma = G(B)_0$.

We note that

$$\sigma(\tau_a)(x) = j\tau_a j(x) = j\tau_a(-x) = -(a-x)(1+ax)^{-1} = (x-a)(1+ax)^{-1} = \tau_{-a}(x),$$

and hence $\sigma(\tau_a) = \tau_{-a} = (\tau_a)^{-1}$. It follows that $\tau_a = (\tau_a)^* \in G(B)_\sigma$. For $0 < r < 1$,

$$\begin{bmatrix} 1 & ra \\ -ra & 1 \end{bmatrix}\begin{bmatrix} 1 & ra \\ -ra & 1 \end{bmatrix} = \begin{bmatrix} 1+r^2|a|^2 & 2ra \\ -2ra & 1+r^2|a|^2 \end{bmatrix} = (1+r^2|a|^2)\begin{bmatrix} 1 & \frac{2ra}{1+r^2|a|^2} \\ \frac{-2ra}{1+r^2|a|^2} & 1 \end{bmatrix}.$$

Since the last matrix is a scalar times a matrix inducing the Möbius translation $\tau_{2ra/(1+r^2|a|^2)}$, it also induces this same translation. Solving $2r/(1 + r^2|a|^2) = 1$ for r, we find the solution $0 < r = 1 - \sqrt{1 - |a|^2} < 1$ and conclude $\tau_{ra}\tau_{ra}^* = \tau_{ra}\tau_{ra} = \tau_a$. Thus each $\tau_a \in P$, in particular $\tau_{ra} \in P$, and hence τ_a has a square root in P. This shows $\{\tau_a : a \in B\} \subseteq P$.

Conversely let $gg^* \in P$. Then (from the last paragraph of the Section 2) we have $g = \sigma_b\theta$ for some $b \in B$ and $\theta \in \mathrm{O}(n)$. Then

$$gg^* = \tau_b\theta\theta^*\tau_b = \tau_b\tau_b = \tau_{2b/(1+|b|^2)},$$

the last equality following from the use of Vahlen matrices as in the preceding paragraph. We conclude that $P = \{\tau_a : a \in B\}$. Finally we see that square roots in P are unique because if $a \neq b \in B$, then $\tau_a^2(0) = 2a/(1+|a|^2) \neq 2b/(1+|b|^2) = \tau_b^2(0)$. It follows from Proposition 4.4 that the factorization $G(B) = P\,\mathrm{O}(n)$ is unique. □

For $a, b \in B$, we have

$$\begin{bmatrix} 1 & a \\ -a & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ -b & 1 \end{bmatrix} = \begin{bmatrix} 1 & (a+b)(1-ab)^{-1} \\ -(a+b)(1-ab)^{-1} & 1 \end{bmatrix} \begin{bmatrix} 1-ab & 0 \\ 0 & 1-ab \end{bmatrix}.$$

The Möbius transformation induced by the right most Vahlen matrix sends x to $(1-ab)x(1-ab)^{-1}$. By Remark 2.3 this map is a rotation. Hence the induced Möbius transformations from the right hand side give the $P\,\mathrm{O}(n)$ factorization, and we conclude from Theorem 4.5 that P is a B-loop with respect to the operation $\tau_a * \tau_b = \tau_{(a+b)(1-ab)^{-1}}$. If we transfer this operation to B via the set bijection $a \leftrightarrow \tau_a$, we obtain a B-loop called the *Möbius loop* on B with operation given in terms of the Clifford algebra operations by

$$a * b = \frac{a+b}{1-ab}\,. \tag{5.4}$$

If we multiply the diagonal Vahlen matrix with entries $1-ab$ by the scalar $1/|1-ab|$, we obtain a new matrix that induces the same Möbius transform. This new matrix has diagonal entries $q := (1-ab)/|1-ab|$. Since

$$|q|^2 = q\overline{q} = \frac{(1-ab)(\overline{1-ab})}{|1-ab|^2} = \frac{|1-ab|^2}{|1-ab|^2} = 1,$$

we conclude that $|q| = 1$. Since q is the product of two members of $\mathbb{R}^n$ by Remark 2.3, we conclude that q is in Spin_n. It follows from Proposition 4.6 that the precession $\gamma_{a,b}$ is equal to conjugation by q. We summarize:

Theorem 5.2. *The Möbius loop on the open unit ball in $\mathbb{R}^n$ has operations given in terms of the Clifford algebra $\mathcal{C}_n$ by*

$$a \oplus b = (a+b)(1-ab)^{-1}, \;\; \gamma_{a,b}(x) = qxq^{-1} \quad \text{where} \quad q = \frac{1-ab}{|1-ab|}\,.$$

Hence $\gamma_{a,b} \in \mathrm{SO}(n, \mathbb{R})$.

Remark 5.3. *A fairly straightforward computation yields that the preceding rotation arising from conjugation by q is actually a rotation in the plane determined by a and b that leaves the orthogonal complement of this plane pointwise fixed.*

6. Gyrogroups

The results of the preceding sections involving B-loops and the Möbius loop can be recast in the framework of gyrogroups, which have been introduced and studied in some detail by A. Ungar [11]. Indeed B-loops are equivalent to uniquely 2-divisible gyrocommutative gyrogroups, with the loop operation $a*b$ corresponding to the gyroaddition $a \oplus b$ and the precession maps $\gamma_{a,b}$ corresponding to the gyroautomorphisms $\mathrm{gyr}[a,b]$. Many of the preceding results involving transversals and loops can be found in the paper [2] of Foguel and Ungar reformulated in the framework of gyrogroups. We recall, for example, [2, Theorem 4.5]:

Theorem 6.1. *Let (G,τ) be an involutive group, let $H \subseteq G^\tau$ be a subgroup, let $L \subseteq G_\tau$ be a twisted subgroup transversal to H such that $hLh^{-1} \subseteq L$ for all $h \in H$. Then L is a gyrocommutative gyrogroup with respect to the transversal operation $\odot(= *)$ induced on it. Furthermore the gyroautomorphisms $\mathrm{gyr}[a,b]$ for $a,b \in L$ are given by $\mathrm{gyr}[a,b](x) = x^{h(a,b)} = h(a,b)xh(a,b)^{-1}$.*

Corollary 6.2. *Let (G,τ) be an involutive group, $P = \{gg^*|g \in G\}$. If P is transversal to G^τ or P is uniquely 2-divisible, then P endowed with the transversal operation is a gyrocommutative gyrogroup with $\mathrm{gyr}[a,b](x) = x^{h(a,b)}$. Furthermore, $a \odot b = (ab^2a)^{1/2}$.*

Proof: By Lemma 4.3 P is a twisted subgroup invariant under conjugation by G^τ and the two conditions of tranversality and unique 2-divisibility are equivalent by Proposition 4.4. Thus for P transversal, the first two conclusions follow from Theorem 6.1. For the last assertion, by definition of the transversal operation we have $ab = (a \odot b)h(a,b)$. Hence

$$(a \odot b)^2 = (a \odot b)(a \odot b)^* = (abh(a,b)^{-1})(h(a,b)ba) = ab^2a,$$

and hence $a \odot b = (ab^2a)^{1/2}$ by unique 2-divisibility. $\square$

We remark that one of the principal objects of study in [11] is the Möbius gyrogroup, or the Möbius loop in our terminology. Ungar [11] defines the Möbius gyroaddition on the unit ball of $\mathbb{R}^n$ by equation (3.2). Our approach via Clifford algebras yields an equivalent, but much more compact formula, given by equation (5.4), which is a more general form of the standard formula for the Möbius loop on the open complex unit ball. We think that this approach via Clifford algebras yields a much more accessible approach from an algebraic point of view. While we have set this approach in the framework of B-loops, it is equally valid in the framework of gyrocommutative gyrogroups.

References

[1] Ahlfors L.V., *Möbius transformations and Clifford numbers*, in Differential Geometry and Complex Analysis (I. Chavel and H.M. Farkas, Eds.), Springer, Berlin, 1985, pp. 65–73.
[2] Foguel T., Ungar A.A., *The involutory decomposition of groups into twisted subgroups and subgroups*, J. Group Theory **3** (2000), 27–46.
[3] Glauberman G., *On loops of odd order I*, J. Algebra **1** (1964), 374–396.
[4] Glauberman G., *On loops of odd order II*, J. Algebra **8** (1968), 393–414.
[5] Karzel H., *Recent developments on absolute geometries and algebraization by K-loops*, Discrete Mahematics **208/209** (1999), 387–409.

[6] Kiechle H., *Theory of K-Loops*, Lecture Notes in Mathematics, 1778, Springer, Berlin, 2002.

[7] Kinyon M., *Global left loop structures on spheres*, Comment. Math. Univ. Carolin. **41** (2000), 325–346.

[8] Kinyon M., Jones O., *Loops and semidirect products*, Comm. Algebra **28** (2000), 4137–4164.

[9] Kreuzer A., *Beispiele endlicher und unendlicher K-loops*, Results Math. **23** (1993), 355–362.

[10] Karzel H., Wefelscheid H., *Groups with an involutory antiautomorphism and K-loops; application to space-time-world and hyperbolic geometry*, Results Math. **23** (1993), 338–354.

[11] Ungar A.A., *Analytic Hyperbolic Geometry and Albert Einstein's Special Theory of Relativity*, World Scientific Publishing Co., Hackensack, NJ, 2008.

[12] Vahlen K.Th., *Über Bewegungen und komplexe Zahlen*, Math. Ann. 55 (1902), p. 585.

[13] Waterman P.L., *Möbius transformations in several dimensions*, Advances in Math. **101** (1993), 87–113.

Department of Mathematics, Louisiana State University, Baton Rouge, LA70803, USA

E-mail: lawson@math.lsu.edu

(*Received* August 24, 2009, *revised* February 8, 2010)