CRITERIA FOR FINITE SYMMETRIC SPACES

XIANGKAI SUN

1. Introduction

Symmetric spaces have been widely studied in the context of differential geometry and representation theory. This concept is motivated by how to define convolution of functions on a space. It turns out that if the space is a quotient space G/K, where G is a finite group and K is a subgroup of G, the functions on the space are symmetric under group actions of K, and the group convolution is commutative, then we can extend the definition of convolution on groups to symmetric spaces. In this paper, we will study the finite symmetric spaces. To determine whether G and K can form a symmetric space, we introduce two criteria, Gelfand's criterion and Selberg's criterion, that are sufficient for G/K to be a finite symmetric space. We will also show that the finite upper half plane is a finite symmetric space.

2. Definition of finite symmetric spaces

For a finite group G and a subgroup K of G, we first define the set of double cosets of G, denoted by $K\backslash G/K$.

Definition 2.1. Given a finite group G and a subgroup K, the *K-double coset of $x \in G$* is the set

$$KxK = \{hxk : h, k \in K\}. \tag{2.1}$$

The set of all K-double cosets is denoted by $K\backslash G/K$.

For double cosets $K\backslash G/K$, we want to assign a convolution operation on the function space defined on double cosets.

Definition 2.2. A *K-bi-invariant function* $f \in L^2(G)$ is a function such that $f(x) = f(hxk)$ for any $h, k \in K$ and $x \in G$. We use $L^2(K\backslash G/K)$ to denote the set of all K-bi-invariant function.

We can define the convolution on $L^2(K\backslash G/K)$ by extending the convolution on $L^2(G)$.

Definition 2.3. Suppose that K is a subgroup of a finite group G. Then the *convolution* on $L^2(K\backslash G/K)$ is an operation:

$$\begin{aligned} *:\ L^2(K\backslash G/K) \times L^2(K\backslash G/K) \to& L^2(K\backslash G/K) \\ (f * g)(KxK) =& \sum_{y \in G} f(Kxy^{-1}K)g(KyK) \\ & \forall f, g \in L^2(K\backslash G/K), x \in G. \end{aligned} \tag{2.2}$$

It is necessary to show that this is well-defined, i.e., it is independent of the choice of representative x, so that the convolution of two functions $f, g \in L^2(K\backslash G/K)$, $f * g$, is also in $L^2(K\backslash G/K)$.

Let x_1, x_2 be two representatives of a coset, so there exists $k_1, k_2 \in K$ such that $x_1 = k_1 x_2 k_2$. Then

$$\begin{aligned}(f * g)(x_1) &= \sum_{y\in G} f(x_1 y^{-1}) g(y) \\ &= \sum_{y\in G} f(k_1 x_2 k_2 y^{-1}) g(y) \\ &= \sum_{yk_2^{-1}\in G} f(x_2(yk_2^{-1})^{-1}) g(yk_2^{-1}) \\ &= (f * g)(x_2).\end{aligned} \tag{2.3}$$

Hence this is a well-defined operation.

In this paper, we will only study finite groups. Here we define the (finite) symmetric spaces. The word "finite" is implied unless specified.

Definition 2.4. Suppose that K is a subgroup of G. Then (G, K) is a *Gelfand pair* if the convolution on $L^2(K\backslash G/K)$ is commutative. The quotient space, G/K, is a *symmetric space*.

3. Criteria of symmetric spaces

In this section, we give two criteria for G/K to be a symmetric space. We start with Gelfand's criterion.

Definition 3.1. A group G and a subgroup K of G satisfy *Gelfand's criterion* if and only if there is a group isomorphism $\tau : G \to G$ such that $s^{-1} \in K\tau(s)K$, or $Ks^{-1}K = K\tau(s)K$, for all $s \in G$.

To show that Gelfand's criterion implies that (G, K) is a Gelfand pair, we first prove a lemma.

Lemma 3.2. *If $\tau : G \to G$ is a group isomorphism, then*

$$(f * g)^\tau = f^\tau * g^\tau \tag{3.1}$$

where $f^\tau(x) = f(\tau(x))$ for all $x \in G$.

Proof. Let $z = \tau(y)$. Since τ is an isomorphism, $z^{-1} = \tau(y^{-1})$. We start with writing down the formula of convolution for the left hand side. For any $x \in G$,

$$\begin{aligned}(f * g)^\tau(x) &= \sum_{z\in G} f(\tau(x) z^{-1}) g(z) \\ &= \sum_{y\in G} f(\tau(xy^{-1})) g(\tau(y)) \\ &= \sum_{y\in G} f^\tau(xy^{-1}) g^\tau(y) \\ &= (f^\tau * g^\tau)(x).\end{aligned} \tag{3.2}$$

$\square$

Theorem 3.3. *If (G, K) satisfies Gelfand's criterion, then (G, K) is a Gelfand pair, i.e. the convolution on $L^2(K\backslash G/K)$ is commutative.*

Proof. For $f \in L^2(K\backslash G/K)$, denote $\check{f}(x) = f(x^{-1})$ for all $x \in G$. Since there exists an isomorphism τ such that for all $x \in G$ we have $x^{-1} \in K\tau(x)K$, then

$$\check{f}(x) = f(\tau(x)) = f^\tau(x). \tag{3.3}$$

By Lemma 3.2, $(f * g)\check{} = (f * g)^\tau = f^\tau * g^\tau = \check{f} * \check{g}$. Since

$$\begin{aligned}(\check{f} * \check{g})(t) &= (f * g)\check{}(t) \\ &= \sum_{s\in G} f(t^{-1}s^{-1})g(s) \\ &= \sum_{b\in G} f(b^{-1})g(bt^{-1}) \\ &= \sum_{b\in G} \check{f}(b)\check{g}(tb^{-1}) = (\check{g} * \check{f})(t),\end{aligned} \tag{3.4}$$

we can derive the commutation relation of the convolution:

$$f * g = \check{\check{f}} * \check{\check{g}} = \check{\check{g}} * \check{\check{f}} = g * f. \tag{3.5}$$

Thus, the convolution on $L^2(K\backslash G/K)$ is commutative. □

As a special case of Gelfand's criterion, if τ is the identity, then we get this useful following corollary.

Corollary 3.4. *If $(KsK)^{-1} = KsK$ for all $s \in G$, then (G, K) is a Gelfand pair.*

Another sufficient condition for (G, K) to be a Gelfand pair is Selberg's criterion.

Definition 3.5. We say that $X = G/K$ satisfies *Selberg's criterion* if there is an one-to-one map $\mu : X \to X$ such that $\mu(eK) = eK$, and for every $x, y \in X$ there is an $m \in G$ such that $mx = \mu y$ and $my = \mu x$.

By definition, to show that (G, K) forms a Gelfand pair, we only need to show that the convolution is commutative on $L^2(K\backslash G/K)$ under Selberg's criterion.

Theorem 3.6. *If (G, K) satisfies Selberg's criterion, then (G, K) is a Gelfand pair, i.e. the convolution on $L^2(K\backslash G/K)$ is commutative.*

Proof. We want to show that the setup of the Selberg criterion is similar to that of the Gelfand criterion. To do this, we define a point-pair invariant $K_f(a, b) = f(b^{-1}a)$ for $a, b \in G/K$ and $f \in L^2(K\backslash G/K)$ which has the property that for all $g \in G$, $K_f(ga, gb) = K_f(a, b) = K_{\check{f}}(b, a)$. By Selberg's criterion, we know that there exists μ such that $K_f(\mu x, \mu y) = K_f(my, mx) = K_f(y, x) = K_{\check{f}}(x, y)$ for all $x, y \in G$. Here μx is a short-hand of $\mu(xK)$, for both μ and K_f are defined with G/K. It follows that $f((\mu y)^{-1}\mu x) = f(x^{-1}y)$.

Now we take $y = K$. Then we get $f(K^{-1}\mu x) = f(x^{-1}K)$. Recall that $f \in L^2(K\backslash G/K)$, this naturally implies that

$$f(\mu x) = f(x^{-1}), \tag{3.6}$$

i.e. for any $x \in G$, $x^{-1} \in K\mu(x)K$. This looks similar to the Gelfand's criterion. In addition,

$$f((\mu y)^{-1}\mu x) = f(x^{-1}y) = f(\mu(y^{-1}x)). \tag{3.7}$$

Notice that 3.6 and 3.7 are identical to 3.3 and 3.2 if μ is replaced with τ, which are derived from the Gelfand's criterion, this statement can be proved following the same procedure as before.

□

Besides the theorem that quotient spaces satisfying either criterion is a symmetric space, we feel obliged to mention that the converse of the statement is not true. That is, a symmetric space does not necessarily satisfy either Gelfand's or Selberg's criterion. Consider the quotient space given by $G = GL(2, \mathbb{F}_q)$ and $K = \text{Aff}(q)$. The quotient space is a symmetric space, yet (G, K) does not satisfy Gelfand's criterion [K].

There a stricter but more useful criterion when K is a normal subgroup of G.

Theorem 3.7. *Let K be a normal subgroup of G. If G/K is an abelian group, then G/K is a symmetric space.*

Proof. We will first show that $G/K = K\backslash G/K$. First, any element gk for some $g \in G$ and $k \in K$ in coset gK is also in the double coset KgK. Thus $gK \subset KgK$. Next, since K is a normal subgroup, for any $k_1 g k_2 \in KgK$ for some $k_1, k_2 \in K$,

$$k_1 g k_2 = g(g^{-1}k_1 g)k_2 = gk' \tag{3.8}$$

where $k' \in K$. Thus $KgK \subset gK$. Combining both statements, we see that $gK = KgK$ for all $g \in G$.

If G/K is an abelian group, then for any $f, g \in L^2(K\backslash G/K)$ and $x \in G/K$,

$$\begin{aligned}(f * g)(x) &= \sum_{y\in G} f(xy^{-1})g(y)\\ &= \sum_{z\in G/K}\sum_{k\in K} f(xz^{-1}k^{-1})g(kg)\\ &= \sum_{z\in G/K}\sum_{k\in K} g(z)f(z^{-1}x)\\ &= \sum_{w\in G} g(w)f(w^{-1}x)\\ &= (g * f)(x).\end{aligned} \tag{3.9}$$

This means that the convolution is commutative on $L^2(K\backslash G/K)$. □

4. Finite upper half plane is a finite symmetric space

An example of symmetric space is the finite upper half plane, which is a "finite version" of the real Poincaré upper half plane [T].

Definition 4.1. The *finite upper half plane* is

$$H_q = \{z = x + y\sqrt{\delta} : x \in \mathbb{F}_q, y \in \mathbb{F}_q\backslash\{0\}\} \tag{4.1}$$

where $q = p^r$ for some odd prime p and $\delta \in \mathbb{F}_q$ is a nonsquare.

To show that the finite upper half plane is a finite symmetric space, we first express H_q as a quotient space of two groups.

Theorem 4.2. *Let $G = GL(2, \mathbb{F}_q)$ where $q = p^r$ for some odd prime p and*

$$K = \left\{ \begin{pmatrix} a & b\delta \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_q, a^2 - \delta b^2 \neq 0 \right\}.$$

The finite upper half plane H_q is isomorphic to G/K.

Before proving the theorem, we first show that there is an isomorphism between K and the multiplicative group $\mathbb{F}_q^\times(\sqrt{\delta})$,

$$\begin{pmatrix} a & b\delta \\ b & a \end{pmatrix} \mapsto a + b\sqrt{\delta}.$$

This follows from the matrix multiplication, where

$$\begin{pmatrix} a & b\delta \\ b & a \end{pmatrix} \begin{pmatrix} c & d\delta \\ d & c \end{pmatrix} = \begin{pmatrix} ac + bd\delta & (ad + bc)\delta \\ ad + bc & ac + bd\delta \end{pmatrix}.$$

Also, we have $(a + b\sqrt{\delta})(c + d\sqrt{\delta}) = (ac + bd\delta) + (ad + bc)\sqrt{\delta}$. Thus, the group K has order $q^2 - 1$ and it is cyclic.

Definition 4.3. The *affine group over field* $\mathbb{F}_q$ is

$$A = \mathrm{Aff}(q) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q \backslash \{0\}, b \in \mathbb{F}_q \right\}.$$

We denote the matrix above as $(a\ b)$ for simplicity.

The affine group has order $q(q-1)$.

Proof. (Proof of Theorem 4.2) We first define the group action of G on H_q as

$$gz = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}. \tag{4.2}$$

First, we want to show that K contains all elements that fix $\sqrt{\delta}$, so K is the stabilizer subgroup with respect to $\sqrt{\delta}$.

Suppose that

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

fixes $\sqrt{\delta}$. Then

$$g\sqrt{\delta} = \frac{a\sqrt{\delta} + b}{c\sqrt{\delta} + d} = \sqrt{\delta} \Rightarrow a = d, b = c\delta.$$

Thus, for any $g, h \in G$ that are in the same coset aK for some $a \in G$, $g\sqrt{\delta} = h\sqrt{\delta}$.

Since G acts transitively on H_q, and $|G/K| = q(q-1) = |H_q|$, there is a bijection between H_q and G/K.

$\square$

Moreover, The orbit of $\sqrt{\delta}$ moved by the affine group A is the whole set H_q, for $z = x + y\sqrt{\delta} = (y\ x)\sqrt{\delta}$. Thus there is a bijection

$$\begin{aligned} A &\leftrightarrow H_q \leftrightarrow G/K \\ g &\mapsto g\sqrt{\delta} \mapsto gK. \end{aligned} \tag{4.3}$$

It turns out that the orbit-stabilizer formula, $|G| = q(q+1)(q-1)^2 = |A||K|$, is satisfied. It follows that we can select a representative $g_i \in A$ for any coset $g_iK \in G/K$. From now on, the notation for a coset $g_iK = (y\ x)K$ can be $g_i\sqrt{\delta}$ or just its representative $g_i \in A$, depending on the context.

To show that H_q is a symmetric space, we will prove that H_q satisfies corollary 3.4.

Remark 4.4. The finite upper half plane G/K also satisfies Selberg criterion [T].

Theorem 4.5. *(G, K) satisfies corollary 3.4, so H_q is a finite symmetric space.*

To prove this theorem, we need to introduce a distance function.

Definition 4.6. The *imaginary part* of $z = x+y\sqrt{\delta} \in H_q$ is denoted as $\mathrm{Im}(z) = y$. The *conjugate* of $z = x + y\sqrt{\delta}$ is $\bar{z} = x - y\sqrt{\delta}$.
The *norm* of z is denoted as $N(z) = z\bar{z}$.

Definition 4.7. The *distance* function on H_q is a map $d : H_q \times H_q \to \mathbb{F}_q$:

$$d(z, w) = \frac{N(z - w)}{\mathrm{Im}(z)\mathrm{Im}(w)}. \tag{4.4}$$

Remark 4.8. This is an analogue of the Poincaré distance on the real upper half plane, where we replace $\sqrt{\delta}$ with complex number i. The length element on the real Poincaré upper half plane is $ds^2 = y^{-2}(dx^2 + dy^2)$.

It is easy to verify that $d(gz, gw) = d(z, w)$ for all $z, w \in H_q$ and $g \in G$. Combined with the fact that K fixes $\sqrt{\delta}$, K fixes the distance between $g_i\sqrt{\delta}$ and $\sqrt{\delta}$.

Lemma 4.9. *For $g_i \in A$, $d(kg_i\sqrt{\delta}, \sqrt{\delta}) = d(kg_i\sqrt{\delta}, k\sqrt{\delta}) = d(g_i\sqrt{\delta}, \sqrt{\delta})$ for all $k \in K$.*

Let $S_q(\sqrt{\delta}, a) \subset H_q$ denote the set of all elements g such that $d(g, \sqrt{\delta}) = a$, which can be interpreted as a sphere of radius a centered at $\sqrt{\delta}$. Then for each $a \in F_q$, $S_q(\sqrt{\delta}, a)$ is a union of left $K-$orbits.

Proof. (Theorem 4.5) It suffices to show that $g^{-1} \in KgK$ for all $g \in G$. We will prove this in two steps. First we will show that the orbit of $g\sqrt{\delta}$ under K equals the set $S_q(\sqrt{\delta}, a)$ to which it belongs. Second, we will show that if $g\sqrt{\delta} \in S_q(\sqrt{\delta}, a)$, then $g^{-1}\sqrt{\delta} \in S_q(\sqrt{\delta}, a)$. [P]

We start with the first statement. First we count the number of elements in the set $S_q(\sqrt{\delta}, a)$.

Lemma 4.10. $|S_q(\sqrt{\delta}, a)| = 1$ *when* $a = 0, 4\delta$ *and* $q + 1$ *otherwise.*

Proof. This can be done by counting the number of elements $(y\ x)$ that satisfy $x^2 = ay + \delta(y-1)^2$. Rearranging this yields

$$x^2 - \delta\left(y + \frac{a}{2\delta} - 1\right)^2 = \frac{a(4\delta - a)}{4\delta}.$$

Redefine $t := y + \frac{a}{2\delta} - 1$ and $r = \frac{a(4\delta-a)}{4\delta}$, we want to find the number of elements $z = x + t\sqrt{\delta}$ that satisfy $N(z) = r$. When $r = 0$, i.e. $a = 0, 4\delta$, there exists a single solution $z = \sqrt{\delta}$. Since $N(z) = z^{q+1} = r$ has $q+1$ solutions when $r \neq 0$, $|S_q(\sqrt{\delta}, a)| = q + 1$ if $a \neq 0, 4\delta$. □

For $a = 0, 4\delta$, the only elements on the "sphere" are $z = (1\ 0)\sqrt{\delta}$ and $z = (-1\ 0)\sqrt{\delta}$, respectively. These two elements are fixed by the group K, so their orbits have order 1. Therefore, we only need to focus on the nontrivial case. It suffices to show that Kg_aK for $g_a \in S_q(\sqrt{\delta}, a)$ $(a \neq 0, 4\delta)$ contains $q+1$ elements. We divide this proof into two steps.

Lemma 4.11. *$Z = \{aI : a \in \mathbb{F}_q \backslash \{0\}\}$ contains all elements in K that fix $z \in H_q$ unless $z = \pm\sqrt{\delta}$.*

Proof. Suppose that $k = \begin{pmatrix} a & b\delta \\ b & a \end{pmatrix}$ fixes z. Then $z(a + bz) = az + b\delta \Rightarrow b\delta = bz^2$. If $z \neq \pm\sqrt{\delta}$, then $b = 0$. □

Next, since K is cyclic, we select a generator κ of K. Since K is isomorphic to the multiplicative group $\mathbb{F}_q^\times(\sqrt{\delta})$, $q+1$ is the smallest positive power r such that $\kappa^r \in Z$. Thus $|\{\kappa^i g_a\sqrt{\delta} : i \in \{0, 1, \cdots, q\}\}| = q + 1 = |S_q(\sqrt{\delta}, a)|$ for $a \neq 0, 4\delta$. Combined with the fact that $\{\kappa^i g_a\sqrt{\delta} : i \in \{0, 1, \cdots, q\}\} \subset Kg_a\sqrt{\delta} \subset S_q(\sqrt{\delta}, a)$, we see that $S_q(\sqrt{\delta}, a)$ contains a single left K-orbit.

The second step is to show the following lemma.

Lemma 4.12. *If $g \in S_q(\sqrt{\delta}, a)$, then $g^{-1} \in S_q(\sqrt{\delta}, a)$.*

Proof. We use the properties of the distance function:

$$d(g\sqrt{\delta}, \sqrt{\delta}) = d(\sqrt{\delta}, g^{-1}\sqrt{\delta}) = d(g^{-1}\sqrt{\delta}, \sqrt{\delta}).$$

□

Thus $g^{-1} \in KgK$ for all $g \in G$. This finishes the proof of the main theorem.

□

Here we give an example of the finite upper half plane H_3 (Figure 1). It contains a sphere of order $4 = 3 + 1$ of radius 1, and 2 poles of radius 0 and $2 = 4\delta$.

5. Conclusion

In this paper, we introduced the finite symmetric spaces, in terms of quotient spaces of a finite group G with a subgroup K of G. We proved that two criteria, Gelfand's criterion and Selberg's criterion, can be used to determine whether K-bi-invariant functions are commutative under convolution. As an analogue of the real Poincaré upper half plane, we showed that the finite upper half plane is a finite symmetric space.

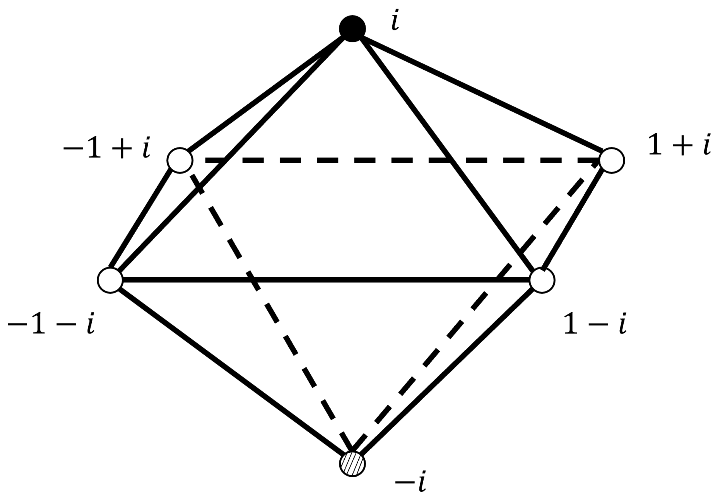

FIGURE 1. A graph for H_3. Here $i = \sqrt{2}$. It contains 6 elements, 4 of which form a sphere of radius 1. In this graph, each line segment has length 1.

References

[T] A. Terras. *Fourier Analysis on Finite Groups and Applications.* Cambridge University Press (1999).

[K] A. Krieg. Hecke algebras. *Memoirs of the American Society*, **87**(435) (September, 1990), 29.

[P] S. Poulos. Graph theoretic and spectral properties of finite upper half-planes. *Ph.D. Thesis, University of California at San Diego*, (1991).

MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 77 MASSACHUSETTS AVENUE, CAMBRIDGE, MA 02139