The Nepali Math. Sc. Report
Vol. 24, No 1, 2005.

Representation of certain probability groups as orbit spaces of groups

H.N. BHATTARAI

Abstract: The set of double cosets of a group with respect to a subgroup and the set of orbits of a group with respect to a group of automorphisms have structures which can be studied as multigroups, hypergroups or Pasch geometries. When the subgroup or the group of automorphisms are finite, the multivalued products can be provided with some weightages forming so-called Probability Groups. It is shown in this paper that certain abstract probability groups can be realized as orbit spaces of groups.

1.Introduction

The set of double cosets of a group with respect to a subgroup and the set of orbits of a group with respect to a group of automorphisms inherit certain structures from the group which have been studied as multigroups ([6], [9]), hypergroups [10], or Pasch geometries. In particular, the points of the projective space $P(V)$ of a vector space V over a (skew)-field F can be taken as the set of orbits V/F^* and the inherited structure provides the geometry of the projective space. In addition, some of these structures possess probabilistic measures whereby there is a certain probability for a given element to belong to the set of products of two given elements. Such structures have been abstractly studied as Probability groups ([1],[7]). Double cosets and orbits of topological groups with convolution of measures have been studied as convos or hypergroups. A probability group is equivalent to a discrete convo of [8]. The prototypes of probability groups are the double cosets and orbits of groups. So a natural converse question would be: what are the necessary and sufficient conditions for an abstract probability group to be realized as an orbit space or a double coset space of a group? It has been proved in [2] that an elementary abelian Pasch geometry is isomorphic as geometries to an orbit space of an abelian group. Also, a geometric space over a geometric sfield is shown to be isomorphic to the orbit space of a vector space (see [5]). We show here that a finite elementary abelian probability group of proper length is isomorphic as probability group to the orbit space of a group. Similarly a probability space of proper dimension over a geometric sfield is shown to be isomorphic to the probability space of a vector space. In particular, it gives that probability group structure on a projective space of finite order is unique. We wish to point out that the

study of projective geometry and related spaces in the framework of Pasch geometry has the convenience of dealing with morphisms and homomorphisms with the availability of homomorphism theorems similar to other algebraic structures (see [3].).

2. Preliminaries

In this section we briefly present the basic concepts and preliminary results on Pasch geometries and probability groups. The details can be found in the references, particularly in [7].

Definition 2.1 By a Pasch geometry is meant a triple (A, e, Δ) where A is a set, $e \in A$, and $\Delta_A = \Delta \subseteq A \times A \times A$ subject to the following axioms:

1. $\forall a \in A$, $\exists$ a unique $b \in A$ with $(a, b, e) \in \Delta$. Let $b = a^{\#}$.
2. $e^{\#} = e$ and $(a^{\#})^{\#} = a \forall a \in A$.
3. $(a, b, c) \in \Delta \Rightarrow (b, c, a) \in \Delta$.
4. $(a_1, a_2, a_3), (a_1, a_4, a_5) \in \Delta \Rightarrow \exists a_6 \in A$ with $(a_6, a_4^{\#}, a_2), (a_6, a_5, a_3^{\#}) \in \Delta$.

The identity element e and the inverse $a^{\#}$ are unique. Throughout this paper, geometry will mean Pasch geometry.

A geometry is called *abelian* if $(a, b, c) \in \Delta \Rightarrow (b, a, c) \in \Delta$. A geometry is called *sharp* if $(a, b, c), (a, b, d) \in \Delta \Rightarrow c = d$. Also, a geometry is called *projective* if $a^{\#} = a \forall a \in A$ and $(a, a, b) \in \Delta \Rightarrow b = e$ or $b = a$.

Now a structure stronger than the geometry defined above is given in the following.

Definition 2.2. A probability group is a pair (A, p) where A is a set and $p : A \times A \times A \to [0, 1]$ is a map to the unit interval, denoted as $(a, b, c) \to p_c(a, b)$, subject to the following axioms:

1. For $a, b \in A$, $p_x(a,b) = 0$ for all but finitely many $x \in A$ and
$$\sum_{x \in A} p_x(a,b) = 1.$$
2. For $a, b, c, d \in A$,
$$\sum_{x \in A} p_x(a,b) p_d(x,c) = \sum_{y \in A} p_d(a,y) p_y(b,c)$$
3. $\exists e \in A$ such that $p_a(e, a) = 1 = p_a(a,e)\ \forall\ a \in A$
4. For each $a \in A$, there exists a unique $b \in A$ with $p_e(a,b) \neq 0$. We denote b by $a^{\#}$.
5. $p_e(a,b) = p_{c^{\#}}(b^{\#}, a^{\#})\ \forall\ a, b, c \in A$.

It should be noted that $p_c(a,b)$ can be read as the probability for the element c to belong to the multivalued product $a.b$. Also, axiom (1) describes probability distribution, (2) gives associativity, the identity e given by (3) is unique and the unique inverse $a^{\#}$ of a given by (4) satisfies $(a^{\#})^{\#} = a\ \forall\ a \in A$. When dealing with more than one probability group, we write them as $(A, p^A), (B, p^B)$ etc. or use the same p to let the

context distinguish. We may simply write A is a probability group, the associated p being understood. A probability group is called *abelian* if $p_c(a,b) = p_c(b,a) \forall a,b,c \in A$.

The following useful relations are obtained as consequences of the axioms:

Lemma 2.3. For any probability group (A, p), we have:

(i) $p_a(c^{\#},a) = p_a(c,a)\ \forall a,c \in A$.

(ii) $p_a(a,a) \neq 1 \forall a \in A^* - \{e\}$

(iii) $p_{c^{\#}}(a,b)\, p_e(c^{\#}, c) = p_e(a,a^{\#})\, p_{a^{\#}}(b,c)$. In particular, if $b = c^{\#}$, we get

$$p_b(a,b)\, p_e(b,b^{\#}) = p_e(a,a^{\#})\, p_{a^{\#}}(b,b^{\#}).$$

(iv) $p_e(a,b) \neq 0$ if and only if $p_{a^{\#}}(b,c^{\#}) \neq 0$.

For a probability group A, let $\Delta_A = \{(a,b,c) : p_{c^{\#}}(a,b) \neq 0\}$. Then

Proposition 2.4. (A, e, Δ_A) is a Pasch Geometry.

Thus, when A is a probability group, we speak of the geometry A to mean the induced Pasch geometry structure as described above. Every probability group is a Pasch geometry but the example (4) below shows that the converse is not true.

A probability group is called *sharp (projective)* if it is sharp (projective) as a geometry.

Examples 2.5.

1. Let G be a group. Define p by $p_a(b,c) = 1$ if $a = b.c$ and 0 otherwise. Then (G, p) is a sharp probability group with $a^{\#} = a^{-1}$. Note that the probability for an element a to be in the product $b.c$ is either 1 or 0. Conversely, every sharp probability group is a group.

2. Let P be the set of points of a finite projective plane of order m. Let $A = P \cup \{e\}$, $e \notin P$. On A, define the map p as follows:

$$p_a(b,c) = \begin{cases} \delta_a(c) & \text{if } b = e, \text{ where } \delta_a(c) = 1 \text{ if } a = c, 0 \text{ otherwise} \\ \delta_a(b) & \text{if } c = e \\ \frac{1}{m-1}\delta_b(c) & \text{if } a = e \\ \frac{m-2}{m-1} & \text{if } a = b = c \neq e \\ \frac{1}{m-1} & \text{if } a, b, c \in P \text{ and } a, b, c \text{ are distinct and collinear} \\ 0 & \text{otherwise} \end{cases}$$

Then (A, p) is a probability group, the induced geometry being that of the projective plane. Note that if $m = 2$, $p_a(a, a) = 0$ and A is sharp.

3. Let G be a finite group and $\hat{G} = \{\chi_1, \chi_2, \ldots \chi_s\}$ be the set of irreducible complex characters of G. For $1 \leq i, j \leq s$, let $\chi_i . \chi_j = \sum_{k=0}^{s} n_k^{i,j} \chi_k$. Let p be defined by

$$p_{\chi_k}(\chi_i, \chi_j) = \frac{n_k^{i,j}\, \chi_k(1)}{\chi_i(1)\chi_j(1)}$$

Then $(\hat{G}, p)$ is a probability group.

4. The multiplicative group of positive rationals Q^+ acts on the additive group of rationals Q with three orbit elements: $\{[1], [-1], [0]\}$. It forms a *Pasch geometry* of orbits) (cf. 2.3). For elements $a = [1]$, $b = [1]$, we have $c = [-1]$ a unique element such that $([1], [1], [-1]) \in \Delta$. So if this geometry were induced by a probability group, then we would have $p_{[1]}([1], [1]) = 1$, contradicting lemma 2.3 (ii).

Now let (A, p) be a probability group and $S \subseteq A$, a finite subset. Set $n_S = \sum_{x \in S} \frac{1}{p_e(x, x^\#)}$. Note that $p_e(x, x^\#) \neq 0$ and S is finite, so n_s is well defined. In particular, n_A is defined if A is finite. If A is sharp and hence a group, then $n_A = |A|$, the order of the group; if A is projective representing a finite projective plane of order m, then $n_A = m^3$.

2.1. Subgeometry and subprobability group. Let A be a geometry and $B \subseteq A$. Then B is called a subgeometry if $e \in B$ and $(b_1, b_2, x) \in \Delta$, $b_1, b_2 \in B \Rightarrow x \in b$. Let $\Delta_B = \Delta_A \cap (B \times B \times B)$. Then (B, e, Δ_B) is a geometry.

Let (A, p) be a probability group and $B \subseteq A$. Then B is called a subprobability group of A if $e \in B$ and (B, p^B) is a probability group on its own where p^B is the restriction of p on $B \times B \times B$. We will simply write p for p^B. It checks that B is a subprobability group of A if and only if B is a subgeometry of A. So B is a subprobability group of A if and only if the following hold: $e \in B$ and $p_a(b_1, b_2) \neq 0$, $b_1, b_2 \in B \Rightarrow a^\# \in B$. We call B a normal subprobability group if B is normal as a subgeometry of A.

2.2. Factor Geometry and factor probability group. Let B be a subgeometry of A. For $a, b \in A$, define $a \sim b$ if $\exists b_1, b_2 \in B$ and $x \in A$ such that $(a, b_1, x^\#), (x, b^\#, b_2) \in \Delta$. This defines an equivalence relation on A. Let $A//B = \{[a] : a \in A\}$ be the set of all equivalence classes. Let $([a],[b],[c]) \in \Delta_{A//B}$ if $\exists x \in [a]$, $y \in [b]$, $z \in [c]$ with $(x, y, z) \in \Delta_A$. Then $A//B$ is a geometry.

In particular, if $A = G$ is a group and $B = H$ is a subgroup, then the set of double cosets $G//H$ is a geometry.

Now suppose B is a finite subprobability group of a probability group A. Then B is a subgeometry of A and so we get the factor geometry $A//B$. For $X, Y, Z \in A//B$ define

$$p_Z(X, Y) = \frac{1}{n_B} \sum_{b \in B} \sum_{z \in Z} \sum_{a \in A} p_a(x, b) p_z(a, y) / p_e(b, b^\#)$$

where $x \in X$, $y \in Y$ are arbitrary elements. The map p is independent of the choice of x and y and makes $A//B$ into a probability group inducing the factor geometry of $A//B$. In particular, if $A = G$ is a group and $B = H$ is finite subgroup of G, then the geometry of double cosets $G//H$ is a probability group. In this case, the map p simplifies to the following:

$$p_z(X,Y)=\frac{|xHy\cap Z|}{|H|}$$

for some $x \in x$, $y \in Y$.

2.3. Geometry and probability groups of orbits. Let A be a geometry. A group Γ is said to act on A if there is a homomorphism from Γ to the geometry automorphisms of A. Thus for $\alpha \in \Gamma$ and $a \in A$, we get $\alpha a \in A$ satisfying obvious properties. In such cases, we call A a Γ-geometry. For $a \in A$, let $\langle a\rangle = \{\alpha a : \alpha \in \Gamma\}$ denote the orbit of A and $A/\Gamma = \{\langle a\rangle : a \in A\}$ be the set of orbits. Let $(\langle a\rangle, \langle b\rangle, \langle c\rangle) \in \Delta_{A/\Gamma}$ iff $\exists x \in \langle a\rangle$, $y \in \langle b\rangle, z \in \langle c\rangle$ with $(x,y,z) \in \Delta_A$. This makes A/Γ a geometry called the geometry of orbits of A by Γ. In particular, if V is a (left) vector space over a skewfield F, then the geometry of orbits V/F^* is the geometry of the classical projective space $P(V)$.

Now, let A be a probability group. Suppose a finite group Γ acts on the geometry A. Then A is called a Γ- probability group if, in addition, $p_{\alpha a}(\alpha b,\alpha c) = p_a(b,c) \forall a, b, c \in A, \alpha \in \Gamma$. Suppose A is a Γ– probability group. Since Γ acts on the geometry A, we get the geometry of orbits A/Γ as above. Define

$$p_{\langle a\rangle}(\langle b\rangle,\langle c\rangle)=\frac{|\langle a\rangle|}{|\langle b\rangle||\langle c\rangle|}\sum_{y\in\langle b\rangle}\sum_{z\in\langle c\rangle}p_x(y,z)$$

for some $x \in \langle a\rangle$. The map is well defined and makes A/Γ into a probability group inducing the geometry of orbits. Thus, if G is a group and Γ is a finite group of automorphisms, then the geometry of orbits G/Γ is a probability group.

A special important case is given by the following:

Example 2.6. Suppose V is a vector space over a finite filed F containing m elements. The multiplicative group F^* acts on V and the set of orbits V/F^* is a probability group of the corresponding projective space.. If $\langle v\rangle \in V/F^*$, $v \neq 0$, then $\langle v\rangle = F^*v$, so $|\langle v\rangle| = |F^*v| = |F^*| = m-1$. Hence the above formula becomes

$$p_{\langle u\rangle}(\langle v\rangle,\langle w\rangle)=\frac{1}{|F^*|}\sum_{y\in\langle v\rangle}\sum_{z\in\langle w\rangle}p_x(y,z)=\frac{1}{m-1}\sum_{\alpha\in F^*}\sum_{\beta\in F^*}p_x(\alpha v,\beta w)$$

A case by case consideration will give p-values exactly as defined in example 2.5(2).

2.4. Homomorphism. Let A and B be geometries and $f: A \to B$ be a map. Then f is called a morphism if $f(e_A) = e_B$ and $(x, y, z) \in \Delta_A \Rightarrow (f(x), f(y), f(z)) \in \Delta_B$. If, in addition, $(f(x), f(y), b) \in \Delta_B \Rightarrow b = f(z)$ for some $z \in A$ with $(x, y, z) \in \Delta$, then the morphism is called a homomorphism.

Let A, B be probability groups and $f: A \to B$ be a map. Then f is called a probability homorphism if $f(e_A) = e_B$ and

$$p_b(f(a_1),f(a_2))=\sum_{x\in f^{-1}(b)}p_x(a_1,a_2)\ \forall a_1,a_2\in A, b\in B.$$

A homomorphism of probability groups is naturally a homomorphism of corresponding geometries. A bijective homomorphism is an isomorphism. So a bijective f is an isomorphism if and only if $p_a(b,c) = p_{f(a)}(f(b), f(c))\ \forall a, b, c \in A$. Note that the context distinguishes p for A and B.

As in geometry, the natural map $A \to A//B$ is a homomorphism if and only if B is normal in A. There are isomorphism theorems for homomorphisms of probability groups similar to those in geometry. A probability group A is said to be of discrete probability type if $\forall a \in A$, there is a finite set F_a with $p_x(a, b) \in F_a\ \forall x, b \in A$. For such we have:

Proposition 2.7. Let A be a probability group of discrete probability type and B,C be subprobability groups of A with C normal in A. Let $B.C = \{x : (b, c, x) \in \Delta$, for some $b \in B, c \in C\}$. The $B.C$ is a subprobability group of A and $B.C//C \cong B//B \cap C$ as probability groups.

In particular, the proposition is true if A is finite.

2.5.Geometry and Probability Spaces over Geometric Skewfields. Let $(A, 0_A, \Delta)$ be an abelian geometry. Suppose, in addition, $(A, .)$ is a semigroup with 1 such that $0 . a = a . 0 = 0$. It is called a geometric ring if $(a, b, c) \in \Delta, x \in A \Rightarrow (ax, bx, cx)$, $(xa, xb, xc) \in \Delta$. It is called a geometrics sfield if $A^* = A - \{0\}$ is a group. Suppose $(V, 0_V, \Delta)$ is an abelian geometry and the geometric sfield A acts on V compatibly as scalars satisfying: $a(bv) = (ab)v$; $0_A . v = a . 0_V = 0_V$; $1 . v = v$; $(u, v, \omega) \in \Delta \Rightarrow$ $(au, av, a\omega) \in \Delta$; $(a, b, c) \in \Delta \Rightarrow (av, bv, cv) \in \Delta$; $(ab, bv, cv) \in \Delta$, $v \neq 0 \Rightarrow (a, b, c) \in \Delta$; $(av, bv, \omega) \in \Delta \Rightarrow \omega = cv$; where $a, b, c \in A$ and $u, v, w \in V$. Then V is said to be a geometric space over geometric sfield A. For such there is a basis and well defined dimension (see[4], [5]). In case V and A have sharp geometries, the geometric space V is a vector space over the usual skewfield A.

If V is a geometric space over a geometric sfield A, then the geometry of orbits V/A^* is projective and so represents a projective space (including degenerate ones).

Now suppose V is a geometric space over A and in addition, (V, p) is a probability group inducing the given geometry. Then we call V a probability space over A if V is A^* - probability group. Hence, $\forall\ u, v, \omega \in V$ and $\forall \alpha \in A^*$, we have

$$p_{\alpha u}(\alpha v, \alpha w) = p_u(v, w)$$

If A is finite, then the projective space V/A^* is a probability group.

2.6. Semi-isomorphism. Let V and W be geometric spaces over geometric sfields A and B respectively. A pair of maps $(\sigma, \hat{\sigma}) : (V, A) \to (W, B)$ is called a semi-isomorphism if $\sigma : V \to W$ is an isomorphism of geometries, $\hat{\sigma} : A \to B$ is an isomorphism of geometric sfields and $\sigma(av) = \hat{\sigma}(a)\, \sigma(v) \forall v \in V, \forall a \in A$.

Suppose, in addition, V and W are probability spaces over A and B respectively. Then $(\sigma, \hat{\sigma})$ is called a semi-isomorphism of probability spaces if $p_u(v, w) =$ $p_{\sigma(u)}(\sigma(v), \sigma(w)) \forall u, v, w \in V$.

3. Elementary abelian probability groups

Let (A,p) be an abelian probability group. Recall that an abelian geometry A is elementary if $\forall a \in A$, the subgeometry $\langle a\rangle$ generated by a is simple in the sense that whenever S is a subgeometry of A and $\{e\} \neq S \subseteq \langle a\rangle$, then $S = \langle a\rangle$ (see [2]). In such a geometry, $\langle a\rangle \neq \langle b\rangle \Rightarrow \langle a\rangle \cap \langle b\rangle = \{e\}$. Now, since B is a subprobability group of A if and only if B is a subgeometry of A, we make the

Definition 3.1 An abelian probability group A is called elementary if it is elementary as a geometry.

Also, the length of the probability group A will mean the length of the corresponding geometry [2].

Lemma 3.2. Let A be a finite elementary abelian probability group of length greater than one. Then

(i) $p_e(a, a^{\#}) = p_e(b,b^{\#})\forall a, b \in A^*$. (ii) $p_a(b, c) = p_{b^{\#}}(c, a^{\#})\forall a, b, c \in A^*$.

Proof: (i) Let $a,b \in A^*$. Suppose $\langle a\rangle \neq \langle b\rangle$. Let $t \in A$ such that $p_t(a,b) \neq 0$, so $(a, b, t^{\#}) \in \Delta$. Since $\langle a\rangle \neq \langle b\rangle$, we have $t \notin \langle a\rangle$, $t \notin \langle b\rangle$. So $\langle a\rangle \cap \langle t\rangle = \{e\}$ and $\langle a,t\rangle = \langle b, t\rangle$. By proposition (2.7), we get

$$\langle a\rangle \cong \langle a\rangle \,//\, \langle a\rangle \cap \langle t\rangle \cong \langle a\rangle.\langle t\rangle \,//\, \langle t\rangle = \langle b\rangle.\langle t\rangle \,//\, \langle t\rangle \cong \langle b\rangle.$$

If the composite map is σ, then $\sigma(a) = b$, so $\sigma(a^{\#}) = b^{\#}$. Hence, $p_e(a, a^{\#}) = p_{\sigma(e)}(\sigma(a), \sigma(a^{\#})) = p_e(b, b^{\#})$. If $\langle a\rangle = \langle b\rangle$, then the length being greater than one, $\exists c \in A^*$ such that $\langle c\rangle \neq \langle a\rangle$. Then, $p_e(a,a^{\#}) = p_e(c,c^{\#}) = p_e(b,b^{\#})$. (ii) It follows from (i) and lemma 2.3 (iii).

Lemma 3.3 Let A be a finite elementary abelian probability group of length greater than 2. Suppose $p_{a_1}(b_1,c_1) \neq 0$, and $p_{a_2}(b_2, c_2) \neq 0$, where $b_1,b_2,c_1,c_2 \in A^*$, $\langle b_1\rangle \neq \langle c_1\rangle$, $\langle b_2\rangle \neq \langle c_2\rangle$. Then, $p_{a_1}(b_1,c_1) = p_{a_2}(b_2,c_2)$.

Proof: In corresponding geometry, we have $(a_1^{\#},b_1,c_1),(a_2^{\#},b_2,c_2) \in \Delta$. Note that $a_1 \neq e$, otherwise it would give $\langle b_1\rangle = \langle c_1\rangle$. Similarly $a_2 \neq e$.

Case (1): $a_2 = a_1$. Suppose first, $b_2 \notin \langle b_1,c_1\rangle$. Then, $(a_1^{\#},b_1,c_1)$, $(a_1^{\#},b_2,c_2) \in \Delta$, so $\exists t \in A$ such that $(t,b_2^{\#},b_1)$, $(t,c_2,c_1^{\#}) \in \Delta$. Note that $t \notin \langle a_1, b_1\rangle$, otherwise $(t,b_2^{\#},b_1) \in \Delta$ would give $b_2^{\#}$ and hence $b_2 \in \langle a_1,b_1\rangle = \langle b_1, c_1\rangle$. So being elementary, we get $\langle t\rangle \cap \langle a_1,b_1\rangle = \{e\} = \langle t\rangle \cap \langle a_1,b_2\rangle$. So by proposition (2.7), we get

$$\langle a_1,b_1\rangle \cong \langle a_1,b_1\rangle // \langle t\rangle \cap \langle a_1,b_1\rangle \cong \langle a_1,b_1\rangle.\langle t\rangle \,//\, \langle t\rangle = \langle a_1,b_2\rangle.\langle t\rangle \,//\, \langle t\rangle \cong \langle a_1,b_2\rangle.$$

Suppose σ is the composite map. If $x \in \langle a_1,b_1\rangle$, then $x \in \langle a_1,b_1\rangle.\langle t\rangle = \langle a_1, b_2\rangle.\langle t\rangle$, so $\exists y \in \langle a_1,b_2\rangle$, $t_1 \in \langle t\rangle$ with $(x, y^{\#}, t_1) \in \Delta$. Since $\langle a_1, b_2\rangle \cap \langle t\rangle = \{e\}$, the elements $y^{\#}$ and t_1 are unique. Chasing the above isomorphism, it easily verifies that $\sigma(x) = y$. In particular, we have $\sigma(a_1) = a_1 = a_2$, $\sigma(b_1) = b_2$, $\sigma(c_1) = c_2$. So, $p_{a_1}(b_1, c_1) = p_{\sigma(a_1)}(\sigma(b_1), \sigma(c_1)) = p_{a_2}(b_2, c_2)$.

Now suppose $b_2 \in \langle b_1,c_1\rangle$. Then $\langle b_1,c_1\rangle = \langle b_2,c_2\rangle$. Since the length of $A > 2$, $\exists b_3$ such that $b_3 \notin \langle b_1,c_1\rangle$. Choose $c_3 \in A$ such that $p_{a_1}(b_3,c_3) \neq 0$. Then, $\langle b_3\rangle \neq \langle c_3\rangle$, otherwise $\langle b_3\rangle = \langle a_1\rangle \subseteq \langle b_1,c_1\rangle$. So from the first part, we get

$$p_{a_1}(b_1,c_1) = p_{a_1}(b_3,c_3) = p_{a_1}(b_2,c_2) = p_{a_2}(b_2,c_2).$$

Case (2): Let a_2 be arbitrary. Since $\langle b_1\rangle \neq \langle c_1\rangle$, either $\langle a_2\rangle \neq \langle b_1\rangle$, or $\langle a_2\rangle \neq \langle c_1\rangle$. We may assume $\langle a_2\rangle \neq \langle b_1\rangle$. Now, $\exists d \in A$ with $p_{b_1^\#}(a_2^\#,d) \neq 0$. By lemma 3.2 (ii), we get $p_{a_1}(b_1,c_1) = p_{b_1^\#}(c_1,a_1^\#)$. Now using case (1), we get

$$p_{b_1^\#}(c_1,a_1^\#) = p_{b_1^\#}(a_2^\#,d) = p_{a_2}(d,b_1) = p_{a_2}(b_2,c_2).$$

Thus in every case $p_{a_1}(b_1,c_1) = p_{a_2}(b_2,c_2)$.

Now, suppose (A,p) is a probability group of length greater than two such that the corresponding geometry is projective. Then the geometry A corresponds to a projective space. Suppose the projective space is of order m so that each line contains $m+1$ points. The following theorem shows that the probability structure on a projective space is unique. This result was proved in [7] by using duality.

Theorem 3.4 *Let (A,p) be a finite probability group such that the induced geometry on A is projective of order m with length $(A) > 2$. Then,*

$$p_a(b,c) = \begin{cases} \delta_a(c) & \text{if } b = e \\ \delta_a(b) & \text{if } c = e \\ \frac{1}{m-1}\delta_b(c) & \text{if } a = e \\ \frac{m-2}{m-1} & \text{if } a = b = c \neq e \\ \frac{1}{m-1} & \text{if } a, b, c \in P \text{ and } a, b, c \text{ are distinct and collinear} \\ 0 & \text{otherwise} \end{cases}$$

Proof: Since A is projective, it is abelian and $(a,a,b) \in \Delta \Rightarrow b = e$ or $b = a$. This implies that $\langle a\rangle = \{e, a\}, \forall a \in A$. So A is elementary abelian.

Now if $b = e$, then $p_a(e,c) = \delta_a(c)$ and if $c = e$, then $p_a(b,e) = \delta_a(c)$ are clear. So suppose $b,c \in A^*$. We consider two cases.

Case (1): $b \neq c$. Then $p_a(b,c) \neq 0$ if and only if $(a,b,c) \in \Delta$. Since A is elementary Abelian, lemma 3.3 gives that $p_a(b,c) = p_x(b,c) \forall x \in A^*$ such that $(x,b,c) \in \Delta$. But $(x,b,c) \in \Delta$ if and only if $x \in L_{bc} - \{b,c\}$, where L_{bc} is the line determined by the points b and c. Since the line L_{bc} has $m+1$ points, the number of $x \in L_{bc} - \{b,c\}$ will be $\{m+1\}-2 = m-1$. So

$$1 = \sum_{x \in A} p_x(b,c) = \sum_{x \in L_{bc}-\{b,c\}} p_x(b,c) = (m-1)\, p_a(b,c).$$

Hence, $p_a(b,c) = \frac{1}{m-1}$.

Case (2): $b = c$. Then $p_a(b, c) \neq 0$ only if $a = b = c$ or $a = e$. Suppose first

$a = b = c$ and $p_a(a, a) \neq 0$. Since length $(A) > 2$, $\exists y \in A^*$ such that $y \neq a$. Let $z \in A$ such that $(a, y, z) \in \Delta$. Clearly $z \neq e, a, y$. So $p_a(y, z) = \frac{1}{m-1}$. Now consider the equation:

$$\sum_{x \in A} p_x(y,z)p_a(a,x) = \sum_{x \in A} p_a(y,x)p_x(z,a)$$

On the left side, $p_a(a, x) = 0$ except for $x = a$ or e. But if $x = e$, then $p_x(y, z) = p_e(y, z) = 0$, since $y \neq z$. So the only nonzero term in the sum is for $x = a$. So Left side $= p_a(y, z)\, p_a(a, a) = \frac{1}{m-1}\, p_a(a, a)$.

Also on the right a, y, z are distinct and collinear, so $p_a(y, x) = p_x(z, a) = \frac{1}{m-1}$ or 0. The number of elements x such that $p_a(y, x) \neq 0$ is $m - 1$ and includes z, but if $x = z$, then $p_z(z, a) = 0$. So the number of elements for which both factors are not zero is $m - 2$. So Right side $= (m-2)\left(\frac{1}{m-1}\right)\left(\frac{1}{m-1}\right) = (m-2)\left(\frac{1}{m-1}\right)^2$.

Thus, $\frac{1}{m-1}\, p_a(a, a) = (m-2)\left(\frac{1}{m-1}\right)^2$ giving $p_a(a, a) = \frac{m-2}{m-1}$.

Finally, suppose $a = e$. Then, we have $p_e(b,b) + p_b(b, b,) = 1$, so $p_e(b,b) = 1 - \frac{m-2}{m-1} = \frac{1}{m-1}$ and the proof is complete.

4. Probability spaces over geometric sfields as orbits of vector spaces

The following theorem establishes uniqueness of the probability structure which induces a given geometric space over a geometric sfield.

Theorem: 4.1 *Let V be a finite geometric space over a geometric sfield A, $\dim_A (V) > 2$. Suppose (V, p) and (V, q) are probability spaces over A inducing the given geometric space over A. Then, $p = q$.*

Proof: Since V is a geometric space over the geometric sfield A, the orbit space V/A^* is a projective space of length greater than 2. Since (V, p) is an A^* –probability group, it gives a probability structure on the orbits V/A^* as follows (cf. 2.3):

$$p_{\langle v_1 \rangle}(\langle v_2 \rangle, \langle v_3 \rangle) = \frac{1}{|A^*|} \sum_{\alpha \in A^*} \sum_{\beta \in A^*} p_{v_1}(\alpha v_2, \beta v_3)$$

Similarly, the A^*–probability group (V,q) gives

$$q_{\langle v_1 \rangle}(\langle v_2, \langle v_3 \rangle) = \frac{1}{|A^*|} \sum_{\gamma \in A^*} \sum_{\delta \in A^*} q_{v_1}(\gamma v_2, \delta v_3)$$

But by (3.4), the two probability structures on the projective space V/A^* must be the same. So

$$\frac{1}{|A^*|} \sum_{\alpha \in A^*} \sum_{\beta \in A} p_{v_1}(\alpha v_2, \beta v_3) = \frac{1}{|A^*|} \sum_{\gamma \in A^*} \sum_{\delta \in A^*} q_{v_1}(\gamma v_2, \delta v_3)$$

i.e

$$\sum_{\alpha \in A^*} \sum_{\beta \in A^*} p_{v_1}(\alpha v_2, \beta v_3) = \sum_{\gamma \in A^*} \sum_{\delta \in A^*} q_{v_1}(\gamma v_2, \delta v_3)$$

Now let $\upsilon_1,\upsilon_2,\upsilon_3 \in V$ be arbitrary. Then $p_{\upsilon_1}(\upsilon_2,\upsilon_3) \neq 0$ if and only if $(\upsilon_2,\upsilon_3,\upsilon_1^{\#}) \in \Delta$ if and only if $q_{\upsilon_1}(\upsilon_2,\upsilon_3) \neq 0$. So let $(\upsilon_2,\upsilon_3,\upsilon_1^{\#}) \in \Delta$. We show $p_{\upsilon_1}(\upsilon_2,\upsilon_3) = p_{\upsilon_1}(\upsilon_2,\upsilon_3)$. We consider the following cases.

Case (1). υ_2,υ_3 are independent over A. Then for any $\upsilon \in span(\upsilon_2,\upsilon_3)$, $\exists$ unique $\alpha, \beta \in A$ such that $(\upsilon, \alpha\upsilon_2, \beta\upsilon_3) \in \Delta$. So, since $p_{\upsilon_1}(\upsilon_2, \upsilon_3) \neq 0$, we get $p_{\upsilon_1}(\alpha\upsilon_2, \beta\upsilon_3) = 0$ except for $\alpha = \beta = 1$. So on the left side of the above equation we get only one nonzero term $p_{\upsilon_1}(\upsilon_2,\upsilon_3)$. Similarly, the right side gives $q_{\upsilon_1}(\upsilon_2,\upsilon_3)$. So, $p_{\upsilon_1}(\upsilon_2,\upsilon_3) = q_{\upsilon_1}(\upsilon_2,\upsilon_3)$.

Case (2). υ_2,υ_3 are dependent. If $\upsilon_2 = 0$ or $\upsilon_3 = 0$, it is obvious. So let $\upsilon_2 \neq 0$, $\upsilon_3 \neq 0$.

Suppose first $\upsilon_1 \neq 0$. Then $\exists v \in V$ such that $\upsilon_1 = \upsilon$, $\upsilon_2 = \alpha\upsilon$, $\upsilon_3 = \beta\upsilon$. So we show $p_\upsilon(\alpha\upsilon, \beta\upsilon) = q_\upsilon(\alpha\upsilon,\beta\upsilon)$. Since $\dim(V) > 2$, $\exists u, w \in V$ independent such that $(u,\omega,\alpha\upsilon^{\#}) \in \Delta$. So by case (1), $p_{\alpha\upsilon}(u, w) = q_{\alpha\upsilon}(u,w) \neq 0$. Also, $p_{\delta\upsilon}(u,w) = q_{\delta\upsilon}(u,w) = 0$ for $\delta \neq \alpha$. In (V, p), we have:

$$\sum_{y\in V} p_y(u,w)p_\upsilon(y,\beta\upsilon) = \sum_{x\in V} p_\upsilon(u,x)p_x(w,\beta\upsilon)$$

But $p_\upsilon(y,\beta\upsilon) \neq 0$ implies $y = \gamma\upsilon$ for some $\gamma \in A$ and $p_{\gamma\upsilon}(u, w) \neq 0$ only when $\gamma = \alpha$. Hence the above equality gives

$$p_{\alpha\upsilon}(u,w)\, p_\upsilon(\alpha\upsilon, \beta\upsilon) = \sum_{x\in V} p_\upsilon(u,x)p_x(w,\beta\upsilon)$$

Similarly we get for q:

$$q_{\alpha\upsilon}(u,w)\, q_\upsilon(\alpha\upsilon, \beta\upsilon) = \sum_{x\in V} q_\upsilon(u,x)q_x(w,\beta\upsilon)$$

Since u,υ are independent $p_\upsilon(u,x) \neq 0$ implies u,x are also independent. So by case (1), $p_\upsilon(u,x) = q_\upsilon(u,x)\ \forall\, x \in V$. Similarly, $p_x(w,\beta\upsilon) = q_x(w,\beta\upsilon)\ \forall\, x \in V$. So the right sides of the above equalities are equal giving the equality of the left sides:

$$p_{\alpha\upsilon}(u,w)\, p_\upsilon(\alpha\upsilon,\beta\upsilon) = q_{\alpha\upsilon}(u,w)\, q_\upsilon(\alpha\upsilon,\beta\upsilon)$$

But again, $p_{\alpha\upsilon}(u,w) = q_{\alpha\upsilon}(u,w) \neq 0$. So we eventually get $p_\upsilon(\alpha\upsilon,\beta\upsilon) = q_\upsilon(\alpha\upsilon,\beta\upsilon)$. Finally, let $\upsilon_1 = 0$. Then, $1 = \sum_x p_x(v_2,v_3) = \sum_x q_x(v_2,v_3)$. Since $p_x(\upsilon_2,\upsilon_3) = q_x(\upsilon_2,\upsilon_3)$ $\forall x \neq 0$, we must have $p_0(\upsilon_2, \upsilon_3) = q_0(\upsilon_2,\upsilon_3)$. Thus $p = q$.

Now suppose V is a vector space over a finite field F, $\dim(V) \geq 3$ and Γ is a subgroup of F^*. Then the orbit spaces V/Γ and F/Γ are probability groups in a natural way (cf. 2.3). It can easily be seen that the probability group V/Γ so defined is F^*/Γ - probability group. So the theorem gives:

Corollary 4.2. Let V be a finite dimensional vector space over a finite field F and Γ be a subgroup of F^*. Then the space V/Γ is a probability space over F/Γ in a unique (natural) way.

Definition 4.3. We call a geometric space V over a geometric sfield A to be of *finite order type* if the corresponding projective space $P(V)$ is of finite order.

The following theorem gives the representation of a probability space over a geometric space as orbits of a vector space.

Theorem 4.4. *Suppose (V, p) is a probability space of finite dimension over a geometric sfield A with $\dim_A V \geq 4$. Suppose V is of finite order type. Then there is a finite dimensional vector space W over a finite F, a subgroup Γ of F^* and a semi-isomorphism of probability spaces:*

$$(\psi, \hat{\psi}) : (W/\Gamma, F/\Gamma) \to (V, A)$$

The same is true if $\dim_A V = 3$ and the geometry of V is D-geometry.

Proof : Since V is a geometric space over the geometric sfield A with proper dimension, there is a vector space W over a skewfield F, a normal subgroup Γ of F^* and a semi-isomorphism of geometric spaces $(\psi, \hat{\psi}) : (W/\Gamma, F/\Gamma) \to (V, A)$ (see [5]). We show that it is a semi-isomorphism of probability spaces. Since V is of finite order type, the projective space $P(W)$ is of finite order and so F is a finite field. So W and hence V is finite. We use the isomorphism ψ to make W/Γ into a probability space as follows:

$$p_{\tilde{u}}(\tilde{v}, \tilde{w}) = p_{\psi(\tilde{u})}(\psi(\tilde{v}), \psi(\tilde{w})), \forall \tilde{u}, \tilde{v}, \tilde{w} \in W/\Gamma.$$

We have for $\tilde{a} \in F^*/\Gamma$, $p_{\tilde{a}\tilde{u}}(\tilde{a}\tilde{v}, \tilde{a}\tilde{w}) = p_{\hat{\psi}(\tilde{a})\psi(\tilde{u})}(\hat{\psi}(\tilde{a})\psi(\tilde{v}), \hat{\psi}(\tilde{a})\psi\tilde{w}))$

$$= p_{\psi(\tilde{u})}(\psi(\tilde{v}), \psi(\tilde{w})) = p_{\tilde{u}}(\tilde{v}, \tilde{w}),$$

as V is A^*-probability group. So this makes W/Γ into F^*/Γ - probability group. But by corollary 4.2, such probability structure is uniquely the natural probability structure of W/Γ.

Hence the theorem is proved.

5. Elementary abelian probability groups as orbits of groups

The following theorem gives orbit space representation of probability groups, which are elementary abelian.

Theorem 5.1 *Suppose A is a finite elementary abelian probability group, length $(A) \geq 4$. Then there exists a vector space V over a finite field F and a subgroup Γ of F^* such that $A \cong V/\Gamma$ as probability groups.*

If length $(A) = 3$, then the same is true if A is a D-geometry.

Proof: Since A is elementary abelian geometry of proper length, there is a vector space V over a skewfield F and a subgroup Γ of F^* such that $\sigma : V/\Gamma \to A$ is an isomorphism of geometries which induces isomorphism of projective spaces $P(V)$ and $P(A)$ (see [2]). We show that σ is an isomorphism of probability groups.

Since A is finite, the projective space $P(A)$ and hence $P(V)$ has finite order. So F is finite and hence a held. Then, V/Γ is a geometric space over F/Γ. We make V/Γ a probability group by defining p as follows:

$$p_x(y, z) = p_{\sigma(x)}(\sigma(y), \sigma(z)) \forall x, y, z \in V/\Gamma.$$

The probability group $(V/\Gamma, p)$ so defined is isomorphic to (A, p). To show that it is the natural probability group, it is sufficient to show that V/Γ is F^*/Γ-probability group. So, let $\alpha \in F/\Gamma$, $\alpha \neq 0$. We show $p_{\alpha x}(\alpha y, \alpha z) = p_x(y, z) \forall x, y, z \in V/\Gamma$. It is obvious if $x = 0$, or $y = 0$, or $z = 0$. So let $x, y, z \in (V/\Gamma)^*$. Suppose first y, z are independent. This means in $P(V)$, $\langle y \rangle \neq \langle z \rangle$, so in $P(A)$, $\langle \sigma(y) \rangle \neq \langle \sigma(z) \rangle$. Similarly, $\langle \sigma(\alpha y) \rangle \neq \langle \sigma(\alpha z) \rangle$. So by lemma 3.3, $p_{\sigma(x)}(\sigma(y), \sigma(z)) = p_{\sigma(\alpha x)}(\sigma(\alpha y), \sigma(\alpha z))$, showing that $p_x(y, z) = p_{\alpha x}(\alpha y, \alpha z)$. Now suppose y, z are dependent. They $y = \beta x$, $z = \gamma x$. Choose $t \in V/\Gamma$ with x, t independent. Then, as in lemma 3.2, $\langle x \rangle \equiv \langle t \rangle \equiv \langle \alpha x \rangle$, the composite isomorphism being given by $x \to \alpha x$. So for $\beta x, \gamma x \in \langle x \rangle$, we get $p_x(\beta x, \gamma x) = p_{\alpha x}(\alpha\beta x, \alpha\gamma x) = p_{\alpha x}(\alpha y, \alpha z)$.

Thus, (V,p) is the natural probability group and $\sigma: V/\Gamma \to A$ is the required isomorphism.

Now since a vector space over a finite field of characteristic, say p, is a vector space over Z_p, and hence is a finite elementary abelian p-group, we may restate

Theorem 5.2. *A finite elementary abelian probability group of length greater than three is isomorphic to the probability group of orbits of a finite elementary abelian p-group with respect to a finite group of automorphisms.*

Acknowledgement

This paper was partly prepared while visiting the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy as an associate. Financial support from the Swedish International Development Cooperation Agency is appreciated.

REFERENCES

[1.] Bhattarai, H.N. and Fernandez, J.W., Join of Double Coset Spaces, *Pacific J. Math.* 98(2) (1982).

[2.] Bhattarai, H.N., An Orbit Space Representation of A Geometry, *J. Algebra* 84(1) (1983), 142–150.

[3.] _____, Categories of Projective Geometries with Morphisms and Homomorphisms, *Geometriae Dedicata* 78(1999), 111–120.

[4.] _____, Pasch geometric spaces inducing finite projective planes, *J. Geometry* 34(1989), 6–13.

[5.] _____, Pasch Geometric Spaces as Orbits of Vector Spaces, *Nep. Math. Sc. Report*, 20(2003).

[6.] Dresher, M. and Ore, O., Theory of Multigroups, *Amer. J. Math.* 60(1938).

[7.] Harrison, D.K., Double Cosets and Orbit Spaces, *Pacific J. Math.* 80(2), 451–491.

[8.] Jewett, R.I., Spaces with an Abstract Convolution of Measures, *Advances in Math.*18(2) (1975), 1–101.
[9.] Prenowitz, W., Projective Geometries as Multigroups, *Amer. J. Math.* 65(1943).
[10.] Roth, R.L., Character and Conjugacy Class Hypergroups, *Annali Di Mat. Pura Ed Appl.*, 55(1975).

H.N. BHATTARAI
Cerntral Department of Mathematics,
Tribhuvan University, Kathamandu, Nepal

The Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

Present Address
University Grants Commision, P.O. Box 10796,
Kathmandu, Nepal,