Algebra and Discrete Mathematics RESEARCH ARTICLE
Number 2. **(2008).** pp. 123 – 129

Random walks on finite groups converging after finite number of steps

A.L. Vyshnevetskiy, $\boxed{\text{E. M. Zhmud'}}$

Communicated by B. V. Novikov

Abstract. Let P be a probability on a finite group G, $P^{(n)} = P * \ldots * P$ (n times) be an n-fold convolution of P. If $n \to \infty$, then under mild conditions $P^{(n)}$ converges to the uniform probability $U(g) = \frac{1}{|G|}$ ($g \in G$). We study the case when the sequence $P^{(n)}$ reaches its limit U after finite number of steps: $P^{(k)} = P^{(k+1)} = \cdots = U$ for some k. Let $\Omega(G)$ be a set of the probabilities satisfying to that condition. Obviously, $U \in \Omega(G)$. We prove that $\Omega(G) \neq U$ for "almost all" non-Abelian groups and describe the groups for which $\Omega(G) = U$. If $P \in \Omega(G)$, then $P^{(b)} = U$, where b is the maximal degree of irreducible complex representations of the group G.

Let G be a finite group, P be a probability on G, $P^{(n)} = P * \ldots * P$ (n times) be an n-fold convolution of probability P. If $n \to \infty$, then under well known conditions (see for example [1]), the sequence $P^{(n)}$ converges to the uniform probability U, where $U(g) = \frac{1}{|G|}$ ($g \in G$).

In this paper we study the case when the sequence $P^{(n)}$ reaches its limit U after some finite number of steps:

$$P^{(k)} = P^{(k+1)} = \cdots = U \tag{1}$$

($k \in \mathbf{N}$ where $\mathbf{N}$ is the set of natural numbers). The set $\Omega(G)$ of the probabilities satisfying (1) is not empty as $U \in \Omega(G)$. It turns out that probabilities from $\Omega(G)$ are tightly connected with nilpotent elements of the group algebra $\mathbf{R}G$ of the group G over the field $\mathbf{R}$ of real numbers and that such probabilities exist for "almost all" non-Abelian groups.

2000 Mathematics Subject Classification: *20P05, 60B15.*
Key words and phrases: *random walks on groups, finite groups, group algebra.*

The main result of the paper is the following.

Theorem. For a finite group G the following conditions are equivalent:

(a) $\Omega(G) = U$;

(b) G is either an Abelian group or Hamiltonian 2-group, i.e. $G = A \times Q$ where A is an elementary Abelian 2-group, Q is the quaternion group of order 8;

(c) The zero is the only nilpotent element of the algebra $\mathbf{R}G$.

1. The set $\Omega(G)$

In what follows we write $\sum_g$ instead of $\sum_{g\in G}$.

The set $F(G)$ of all functions $G \to \mathbf{R}$ is an algebra over $\mathbf{R}$ with respect to operations of addition and convolution

$$F_1 * F_2(h) = \sum_g F_1(hg^{-1})F_2(g), \qquad F_1, F_2 \in F(G)$$

A map $\varphi : F \to f = \sum_g F(g)g$ is an isomorphism of this algebra on the group algebra $\mathbf{R}G$. We denote functions from $F(G)$ by capital letters and their φ-images by corresponding small letters: if $F \in F(G)$, then $\varphi(F) = f$. For example, $\varphi(U) = u = \frac{1}{|G|}\sum_g g$.

A probability on G is a non-negative function $P : G \to \mathbf{R}$ such that $\sum_g P(g) = 1$.

Let $\Pi(G)$ be the set of all probabilities on a group G. For an arbitrary element $x = \sum_g X(g)g \in \mathbf{R}G$ we denote $|x| = \sum_g X(g)$. If $P \in \Pi(G)$, then $|p| = 1$.

For any $x, y \in \mathbf{R}G$ we have

$$|x + y| = |x| + |y|, \quad |x - y| = |x| - |y| \tag{2}$$

As

$$xu = ux = |x|u \tag{3}$$

and $xyu = xyu^2 = xu \cdot yu$, we have

$$|xy| = |x| \cdot |y| \tag{4}$$

Let $Nil(A)$ be the set of all nilpotent elements of an arbitrary algebra A.

Lemma 1.1. $|x| = 0$ for each $x \in Nil(A)$.

Proof. As $x^k = 0$ for some $k \in \mathbf{N}$, then $0 = |x^k| = |x|^k$ by (4), so $|x| = 0$.

Lemma 1.2. If $P \in \Pi(G)$ and $x = p - u$, then $p^n = x^n + u$ for any $n \in \mathbf{N}$.

Proof. As $|x| = |p| - |u| = 0$, then by (3) $xu = ux = 0$. Under the binomial formula, $p^n = (x + u)^n = x^n + u^n = x^n + u$.

Corollary 1.3. $P \in \Omega(G)$ if and only if $x \in Nil(\mathbf{R}G)$.

Proof. $P \in \Omega(G)$ if and only if $p^n = u$ for the some $n \in \mathbf{N}$.

Theorem 1.4. If $P \in \Omega(G)$, then $P^{(b)} = U$, where b is the maximal degree of irreducible representations of G over the field $\mathbf{C}$ of complex numbers.

Proof. By Lemma 1.2 it is enough to prove that $x^b = 0$, where $x = p - u$. For this purpose, in turn, it is enough to prove that $\Gamma(x^b) = 0$ for any irreducible $\mathbf{C}$-representation Γ of group G, extended by linearity to the group algebra $\mathbf{C}G$.

Let n be the degree of a representation Γ, $F(t)$ be the characteristic polynomial of a matrix $\Gamma(x)$. As $\deg F(t) = n$ and matrix $\Gamma(x)$ is nilpotent by Corollary 1.3, then $F(t) = t^n$. By Hamilton-Cayley theorem $(\Gamma(x))^n = 0$, and as $n \le b$, then $\Gamma(x^b) = (\Gamma(x))^b = 0$. The theorem is proved.

If $P \in \Pi(G)$, then $P * U = U$. Therefore condition (1) is equivalent to $P^{(n)} = U$ for some $n \in \mathbf{N}$. By Theorem 1.4 condition (1) for $k = b$ holds for any probability $P \in \Omega(G)$.

A function X on a group G is called a class function if X is constant on each class of conjugate elements of G. For a class function X its φ-image x is in the center $Z(\mathbf{R}G)$ of the algebra $\mathbf{R}G$.

Lemma 1.5. If $P \in \Omega(G)$ is a class function, then $P = U$.

Proof. Let $x = p - u$. As $p, u \in Z(\mathbf{R}G)$, then $x \in Z(\mathbf{R}G)$. By Corollary 1.3 $x \in Nil(\mathbf{R}G)$, so $xy \in Nil(\mathbf{R}G)$ for any $y \in \mathbf{R}G$. Therefore the principal ideal of algebra $\mathbf{R}G$, generated by element x, is nilpotent. As $\mathbf{R}G$ is semisimple, then $x = 0$, i.e. $P = U$.

For $f \in \mathbf{R}G$ and $a \in \mathbf{R}$ we write $f \ge a$ if $F(g) \ge a$ for any $g \in G$ (we recall that $F = \varphi^{-1}(f)$, see the first paragraph of this section).

Let $N(G) = \{x \in Nil(\mathbf{R}G) \mid x \ge -\frac{1}{|G|}\}$. Since $Nil(\mathbf{R}G) = \{\mathbf{R}x \mid x \in N(G)\}$, then

$$Nil(\mathbf{R}G) = \{0\} \Leftrightarrow N(G) = \{0\}. \tag{5}$$

Theorem 1.6. There is a bijection $\theta : N(G) \to \Omega(G)$.

Proof. For $x \in N(G)$ we let $\theta_1 : x \to x + u$. Then $\theta_1(x) \geq 0$ by definition of $N(G)$; by (2) and Lemma 1.1 $|\theta_1(x)| = |x| + |u| = 1$. Let $\theta = \varphi^{-1} \cdot \theta_1$ (composition of mappings); then $\theta(x) \in \Pi(G)$. Since $x = \theta_1(x) - u \in Nil(\mathbf{R}G)$, then by Corollary 1.3 $\theta(x) \in \Omega(G)$. So $\theta(N(G)) \subset \Omega(G)$.

Since φ is a bijection and θ_1 is an injection, then θ is an injection. Let $P \in \Omega(G)$ and $x = p - u$. By Corollary 1.3 $x \in Nil(\mathbf{R}G)$. Since $p \geq 0$, then $x \geq -\frac{1}{|G|}$. So $x \in N(G)$. Since $p = \theta_1(x)$, then $P = \varphi^{-1}(p) = \theta(x)$. So θ is a surjection. Thus θ is a bijection.

The proof of Theorem 1.6 gives a way to obtain every probability of $\Omega(G)$: for $x \in N(G)$ a function $P = \varphi^{-1}(x + u)$ is in $\Omega(G)$ and any $P \in \Omega(G)$ can be obtained this way.

Now we name the groups we study.

Definition. A group is called S-group if $\Omega(G) = \{U\}$.

2. Description of S-groups

Let $M_n(K)$ be the algebra of all $n \times n$ matrices over a skew field K.

Lemma 2.1. $Nil(M_n(K)) = \{0\}$ if and only if $n = 1$, i.e. $M_n(K) = K$.

Proof. If $n = 1$, then $M_n(K) = K$ is a skew field, so $Nil(M_n(K)) = \{0\}$. If $n > 1$, matrix units E_{ij} are nilpotent if $i \neq j$ (E_{ij} is a matrix which (i, j)-th element is 1 and others are 0).

The following theorem is a key one.

Theorem 2.2. The following conditions are equivalent:

(a) G is a S-group;

(b) $Nil(\mathbf{R}G) = \{0\}$;

(c) The algebra $\mathbf{R}G$ is an orthogonal direct sum of skew fields.

Proof. (a) $\Leftrightarrow$ (b). By definition, the statement (a) means that $|\Omega(G)| = 1$. By Theorem 1.6 it is equivalent to $|N(G)| = 1$, i.e. $N(G) = \{0\}$. By (5) it means that $Nil(\mathbf{R}G) = \{0\}$.

(b) $\Leftrightarrow$ (c). By Wedderburn's theorem algebra $\mathbf{R}G$ decomposes into orthogonal direct sum of matrix algebras over skew fields. The equality $Nil(\mathbf{R}G) = \{0\}$ is equivalent to $Nil(M_n(K)) = \{0\}$ for each of such algebras $M_n(K)$, and by Lemma 2.1, to $M_n(K) = K$.

Note 2.3. For a S-group G let a skew field K be one of direct summands of $\mathbf{R}G$ (see point (c) of Theorem 2.2). As K is a finite-dimensional algebra over $\mathbf{R}$, then by well known theorem of Frobenius ([2], p. 465), K is isomorphic either to field $\mathbf{R}$, or to field $\mathbf{C}$ of complex numbers, or to quaternion skew field $\mathbf{Q}$.

Lemma 2.4. Subgroups of an S-group are S-groups.

Proof. Let H be a subgroup of S-group G. By Theorem 2.2 we have $Nil(\mathbf{R}G) = \{0\}$. As $Nil(\mathbf{R}H) \subset Nil(\mathbf{R}G)$, then by Theorem 2.2 H is S-group.

Let $Z(G)$ be the center of G.

Lemma 2.5. If $x \in Nil(\mathbf{R}G)$, then $X(g) = 0$ for any $g \in Z(G)$.

Proof. Let T be the regular representation of a group G, ρ be its character, extended by linearity on algebra $\mathbf{R}G$. As $\rho(g) = 0\,(g \neq 1)$ and $\rho(1) = |G|$, then

$$\rho(x) = \sum_g X(g)\rho(g) = X(1)|G|$$

On the other hand, the matrix $T(x)$ is nilpotent, so $\rho(x) = \mathrm{tr}\,(T(x)) = 0$. Therefore $X(1) = 0$, and lemma is proved for special case $g = 1$.

For proof in general case we let $y = g^{-1}x$. Then $y \in Nil(\mathbf{R}G)$. By the above paragraph $Y(1) = 0$. As $Y(1) = X(g)$, the proof is complete.

Corollary 2.6. Abelian groups are S-groups.

Proof. For an Abelian group G we have $G = Z(G)$, so $Nil(\mathbf{R}G) = \{0\}$. By Theorem 2.2, G is S-group.

Another proof we obtain from Lemma 1.5, since any function on Abelian group is a class function.

A non-Abelian group is called Hamiltonian if all its subgroups are normal.

Lemma 2.7. ([3], p. 308). A group G is Hamiltonian if and only if

$$G = N \times A \times Q, \tag{6}$$

where N is an Abelian group of odd order, A is an elementary Abelian 2-group, Q is the quaternion group of order 8.

Let G be a Hamiltonian S-group. As its subgroup N is Abelian, then algebra $\mathbf{R}N$ decomposes into an orthogonal direct sum of fields:

$$\mathbf{R}N = \Lambda_1 \oplus \ldots \oplus \Lambda_r \tag{7}$$

Lemma 2.8. We have

(a) $\Lambda_i \cong \mathbf{R}$ $(i = 1, \ldots, r)$;

(b) G is a 2-group.

Proof. (a) If statement (a) does not hold, then by note 2.3, $\Lambda_i \cong \mathbf{C}$ for some i. The algebra $\mathbf{R}Q$ is an orthogonal direct sum of skew fields, and as the group Q is non-Abelian, then one of these skew fields (say, K) is isomorphic to the quaternion skew field $\mathbf{Q}$. By (6) the algebra $\mathbf{R}Q$ contains an ideal $I = \Lambda_i \cdot K \cong \mathbf{C} \otimes \mathbf{Q}$. As the ring $\mathbf{C} \otimes \mathbf{Q}$ is isomorphic to the full matrix ring $M_2(\mathbf{C})$ and $Nil(M_2(\mathbf{C})) \neq 0$ (Lemma 2.1), then $Nil(I) \neq 0$ whence $Nil(\mathbf{R}G) \neq 0$. As it contradicts to Theorem 2.2, the statement (a) is proved.

(b) By (6) it is enough to prove that $N = \{1\}$. By (7), an arbitrary element $g \in N$ has decomposition $g = x_1 + \cdots + x_r$, where $x_i \in \Lambda_i$ $(i = 1, \ldots, r)$. Let $n = |N|$. Elements x_i are mutually orthogonal, so $1 = g^n = {x_1}^n + \cdots + {x_r}^n$. As $1 = e_1 + \cdots + e_r$, where e_i is the unit of Λ_i, then ${x_i}^n = e_i$ $(i = 1, \ldots, r)$. Therefore x_i is an element of finite order in the multiplicative group of the field Λ_i. As $\Lambda_i \cong \mathbf{R}$, then $x_i = \pm e_i$ $(i = 1, \ldots, r)$ and $g^2 = {x_1}^2 + \cdots + {x_r}^2 = 1$. But N is a group of odd order, so $g = 1$, therefore $N = \{1\}$.

Theorem 2.9. The following conditions are equivalent:

(a) G is a Hamiltonian 2-group;

(b) G is a non-Abelian S-group.

Proof. (a)$\Rightarrow$(b) Let G be a Hamiltonian 2-group. By Lemma 2.7 $G = A \times Q$, therefore $Z(G) = A \times Z(Q)$. For any $s \in G \setminus Z(G)$ we have $s = at$, where $a \in A$, $t \in Q \setminus Z(Q)$. So $s^2 = a^2 t^2 = t^2 = z$, where z is the unique element of order 2 in group Q.

Let $y \in Nil(\mathbf{R}G)$. If $y \neq 0$, then $y^n = 0$, $y^{n-1} \neq 0$ for the some $n \in \mathbf{N}$. Let $x = y^{n-1}$; then $x^2 = 0$, $x \neq 0$. Therefore

$$\sum_s X(s)X(s^{-1}g) = 0 \tag{8}$$

for any $g \in G$. By Lemma 2.5 we can assume that in (8) $s \in G \setminus Z(G)$ instead of $s \in G$. Then by above $s^2 = z$. Substituting in (8) $g = z$ we obtain $\sum_s (X(s))^2 = 0$, whence $X(s) = 0$ for any $s \in G \setminus Z(G)$. Again by Lemma 2.5 $X(s) = 0$ for $s \in Z(G)$, so $X = 0$ i.e. $x = 0$ — a contradiction. Therefore $Nil(\mathbf{R}G) = \{0\}$ and G is a S-group.

(b)⇒(a) Let G be a non-Abelian 2-group. For arbitrary elements $g, s \in G$ we let

$$\nu = (g-1)s(g^{n-1} + g^{n-2} + \cdots + g + 1) \in \mathbf{R}G$$

where n is order of the element $g \in G$. Since $(g-1)(g^{n-1} + g^{n-2} + \cdots + g+1) = g^n - 1 = 0$, we have $\nu^2 = 0$. By Theorem 2.2 $Nil(\mathbf{R}G) = \{0\}$, so $\nu = 0$. As $\nu = gsg^{n-1} + \cdots + gs - sg^{n-1} - \cdots - s$, then $gs = sg^k$ for some $k \in \{0, 1, \ldots, n-1\}$. Therefore $s^{-1}gs = g^k$. So the subgroup generated by g is normal in G. It yields that each subgroup of G is normal, i.e. G is Hamiltonian. By the statement (b) of Lemma 2.8, G is a 2-group. Theorem is proved.

As a consequence of Theorems 2.2 and 2.9 we obtain

Theorem 2.10. For a finite group G the following conditions are equivalent:

(a) $\Omega(G) = U$;

(b) G is an Abelian group or a Hamiltonian 2-group;

(c) The zero is the only nilpotent element of the algebra $\mathbf{R}G$.

References

[1] Saloff-Coste L. Random walks on finite groups. In: Probability on Discrete structures, H Kesten (editor), Springer, 2004.

[2] Huppert B. Endliche Gruppen I. Springer-Verlag, Berlin, 1967.

[3] Vinberg E.B. A course in algebra. AMS, Providence, 2003.

Contact information

A. L. Vyshnevetskiy Karazina st. 7/9, apt. 34, 61078, Kharkov, Ukraine
E-Mail: alexwish@mail.ru