COLLOQUIUM MATHEMATICUM

Online First version

CONDITIONS OF CONVERGENCE OF A RANDOM WALK ON A FINITE GROUP

BY

A. L. VYSHNEVETSKIY (Kharkiv)

Abstract. Let P be a probability on a finite group G, and V its carrier. Conditions of convergence of the n-fold convolution $P^{(n)}$ to the uniform probability on G ($n \to \infty$) in terms of V are known. We consider conditions under which the carrier V^n of the probability $P^{(n)}$ converges as $n \to \infty$, i.e. $V^n = V^{n+1} = \cdots$ for n large. The convergence of V^n is equivalent to the convergence of $P^{(n)}$. Instead of G one can take its subgroup $\langle V \rangle$, generated by V. Then V^n does not converge if and only if V lies in a non-identity coset in $\langle V \rangle$ of a normal subgroup with a cyclic factor group. The article can be considered as a study of the behavior of the powers V^n of a subset V of a finite group as $n \to \infty$.

1. Introduction. Let P be a probability on a finite group G, and $P^{(n)} = P * \cdots * P$ the n-fold convolution of the function P. Numerous works have been devoted to evaluation of the speed of convergence of $P^{(n)}$ to the uniform (trivial) probability on G as $n \to \infty$ (see, e.g., the review [3]). For topological groups the problem can be reduced to the above mentioned problem of behavior of convolutions on finite groups [1].

A necessary and sufficient condition for the convergence is known [2]: the carrier V of the probability P must not lie in a non-identity coset in G of any subgroup (of G). We consider conditions under which the carrier V^n of $P^{(n)}$ stabilizes (converges) as $n \to \infty$, i.e. $V^n = V^{n+1} = \cdots$ for sufficiently large n. Such conditions are of interest because convergence of V^n is equivalent to convergence of $P^{(n)}$ (Corollary 2.13). It is proved that as $n \to \infty$ the carrier V^n of $P^{(n)}$ does not converge if and only if V lies in a non-identity coset in G, generated by the set V, of a normal subgroup with a cyclic factor group.

As the carrier V of a probability on a finite group can be any non-empty subset of the group, the results of this work can be considered as regarding the behavior of powers V^n of any non-empty subset of a finite group as $n \to \infty$.

2020 *Mathematics Subject Classification*: Primary 60B15, 60B10; Secondary 20D99.
Key words and phrases: probability, finite group, convergence, convolution.
Received 8 March 2020.
Published online 12 May 2021.

DOI: 10.4064/cm8196-5-2020

2. Conditions of convergence. Let $\mathbb{N}$ be the set of all natural numbers, $n \in \mathbb{N}$, V a non-empty subset of a finite group G, and $S = \langle V \rangle$ the subgroup generated by the set V.

LEMMA 2.1. *There exists $r \in \mathbb{N}$ such that $|V^n| = |V^r|$ for all $n > r$.*

Proof. Since the subset $V^k g \subset V^{k+1}$ ($k \in \mathbb{N}$) contains $|V^k|$ different elements, we have $|V| \le |V^2| \le \cdots$. Therefore, the statement follows from the finiteness of G. ∎

LEMMA 2.2. *There exists $l \in \mathbb{N}$ with $l > r$ such that $1 \in V^l$.*

Proof. Since the group S is finite, we have

$$S = \bigcup_{n \in \mathbb{N}} V^n. \tag{2.1}$$

Hence $1 \in V^n$ for some $n \in \mathbb{N}$. So $1 \in V^{nk}$ for any $k \in \mathbb{N}$. Choosing k such that $nk > r$, we get $1 \in V^l$ with $l = nk$. ∎

By Lemma 2.2,

$$V^m = V^m \cdot 1 \subset V^m \cdot V^l = V^{m+l} \tag{2.2}$$

for any $m \in \mathbb{N}$. In particular, for $m = 1$ we get

$$V \subset V^{l+1}. \tag{2.3}$$

By (2.2), the terms with $n < l$ in (2.1) can be omitted:

$$S = \bigcup_{m=0}^{\infty} V^{l+m}. \tag{2.4}$$

LEMMA 2.3. *If $g \in V^m$ ($m \in \mathbb{N}$), then*

$$V^{l+m} = V^l g, \quad V^{l+m} = g V^l. \tag{2.5}$$

Proof. Since $l > r$, we have $l + m > r$ and by Lemma 2.1, $|V^{l+m}| = |V^l|$ ($= |V^r|$). Since $|V^l g| = |V^l|$, we get $|V^{l+m}| = |V^l g|$. Therefore, from $V^l g \subset V^l V^m = V^{l+m}$ we obtain the first of the equalities (2.5). The second is proved similarly.

THEOREM 2.4.

(a) $V^l \lhd S$.
(b) *V^{l+m} is a coset of the subgroup V^l of S ($m = 0, 1, \ldots$).*

Proof. (a) Since $1 \in V^l$, in (2.5) we can put $g = 1$ and $m = l$. Then from (2.5) we get $(V^l)^2 = V^l$, i.e. V^l is closed under multiplication. Since V^l is a subset of the finite group S, it is a subgroup of S. Moreover, if $g \in S$, then by (2.1), $g \in V^m$ for some m. Therefore from (2.5) we get $gV^l = V^l g$ for any $g \in S$, i.e. $V^l \lhd S$.

(b) For $m = 0$ the statement is obvious. For an arbitrary $m \in \mathbb{N}$ we choose $g \in V^m$. Then (2.5) is fulfilled. The theorem is proved. ∎

Let $D = \{n \in \mathbb{N} \mid V^n \subset V^l\}$. Since V^l is a group, $m_1, m_2 \in D$, $m_1 \geq m_2$ implies $m_1 - m_2 \in D$. Therefore, the remainder of dividing an arbitrary number from D by the smallest number $d \in D$ is zero, i.e.

$$D = \{dm \mid m \in \mathbb{N}\}. \tag{2.6}$$

Since $l \in D$, we have $d \mid l$.

THEOREM 2.5. *The sequence* $\{V^l, V^{l+1}, \ldots\}$ *has the least period* d. *The cosets* $V^l, V^{l+1}, \ldots, V^{l+d-1}$ *are different.*

Proof. Put by definition $V^0 = \{1\}$. Let $n, m \in \mathbb{N}$ with $n \geq m > l$. Then V^n, V^m are cosets of the subgroup V^l of G. Therefore $V^n = V^m$ if and only if $V^{n-m} \subset V^l$, i.e. $n - m \in D$. In view of (2.6), this is equivalent to $n \equiv m \pmod{d}$. This proves both the statements of the theorem. ∎

From (2.4) and Theorem 2.5 we obtain

COROLLARY 2.6. $S = \bigcup_{k=0}^{d-1} V^{l+k}$ *is a decomposition* S *into cosets of the subgroup* V^l.

Let the bar over a subset of S denote its image under the natural homomorphism $S \to \overline{S} = S/V^l$.

COROLLARY 2.7. $\overline{S}$ *is a cyclic group of order* d.

Proof. The congruence $(V^{l+1})^k \equiv V^{l+k} \pmod{V^l}$ is obvious for $k = 0$, and for $k \in \mathbb{N}$ it follows from $(V^{l+1})^k = V^{(k-1)l} V^{l+k}$. Therefore, by the previous corollary, the cosets $(V^{l+1})^k$ $(k = 0, 1, \ldots, d-1)$ exhaust all elements of the group S , i.e. $\langle \overline{V^{l+1}} \rangle = \overline{S}$.

THEOREM 2.8. *The order of every element of* V *is divisible by* d.

Proof. Let f be the order of $v \in V$. Since by (2.2), $V^f \subset V^{f+l}$, we have $1 = v^f \in V^f \subset V^{f+l}$. Since $1 \in V^l$, it follows that $V^l \cap V^{l+f} \neq \emptyset$. Since V^{l+f} is a coset of the subgroup V^l of S, we have $V^f = V^{f+l}$. Since $V^f \subset V^{f+l}$, we get $V^f \subset V^l$, i.e. $f \in D$. By (2.6), $d \mid f$. ∎

COROLLARY 2.9. *If* V *contains a subset of elements whose orders have no common prime factor, then* $d = 1$. *In particular,* $d = 1$ *if* $1 \in V$.

For any subset $M \in S$ put $M^{-1} = \{x^{-1} \mid x \in M\}$, $M^S = \{s^{-1}xs \mid x \in M, s \in S\}$ and $\langle\langle M \rangle\rangle = \langle M^S \rangle$. Note that $\langle\langle M \rangle\rangle$ is the smallest normal subgroup of S containing M.

Let $T = \langle\langle V V^{-1} \rangle\rangle$.

THEOREM 2.10. $T = V^l$.

Proof. Let Λ be the set of cosets of the subgroup V^l of the group S. By (2.3), $V \subset V^{l+1}$; by Theorem 2.4, $V^{l+1} \in \Lambda$. Since $V^l \lhd S$, Λ is a group.

Therefore V^{-1} and hence VV^{-1} are in some coset Y from Λ: $VV^{-1} \subset Y \in \Lambda$. Since $1 \in VV^{-1}$, we have $Y = V^l$, i.e. $VV^{-1} \subset V^l$. Since $V^l \lhd S$, we see that

$$T \subset V^l. \tag{2.7}$$

Fix some $v \in V$. For any $v_1 \in V$ we have $v_1 = (v_1 v^{-1})v$. Since $v_1 v^{-1} \in T$, we have $Tv = Tv_1$. Raising to the lth power and taking into account that $V^l \lhd S$, we obtain $TV^l = Tv^l$. Therefore by (2.7) we get $V^l = Tv^l$. Since $1 \in V^l$, the coset Tv^l contains 1. Therefore $Tv^l = T$ and $T = V^l$. ∎

It follows from this theorem that the subgroup V^l is uniquely determined by the set V (we are not claiming that V uniquely determines the number l).

Corollary 2.11. $|S : T| = d$.

Proof. $|S : V^l| = d$ by Corollary 2.2.

Theorem 2.12. *The following statements are equivalent:*

(a) $d > 1$.
(b) $V \cap T = \emptyset$.
(c) $T \neq S$ *and* $V \subset Tv$ *for some* $v \in V$,
(d) $V \subset Nx$, *where* $N \lhd S$, $N \neq S$, $x \in S$.

Proof. (a)⇒(b). If $d > 1$, then by Theorem 2.2, $V^l \cap V^{l+1} = \emptyset$. Since $V^l = T$ (Theorem 2.10) and $V \subset V^{l+1}$ (formula (2.3)), we get $V \cap T = \emptyset$.

(b)⇒(c). Since $V \cap T = \emptyset$, we have $T \neq S$. Let $v \in V$. Then $v \in V^{l+1}$ since $V \subset V^{l+1}$. Since V^{l+1} and $V^l v$ are cosets of V^l and $V^{l+1} \supset V^l v$, we have $V^{l+1} = V^l v$. Since $T = V^l$ and $V \subset V^{l+1}$, we get $V \subset Tv$.

(c)⇒(d). In (c), put $N = T$, $x = v$.

(d)⇒(a). If $V \subset Nx$, then $V^{-1} \subset (Nx)^{-1} = x^{-1}N$. So $VV^{-1} \subset Nxx^{-1}N = N$, and since $N \lhd S$, $T = \langle\langle VV^{-1} \rangle\rangle$ is a subgroup of N. By Corollary 2.5, $d = |S : T| \geq |S : N| > 1$. ∎

By Corollary 2.1, failure to fulfill any of the conditions (a)–(d) of the theorem is equivalent to convergence (stabilization) of the sequence $\{V^n\}$.

Corollary 2.13. *The sequence* $\{V^n\}$ *converges* (*stabilizes*) *if and only if the sequence* $\{P^{(n)}\}$ *converges to the uniform* (*trivial*) *probability on* S.

Indeed, condition (c) means that the carrier V of the probability P is contained in a coset of a subgroup of S, but it is a necessary and sufficient condition for the absence of convergence $P^{(n)}$ ([2]), as stated at the beginning of the article.

From the equivalence (d)⇔(a) we get

Corollary 2.14. *If* S *is a simple group, then the sequence* $\{V^n\}$ *converges* (*stabilizes*).

COROLLARY 2.15. *If $S = S_m$ is the symmetric group of degree m, then the sequence $\{V^n\}$ does not converge if and only if the set V consists of odd permutations.*

Proof. If $V = \{1\}$, then $V^n = 1$ for any n and $\{V^n\}$ converges. The only non-trivial normal subgroup in S_m is the alternating group A_m of index 2. The non-identity coset of A_m in S_m consists of all odd permutations in S_m.

REFERENCES

[1] A. Bendikov, A. Grigor'yan, Ch. Pittet and W. Woess, *Isotropic Markov semigroups on ultrametric spaces*, Russian Math. Surv. 69 (2014), 589–680.
[2] P. Diaconis, *Group Representations in Probability and Statistics*, Inst. Math. Statist., Hayward, CA, 1988.
[3] L. Saloff-Coste, *Random walks on finite groups*, in: Probability on Discrete Structures, H. Kesten (ed.), Springer, 2004, 263–346.

A. L. Vyshnevetskiy
Kharkiv National Automobile and Highway University
Yaroslava Mudrogo St. 25
61002, Kharkiv, Ukraine
E-mail: alexwish@mail.ru