ISSN 2221-5646(Print) 2523-4641(Online)
Visnyk of V.N.Karazin Kharkiv National University
Ser. "Mathematics, Applied Mathematics
and Mechanics"
2025, Vol. 101, p. 40–47
DOI: 10.26565/2221-5646-2025-101-04
УДК 519.21

Вісник Харківського національного
університету імені В.Н. Каразіна
Серія "Математика, прикладна
математика і механіка"
2025, Том 101, с. 40–47

O. L. Vyshnevetskiy
Associate Professor, Candidate of Physical and Mathematical Sciences
Associate Professor of the Department of Higher Mathematics
Kharkiv National Automobile and Highway University
25 Yaroslava Mudryho St., Kharkiv, 61002, Ukraine
alexwish50@gmail.com *http://orcid.org/0000-0003-1757-0416*

Convolution of probabilities constant in a subgroup and outside a subgroup

Let be P the probability on a finite group G, i.e. the function $P(g)$ takes non-negative values and $\sum_g P(g) = 1$ $(g \in G)$. For any two functions $F_1(g)$ and $F_2(g)$ their G convolution

$$(F_1 * F_2)(t) = \sum_{h \in G} F_1(h) F_2\left(h^{-1}t\right), t \in G$$

is also a function on G.

In recent years, the topic of studying random walks (and not only on groups) has become very popular. From an analytical point of view, the study of random walks is only the study of their transition function, that is, the n-fold convolution of probability measures. It is well known that under simple conditions, imposed on the probability support P on the group G, n-fold convolution $P^{(n)} = P * ... * P$ (n times) with $n \to \infty$ converges to uniform probability $U(g) = \frac{1}{|G|}(\ g \in G)$, which is obviously a constant on G.

We study convolution of functions that may be different but are constant in or outside some subgroup. In short, we study the cases where the convolution of such functions has the same properties of constancy with respect to some subgroup.

The article considers the convolution of probabilities (and, in general, real functions) constant outside (or inside) a subgroup of H the finite group G. Let $D = G \backslash H$. For a given function F on G the subgroup H, for which F is constant on D, is unique in the following sense: there is at most one such number c and one smallest subgroup H of the group G such that $F(g) = c$ for all elements $g \in D$.

It is proved that if the functions F_1, F_2 are constants on D, $F_1(x) = c_1, F_2(x) = c_2$ for arbitrary $x \in D$, then their convolution $F_1 * F_2$ is also a constant on D. The value for this constant is found in terms of the numbers c_1, c_2. Functions on the group G that are constant on D form a semigroup with respect to the convolution.

If one of functions F_1, F_2 is constant on the subgroup H and other is constant on D, then it is proved that the convolution $F_1 * F_2$ is constant on H. The value for this constant is found.

In the above statements about a convolution, one of two factors is constant outside the subgroup. But if both factors are constant on the same subgroup, then their convolution is not necessarily constant on the subgroup. An example is given of two functions that are constant on subgroup H, but their convolution is not constant on H.

This example is not presented in the language of probabilities (or functions) on a group (as in all other parts of the article), but in the language of group algebras. The group algebra KG of the group G over the field K appears in questions related to convolutions of functions on the group G in the following way: each function $F(g)$ on G with values in an arbitrary field K determines an element $\sum_g F(g)\, g\ (g \in G)$ of the algebra KG; the convolution of probabilities corresponds to the product of elements of the algebra KG. So usage of group algebra is natural for studying convolution on a group. If the function $F(g)$ is a probability, then K is the field of real numbers.

Keywords: **probability; finite group; convolution.**

2020 Mathematics Subject Classification: 620D99; 60B15.

1. Introduction

In the article we consider convolution of probabilities (and in general, real-valued functions) that are constant outside (or in) a subgroup of a finite group. We prove that convolution of such probabilities is also constant outside (or in) the subgroup. We also evaluate the constant of the convolution.

From analytical point of view, study of random walks is just study of its transition function, i.e. n-fold convolution of probability measures. We refer to the interesting works A. Bendikov, L. Saloff-Coste [1], [2] and L. Saloff-Coste [3]. We study convolution of probability measures that may be different, but are constant in or outside a subgroup. We show that their convolution has the same property. It is well known (see [3], some refinements see in [4]) that under mild conditions on the carrier of a probability P on a group G, its n-fold convolution power $P^{(n)}$ (n times) at $n \to \infty$ tends to the uniform probability, which is constant on G.

Let H be a subgroup of a finite group G, $H \neq G$ (we write $H < G$), $D = G \backslash H$.

Lemma 1. *1. Element $g \in D$ if and only if $g^{-1} \in D$.*

2. For a fixed element $h \in H$ mapping $x \to hx$ $(x \in D)$ is a bijection $D \to D$.

Proof.

1. By contradiction, because $g \in H$ if and only if $g^{-1} \in H$.
2. By contradiction $hx \in D$. $|hD| = |D|$ and elements of the set hD are pairwise distinct.

Lemma 2. *If $H_1, H_2 < G$ then $H_1 \cup H_2 \neq G$.*

*Proof.*By contradiction, let $H_1 \cup H_2 = G$. For any $x \in H_1, y \in H_2$ their product $xy \in G = H_1 \cup H_2$. We may suppose $xy \in H_1$. Then $y \in H_1$, so $H_2 \subset H_1$ and $G = H_1$.

Let F be a function on a group G. For a subset $M \subset G$ we denote $F(M) = \sum_{g \in M} F(g)$ and $\overline{M} = G \backslash M$. We write $F \in S(H, c)$ if there exist a subgroup H of G and a number c such that $F(t) = c$ for any $t \in \overline{H}$; if number c does not matter we drop it and write $F \in S(H)$.

Theorem 1. *If $F \in S(H_1, c_1)$, $F \in S(H_2, c_2)$, then $F \in S(H_1 \cap H_2, c)$, where $c = c_1 = c_2$.*

Proof. Due to Lemma 2 $H_1 \cup H_2 \neq G$, so there exist an element $x \in \overline{H_1 \cup H_2}$. Since $\overline{H_1 \cup H_2} = \overline{H}_1 \cap \overline{H}_2$, then $c_1 = F(x) = c_2$. Put $c = c_1 = c_2$. So $F(t) = c$ for any $t \in \overline{H}_1 \cup \overline{H}_2 = \overline{H_1 \cap H_2}$.

Corollary 1. *For a given function F and all subgroups H of G there exist*

1. *at most one number c such that $F \in S(H, c)$*
2. *the smallest (with respect to inclusion) subgroup H such that $F \in S(H)$.*

Let function F be a real-valued one and $q = F(G)$.

Theorem 2. *If $F \in S(H, c)$ and $F \geq 0$, then $|q - c|G|| \leq q$ with equality if and only if either a)$|H| = \frac{|G|}{2}$ and $F(h) = 0$ for any $h \in H$ or b)$c = 0$.*

Proof. Rewrite the last inequality as

$$-q \leq q - c|G| \leq q \tag{1}$$

The right-hand inequality is obvious and is equality if and only if $c = 0$. The left-hand inequality is equivalent to

$$c|G| \leq 2q.$$

As H is a subgroup of G, then $|H| \leq \frac{|G|}{2}$, $|D| \geq \frac{|G|}{2}$ and

$$q = F(G) = \sum_{g \in D} F(g) + \sum_{h \in H} F(h) \geq c|D| \geq c\frac{|G|}{2},$$

so (1) is proved. Left-hand inequality in (1) is equality if and only if two last inequalities are equalities. First of the equalities yields $F(h) = 0$ $(h \in H)$, second yields $|H| = \frac{|G|}{2}$.

Corollary 2. *If $P \in S(H, c)$ for a probability P on group G, then $|1 - c|G|| \leq 1$ and*

$$|1 - c|G|| < 1 \tag{2}$$

if and only if neither of conditions a) and b) of the last theorem satisfy.

If $c = 0$ we can take $G = H$.

2. Convolution of functions and probabilities

For a function F defined on some set $M \supseteq H$, we denote F_H restriction F to H. For example, such a restriction of convolution of functions $F_1,\ F_2$, defined on G is:

$$(F_1 * F_2)_H(t) = \sum_{h \in H} F_1(h)\, F_2\left(h^{-1}t\right), t \in H.$$

If $H = G$ we drop the subscript H. We remind that $F_i(M) = \sum_{g \in M} F_i(g)$ for a subset $M \subset G$, $i = 1, 2$. Let $q_i = F_i(G)\,,\ i = 1, 2$.

Theorem 3. *Let functions F_1, F_2 be defined on group G and constant on $D = G \backslash H$: $F_i(t) = c_i,\ i = 1, 2\ (t \in D)$. Then*

1. *If $x \in D$, then $(F_1 * F_2)(x) = c$, where*

$$q_1 q_2 - c\,|G| = (q_1 - c_1\,|G|)(q_2 - c_2\,|G|\,) \tag{3}$$

2. *If $x \in H$, then*

$$(F_1 * F_2)(x) = (F_1 * F_2)_H(x) + c_1 c_2\,|D|\,, \tag{4}$$

Proof. For any $x \in G$ we have

$$\begin{aligned} F_1 * F_2(x) = & \sum_{g \in G} F_1(g) F_2(g^{-1}x) = \\ & \sum_{h \in H} F_1(h) F_2(h^{-1}x) + \sum_{g \in D} F_1(g) F_2(g^{-1}x) \end{aligned} \tag{5}$$

We denote the last two sums $S_1(x)$ and $S_2(x)$.

1. Let $x \in D$. Then in $S_1(x)$ we have $h^{-1}x \in D$, so $F_2(h^{-1}x) = c_2$; besides, since $F_1(G) = F_1(H) + F_1(D)$, then $F_1(H) = q_1 - c_1\,|D|$. So $S_1(x) = c_2 F_1(H) = c_2(q_1 - c_1\,|D|)$.

   In the sum $S_2(x)$ in (5) we have $F_1(g) = c_1$. So

$$S_2(x) = \sum_{g \in D} c_1 F_2(g^{-1}x) = c_1 \left(\sum_{g \in G} F_2(g^{-1}x) - \sum_{g \in H} F_2(g^{-1}x) \right) \tag{6}$$

   In the first of two last sums element $g^{-1}x$ runs over group G when g does the same; in the second sum $g^{-1}x$ runs over D when g does the same (Lemma 1, point 2). So expression (6) equals to $c_1(q_2 - c_2\,|H|)$, and coming back to (5), we get

   $F_1 * F_2(x) = S_1(x) + S_2(x) = c_2(q_1 - c_1\,|D|) + c_1(q_2 - c_2\,|H|) = c_2 q_1 + c_1 q_2 - |G|\ c_1 c_2$.

   For $c = c_2 q_1 + c_1 q_2 - |G|\ c_1 c_2$, equality (3) is identity, so point 1 of the theorem is proved.

2. Let $x \in H$. Then $S_1(x) = (F_1 * F_2)_H(x)$. If $g \in D$, then $g^{-1}x \in D$. So in $S_2(x)$ we have $F_1(g) = c_1,\ F_2(g^{-1}x) = c_2$ and we get (4).

Since $\sum_{g\in G} P(g) = 1$ for a probability $P(g)$ on a group G, than equalities (3) and (4) prove

Corollary 3. *Assume that conditions of Theorem 3 hold. If functions F_1, F_2 are probabilities P_1, P_2 on group G, then*

1. *If $x \in D$, then $(P_1 * P_2)(x) = c$, where*

$$1 - c\,|G| = (1 - c_1\,|G|)(1 - c_2\,|G|\,). \tag{7}$$

2. *If $x \in H$, then*

$$(P_1 * P_2)(x) = (P_1 * P_2)_H(x) + c_1 c_2\,|D| \tag{8}$$

Indeed, $q_1 = q_2 = 1$ for probabilities $P_1,\ P_2$.

Corollary 4. *The functions on group G constant on D form a semigroup on convolution; the same is true for probabilities on group G constant on D.*

We denote these semigroups T and T_P.

Theorem 4. *Let function F_2 be constant on D: $F_2(x) = c_2$ $(x \in D)$. If F_1 is constant on H: $F_1(h) = c_1$ $(h \in H)$, then $F_1 * F_2$ is constant on H: $(F_1 * F_2)(h) = c$, where*

$$q_1 q_2 - c\,|G| = (q_1 - c_1\,|G|)(q_2 - c_2\,|G|\,) \tag{9}$$

Proof. For any $h \in H$ we have

$$\begin{aligned} F_1 * F_2(h) = &\sum_{g\in G} F_1(g)F_2(g^{-1}h) = \\ &\sum_{g\in H} F_1(g)F_2(g^{-1}h) + \sum_{g\in D} F_1(g)F_2(g^{-1}h) \end{aligned} \tag{10}$$

In the first of two last sums $F_1(g) = c_1$, and for $h \in H$ fixed, $g^{-1}h$ runs over H when g runs over H, so the sum equals to

$$c_1 \sum_{g\in H} F_2(g^{-1}h) = c_1 F_2(H) = c_1 (F_2(G) - F_2(D)) = c_1 q_2 - c_1 c_2\,|D|\,.$$

In the second sum $F_2(g^{-1}h) = c_2$, since $g^{-1}h$ runs over D when g runs over D (Lemma 1), so the sum is

$$c_2 \sum_{g\in D} F_1(g) = c_2 F_1(D) = c_2 (F_1(G) - F_1(H)) = c_2 q_1 - c_1 c_2\,|H|$$

So right-hand part of (10) equals to

$$c_1 q_2 - c_1 c_2\,|D| + c_2 q_1 - c_1 c_2\,|H| = c_1 q_2 + c_2 q_1 - |G|\ c_1 c_2$$

It is equivalent to (9) at $c = c_1 q_2 + c_2 q_1 - |G|\ c_1 c_2$.

Theorem 5. *Previous theorem is true for $F_2 * F_1$.*

First we note that this theorem is not a direct corollary of the previous one, because:

1. in general $Q_1 * Q_2 \neq Q_2 * Q_1$ for functions Q_1 and Q_2 on a group,
2. F_1 and F_2 are constant on different subsets of group G.

Proof. Interchanging F_1 and F_2 in (10), we obtain

$$F_2 * F_1(h) = \sum_{g\in H} F_2(g)F_1(g^{-1}h) + \sum_{g\in D} F_2(g)F_1(g^{-1}h);$$

in the first sum $F_1(g^{-1}h) = c_1$ as $g^{-1}h$ runs over H when g does the same and $h \in H$ is fixed; so the sum equals to

$$c_1 \sum_{g\in H} F_2(g) = c_1 F_2(H) = c_1 (q_2 - F_2(D)) = c_1 q_2 - c_1 c_2 |D|, \tag{11}$$

In the second sum $F_2(g) = c_2$ and by the Lemma 1 $g^{-1}h$ runs over D when g does the same and $h \in H$ is fixed, so the sum equals to

$$c_2 \sum_{g\in D} F_1(g^{-1}h) = c_2 F_1(D) = c_2 (F_1(G) - F_1(H)) = c_2 q_1 - c_1 c_2 |H|. \tag{12}$$

Sum of (11) and (12) is $c_1 q_2 + c_2 q_1 - |G|\ c_1 c_2$.

Corollary 5. *Let a probability P_2 be constant on D: $P_2(x) = c_2$ $(x \in D)$. If P_1 is constant on H: $P_1(h) = c_1$ $(h \in H)$, then $P_1 * P_2$ is too: $(P_1 * P_2)(h) = c$, where*

$$1 - c|G| = (1 - c_1|G|)(1 - c_2|G|) \tag{13}$$

The same is true for $P_2 * P_1$.

Indeed, $q_1 = q_2 = 1$ in (9) for probabilities $P_1,\ P_2$.

In Theorem 3 we proved that convolution $F_1 * F_2$ is constant on $D = G\backslash H$ if one of functions $F_1,\ F_2$ is constant on D, another on D or on H. But if both $F_1,\ F_2$ are constant on H, then $F_1 * F_2$ can be not constant on H. The corresponding example is given below.

We use group algebra instead of functions on group G. Namely, let RG be a group algebra of the group G over the field R of real numbers. Each function $F(g)$ on the group G corresponds to an element $f = \sum_{g\in G} F(g)\, g \in RG$. We denote a function (or a probability) on the group G with a capital letter and the corresponding element of RG with the same (but small) letter, and call the latter a probability on RG. Convolution of two functions $P,\ Q$ on G corresponds to product pq of corresponding elements $p,\ q \in RG$. In particular, $P*P$ corresponds to $p^2 \in RG$.

Let $G = \langle a,\ b;\ a^2 = b^2 = 1,\ ab = ba\rangle$ be an elementary abelian 2-group of order 4. We define a function (even a probability) P on G as follows: $P(b) = 0$, $P(1) = P(a) = P(ab) = \frac{1}{3}$. Corresponding to P element of RG is $p = \frac{1}{3}(1 + a + ab)$. Then

$$p^2 = \frac{1}{9}(1 + a + ab)^2 = \frac{1}{9}(3 + 2(a + ab + b)) = \frac{1}{3} + \frac{2}{9}(a + ab + b)$$

Function P is constant on subgroup $H = \{1,\ a\}$, but function $P * P$ corresponding to element $p^2 \in RG$ takes different values $\frac{1}{3}$ and $\frac{2}{9}$ on H. So $P * P$ is not a constant on H.

REFERENCES

1. A. Bendikov, L. Saloff-Coste. Random walks on groups and discrete subordination, Math. Nachr., 285(5-6), 2012. -P. 580–605,

2. A. Bendikov, L. Saloff-Coste, Random walks on some countable groups, Groups, graphs and random walks, London Math. soc. Lecture Note Ser., 436, Cambridge Univ. Press, 2017. -P. 77–103.

3. L. Saloff-Coste, Random walks on finite groups, in: Probability on Discrete Structures, H. Kesten (ed.), Springer, 2004.

4. O. L. Vyshnevetskiy, Conditions of convergence of a random walk on a finite group, Colloquium Mathematicum. -167, -2022. -P. 109-113.

Article history: Received: 8 March 2025; Final form: 1 June 2025
Accepted: 5 June 2025.

How to cite this article:

O. L. Vyshnevetskiy. Convolution of probabilities constant in a subgroup and outside a subgroup, Visnyk of V. N. Karazin Kharkiv National University. Ser. Mathematics, Applied Mathematics and Mechanics, Vol. 101, 2025, p. 40–47. DOI: 10.26565/2221-5646-2025-101-04

Згортка ймовірностей, сталих на підгрупі та поза підгрупою

Вишневецький О. Л.
кафедра вищої математики
Харківський національний автомобільно-дорожний університет
25 Ярослава Мудрого вул., Харків, 61002, Україна

Нехай P - ймовірність на скінченній групі G, тобто функція $P(g)$ приймає невід'ємні значення і $\sum_g P(g) = 1$ $(g \in G)$. Для будь-яких двох функцій $F_1(g)$ і $F_2(g)$ на G їх згортка

$$(F_1 * F_2)(t) = \sum_{h \in G} F_1(h) F_2\left(h^{-1}t\right), t \in G$$

також є функцією на G.

За останні роки тематика дослідження випадкових блукань (і не тільки на групах) стала дуже популярною. З аналітичної точки зору, дослідження випадкових блукань є лише вивченням їх функції переходу, тобто n-кратної згортки ймовірнісних мір. Добре відомо, що за нескладних умов, накладених на носій ймовірності P на групі G, n-кратна згортка $P^{(n)} = P * ... * P$ (n разів) при $n \to \infty$ збігається до рівномірної ймовірності $U(g) = \frac{1}{|G|}$ $(g \in G)$, яка, очевидно, є сталою на G.

Ми вивчаємо згортку функцій, які можуть бути різними, але сталими на деякій підгрупі або поза нею. Коротко кажучи, ми вивчаємо випадки, коли згортка таких функцій має ті ж властивості сталості відносно деякої підгрупи.

У статті розглядається згортка ймовірностей (і, взагалі, дійсних функцій), сталих поза (або всередині) підгрупи H скінченної групи G. Нехай $D = G \backslash H$. Для даної функції F на G підгрупа H, для якої F є сталою на D, є єдиною в наступному сенсі: існує щонайбільше одна таке число c та одна найменша підгрупа H групи G такі, що $F(g) = c$ для усіх елементів $g \in D$.

Доведено, що якщо функції F_1, F_2 є сталими на D, $F_1(x) = c_1, F_2(x) = c_2$ для довільного $x \in D$, то їхня згортка $F_1 * F_2$ також є сталою (константою) на D. Знайдено вираз для цієї константи через числа c_1, c_2. Функції на групі G, які є сталими на D, утворюють півгрупу відносно згортки.

Якщо одна з функцій F_1, F_2 є сталиою на підгрупі H, а інша є сталою на D, то доведено, що згортка $F_1 * F_2$ є сталою на H. Знайдено значення цієї сталої.

У наведених твердженнях про згортку принаймні один її множник був сталим поза підгрупою. Але якщо обидва множники є сталими на деякій підгрупі, то їхня згортка не обов'язково має ту ж властивість. Наведений приклад двох функцій, які є сталими на підгрупі H, але їхня згортка не є сталою на H.

Цей приклад викладений не мовою ймовірностей (чи функцій) на групі (як в усіх інших частинах статті), а мовою групових алгебр. Групова алгебра KG групи G над полем K з'являється у питаннях, пов'язаних зі згортками функцій на групі G, наступним чином: кожна функція $F(g)$ на G із значеннями у довільному полі K визначає елемент $\sum_g F(g)g$ $(g \in G)$ алгебри KG; згортці ймовірностей відповідає добуток елементів алгебри KG. Отже використання групової алгебри є природним при вивченні згортки на групі. Якщо функція $F(g)$ є ймовірністю, то K є полем дійсних чисел.

Ключові слова: **ймовірність; скінченна група; згортка; групова алгебра.**

Історія статті: отримана: 8 березня 2025; останній варіант: 1 червня 2025
прийнята: 5 червня 2025.