I. P. Il'inskaya

PHASE RETRIEVAL FOR PROBABILITY MEASURES
ON CYCLIC GROUPS

I. P. Il'inskaya. *Phase retrieval for probability measures on cyclic groups*, Mat. Stud. **46** (2016), 89–95.

We construct the classes of probability measures on the groups $\mathbb{Z}_n$ and $\mathbb{Z}$ for which the identification of a measure given modulus of its characteristic function is possible up to a shift and the central symmetry. For groups $\mathbb{Z}_3$, $\mathbb{Z}_4$ we give the completely description of such classes.

1. Introduction. The importance of phase retrieval in physics has been described in [1], where a list of references can be founded. The problem can be formulated as follows. Let G be a locally compact abelian group, $M^1(G)$ be a convolution semigroup of probability measures on G. It is physically possible to measure the absolute value of the characteristic function $\widehat{m}$ of the measure $m \in M^1(G)$, but not its argument. What can then be said about m?

Let us give the main definitions.

Definition 1. We call the measures $m, \mu \in M^1(G)$ *equivalent* $(m \sim \mu)$ if

$$|\widehat{m}| = |\widehat{\mu}|. \tag{1}$$

Obviously, for all $g \in G$ we have $m \sim m * \delta_g$ (δ_g is the degenerate at the point g probability measure) and $m \sim \widetilde{m} * \delta_g$, where $\widetilde{m}(E) = m(-E)$ for all Borel sets $E \subset G$.

Definition 2. Let $m \in M^1(G)$. The set $E(m)$ of all measures $\mu \in M^1(G)$ such that $\mu \sim m$ is called the *equivalence class* of the measure m.

Definition 3. We say that a measure m has a *trivial equivalence class* and write $m \in TEC(G)$ if $E(m) = \{m * \delta_g : g \in G\} \cup \{\widetilde{m} * \delta_g : g \in G\}$.

Some classes of measures on locally compact abelian groups with a trivial equivalence class were constructed in [2–8]. Our aim is to give conditions under which measures on groups $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ have a trivial equivalence class.

2. Statement of results. At first we shall consider probability measures on the group $\mathbb{Z}_n$. Elementary examples of measures from $TEC(\mathbb{Z}_n)$ are the Haar measure (uniform distribution on $\mathbb{Z}_n$) and all measures δ_g, $g \in \mathbb{Z}_n$. The following theorem was proved in [3].

Theorem A ([3]). *On $\mathbb{Z}_n$ the uniform distribution on $\{0, 1, \ldots, s - 1\} \subset \mathbb{Z}_n$ has a trivial equivalence class if $2s \leq n$.*

Denote by $\sigma(m)$ the support of the measure m and by $|C|$ the number of the points of a set C.

In Theorem 1 the class of measures $m \in M^1(\mathbb{Z}_n)$ with $|\sigma(m)| = 2$, that have a trivial equivalence class, is completely described.

Theorem 1. (*i*) *For $n \neq 3r$, $r \in \mathbb{N}$, all measures $m \in M^1(\mathbb{Z}_n)$ such that $|\sigma(m)| = 2$ have a trivial equivalence class.*

(*ii*) *For $n = 3r$, $r \in \mathbb{N}$, all measures $m \in M^1(\mathbb{Z}_n)$ with $\sigma(m) = \{k, k + r\}$, $k \in \mathbb{Z}_n$, have a nontrivial equivalence class. All another measures $m \in M^1(\mathbb{Z}_{3r})$ with $|\sigma(m)| = 2$ have a trivial equivalence class.*

In Theorem 2 the examples of measures from $M^1(\mathbb{Z}_{2l})$, $l \in \mathbb{N}$, with a trivial equivalence class are given.

Theorem 2. *All measures $m \in M^1(\mathbb{Z}_{2l})$, $l \in \mathbb{N}$, such that*

$$m(\{2k\}) = a, \ m(\{2k + 1\}) = b, \ a \geq 0, \ b \geq 0, \ a + b = \frac{1}{l}, \ k = 0, 1, \ldots, l - 1,$$

have a trivial equivalence class.

It is well known that all measures on the group $\mathbb{Z}_2$ have a trivial equivalence class. In the following theorem we give the complete description of measures on the groups $\mathbb{Z}_3$ and $\mathbb{Z}_4$ with a trivial equivalence class.

Theorem 3. (*i*) *On the group $\mathbb{Z}_3$ the Haar measure, all measures δ_g, $g \in \mathbb{Z}_3$, and only these measures have a trivial equivalence class.*

(*ii*) *On the group $\mathbb{Z}_4$ the following measures and only one have a trivial equivalence class: the measures m such that $|\sigma(m)| \leq 2$, and all measures m with the property $m(\{0\}) = m(\{2\})$, $m(\{1\}) = m(\{3\})$.*

We can not give the completely description of the classes $TEC(\mathbb{Z}_n)$, $n \geqslant 5$, because it runs into technical difficulties. But the following conjecture can be formulated: *on the groups $\mathbb{Z}_p$, where p is a prime, $p \geq 5$, the class $TEC(\mathbb{Z}_p)$ consists of the Haar measure and the measures m with $|\sigma(m)| \leq 2$ only.*

Now we consider the probability measures on the group $\mathbb{Z}$. Elementary examples of measures from $TEC(\mathbb{Z})$ are all measures δ_g, $g \in \mathbb{Z}$. The following theorem was proved in [3].

Theorem B ([3]). *On the group $\mathbb{Z}$ the uniform distribution on the every finite interval $\{i, i + 1, i + 2, \ldots, i + s\}$, $i \in \mathbb{Z}$, $s \in \mathbb{N}$, has a trivial equivalence class.*

In Theorem 4 we give another examples of measures on the group $\mathbb{Z}$ with a trivial equivalence class.

Theorem 4. *All measures $m \in M^1(\mathbb{Z})$ such that $|\sigma(m)| = 2$ have a trivial equivalence class.*

3. Proof of results.

Proof of Theorem 1. Note that the condition (1) may be written as $\widehat{\mu} \cdot \overline{\widehat{\mu}} = \widehat{m} \cdot \overline{\widehat{m}}$. Hence (1) is equivalent to the condition

$$\mu * \widetilde{\mu} = m * \widetilde{m}. \tag{2}$$

Let $m, \mu \in M^1(\mathbb{Z}_n)$ and $m \sim \mu$. We denote $a_k = m(\{k\})$, $\alpha_k = \mu(\{k\})$, $k = 0, 1, \ldots, n-1$. Obviously,

$$\sum_{k=0}^{n-1} a_k = 1, \qquad \sum_{k=0}^{n-1} \alpha_k = 1. \tag{3}$$

The equality (2) may be written in the form

$$\sum_{k=0}^{n-1} \alpha_k \alpha_{k+t} = \sum_{k=0}^{n-1} a_k a_{k+t}, \quad t = 0, 1, \ldots, \left[\frac{n}{2}\right], \tag{4}$$

where $a_l = a_{l-n}$, $\alpha_l = \alpha_{l-n}$ if $l \geq n$. In the sequel the values α_k be unknown and the values a_k be given.

Obviously $E(m) = E(m * \delta_g)$. Therefore we may consider the measures m with the property $\sigma(m) = \{0, j\}$, $j \leq [n/2]$. Let $\mu \sim m$. We may take $\alpha_0 = \mu(\{0\}) \neq 0$. Equation system (4) can be written in the form

$$\begin{cases} \sum\limits_{k=0}^{n-1} \alpha_k^2 = \sum\limits_{k=0}^{n-1} a_k^2, \\ \sum\limits_{k=0}^{n-1} \alpha_k \alpha_{k+t} = 0, \qquad t = 1, 2, \ldots, j-1, j+1, \ldots, [n/2], \\ \sum\limits_{k=0}^{n-1} \alpha_k \alpha_{k+j} = a_0 a_j. \end{cases} \tag{5}$$

Put $t = 1$ in (5). Since $\alpha_0 \neq 0$, we have $\alpha_1 = 0$, $\alpha_{n-1} = 0$. For $t = 2$ we see that $\alpha_2 = 0$, $\alpha_{n-2} = 0$. Next, for $t = 3, 4, \ldots, j-1, j+1, \ldots, [n/2]$, we have $\alpha_s = 0$ for $s \neq 0, j, n-j$. Therefore $\sigma(\mu) \subset \{0, j, n-j\}$.

First let us consider the cases $n \neq 3r$, $r \in \mathbb{N}$, or $n = 3r$ and $\sigma(m) = \{0, j\}$, $j \neq r$. Since $j \neq n/3$, we have $(n-j) - j \neq j$. Therefore $\alpha_j \alpha_{n-j} = 0$ and $\alpha_j = 0$ or $\alpha_{n-j} = 0$.

If $\alpha_{n-j} = 0$, then $\sigma(\mu) = \{0, j\}$ and system (5) has the form

$$\begin{cases} \alpha_0^2 + \alpha_j^2 = a_0^2 + a_j^2, \\ \alpha_0 \alpha_j = a_0 a_j. \end{cases}$$

This system has two solutions: $\alpha_0 = a_0$, $\alpha_j = a_j$ and $\alpha_0 = a_j$, $\alpha_j = a_0$. In the first case we have $\mu = m$ and in the second case we have $\mu = \widetilde{m} * \delta_j$.

If $\alpha_j = 0$, then $\sigma(\mu) = \{0, n-j\}$ and system (5) has the form

$$\begin{cases} \alpha_0^2 + \alpha_{n-j}^2 = a_0^2 + a_j^2, \\ \alpha_0 \alpha_{n-j} = a_0 a_j. \end{cases}$$

The solutions are: 1) $\alpha_0 = a_0$, $\alpha_{n-j} = a_j$ and therefore $\mu = \widetilde{m}$, 2) $\alpha_0 = a_j$, $\alpha_{n-j} = a_0$ and therefore $\mu = m * \delta_{n-j}$.

Thus, if $n \neq 3r$ then all measures m on $\mathbb{Z}_n$ such that $|\sigma(m)| = 2$ have a trivial equivalence class. If $n = 3r$, $r \in \mathbb{N}$, then all measures $m \in M^1(\mathbb{N}_{3r})$ with the condition $\sigma(m) = \{0, j\}$, $j \neq r$, have a trivial equivalence class.

Now we consider the case $n = 3r$, $\sigma(m) = \{0, r\}$. Resoning as earlier we see that if $\mu \sim m$ then $\sigma(\mu) \subset \{0, r, 2r\}$. In this case system (4) and conditions (3) have the form

$$
\begin{cases}
\alpha_0 + \alpha_r + \alpha_{2r} = a_0 + a_r = 1, \\
\alpha_0^2 + \alpha_r^2 + \alpha_{2r}^2 = a_0^2 + a_r^2, \\
\alpha_0 \alpha_r + \alpha_r \alpha_{2r} + \alpha_{2r} \alpha_0 = a_0 a_r.
\end{cases}
\tag{6}
$$

The third equation of this system is a direct consequence of the first and the second one. The first equation of system (6) yields the part of the plane that lies in the first octant. The distance between this plane and the origin is equal to $1/\sqrt{3}$. The second equation of system (6) yields the part of the sphere with the radius $\sqrt{a_0^2 + a_r^2}$, $1/\sqrt{2} \leq \sqrt{a_0^2 + a_r^2} < 1$. Since $1/\sqrt{3} < 1/\sqrt{2}$, the sphere and the plane have infinitely many common points $(\alpha_0, \alpha_r, \alpha_{2r})$. Therefore system (6) has infinitely many positive solutions and $m \notin TEC(\mathbb{Z}_{3r})$. $\qquad\square$

Proof of Theorem 2. Let us now consider the equations of system (4) with $n = 2l$, $t \in \{0, 2\}$:

$$
\sum_{k=0}^{2l-1} \alpha_k^2 = \sum_{k=0}^{2l-1} a_k^2, \quad \sum_{k=0}^{2l-1} \alpha_k \alpha_{k+2} = \sum_{k=0}^{2l-1} a_k a_{k+2}.
$$

It follows from these equations that

$$
\sum_{k=1}^{l} (\alpha_{2k-1} - \alpha_{2k+1})^2 + \sum_{k=0}^{l-1} (\alpha_{2k} - \alpha_{2k+2})^2 = \sum_{k=1}^{l} (a_{2k-1} - a_{2k+1})^2 + \sum_{k=0}^{l-1} (a_{2k} - a_{2k+2})^2.
$$

Using the condition of Theorem 2 we see that the right part of this equation is equal to zero. Then the left part is equal to zero too. Thus $\alpha_{2k} = c$, $\alpha_{2k+1} = d$ for all k, being $c + d = 1/l$. Substituting these values into (4) with $t = 0$ and using (3), we find that

$$
\begin{cases}
c + d = a + b, \\
c^2 + d^2 = a^2 + b^2.
\end{cases}
$$

Therefore $c = a$, $d = b$ or $c = b$, $d = a$. These values of α_k satisfy another equations of system (4). Hence $\mu = m$ or $\mu = m * \delta_1$. $\qquad\square$

Proof of Theorem 3. Consider first measures on the group $\mathbb{Z}_3$. It follows from Theorem 1 ($n = 3$, $r = 1$) that all measures $m \in M^1(\mathbb{Z}_3)$ such that $|\sigma(m)| = 2$ have a nontrivial equivalence class. Let $|\sigma(m)| = 3$. In this case system (4) and conditions (3) have a form

$$
\begin{cases}
\alpha_0 + \alpha_1 + \alpha_2 = a_0 + a_1 + a_2 = 1, \\
\alpha_0^2 + \alpha_1^2 + \alpha_2^2 = a_0^2 + a_1^2 + a_2^2, \\
\alpha_0 \alpha_1 + \alpha_1 \alpha_2 + \alpha_2 \alpha_0 = a_0 a_1 + a_1 a_2 + a_2 a_0.
\end{cases}
\tag{7}
$$

The third equation of this system is a direct consequence of the first and the second one. If $a_0 = a_1 = a_2 = 1/3$ then the plane and the sphere (7) have a unique common point $\alpha_0 = \alpha_1 = \alpha_2 = 1/3$. Hence $\mu = m$. In another cases the plane and the sphere have infinitely many common points, system (7) has infinitely many solutions and $m \notin TEC(\mathbb{Z}_3)$.

Consider now measures on the group $\mathbb{Z}_4$. It follows from Theorems 1 and 2 that we need to prove the following claim. If the measure m satisfies the conditions $|\sigma(m)| > 2$,

$m(\{0\}) \neq m(\{2\})$ or $m(\{1\}) \neq m(\{3\})$, then $m \notin TEC(\mathbb{Z}_4)$. System (4) and conditions (3) have a form

$$\begin{cases} \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 = a_0 + a_1 + a_2 + a_3 = 1, \\ \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = a_0^2 + a_1^2 + a_2^2 + a_3^2, \\ \alpha_0\alpha_1 + \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_0 = a_0a_1 + a_1a_2 + a_2a_3 + a_3a_0, \\ \alpha_0\alpha_2 + \alpha_1\alpha_3 = a_0a_2 + a_1a_3. \end{cases} \tag{8}$$

Let us subtract from the second equation of system (8) the third equation multiplied by 2 and add the forth one multiplied by 2. We obtain the following equation

$$(\alpha_0 - \alpha_1 + \alpha_2 - \alpha_3)^2 = (a_0 - a_1 + a_2 - a_3)^2.$$

Consider now the case $\alpha_0 - \alpha_1 + \alpha_2 - \alpha_3 = a_0 - a_1 + a_2 - a_3$. It follows from this equation and from the first equation of (8) that

$$\begin{cases} \alpha_0 + \alpha_2 = a_0 + a_2, \\ \alpha_1 + \alpha_3 = a_1 + a_3. \end{cases} \tag{9}$$

If we subtract from the second equation of system (8) the forth equation multiplied by 2 we obtain the following equation

$$(\alpha_0 - \alpha_2)^2 + (\alpha_1 - \alpha_3)^2 = (a_0 - a_2)^2 + (a_1 - a_3)^2. \tag{10}$$

Substituting α_2 and α_3 from (9) into (10), we find that

$$\left(\alpha_0 - \frac{a_0 + a_2}{2}\right)^2 + \left(\alpha_1 - \frac{a_1 + a_3}{2}\right)^2 = \left(\frac{a_0 - a_2}{2}\right)^2 + \left(\frac{a_1 - a_3}{2}\right)^2. \tag{11}$$

The distance R between the center of this circle and the origin is equal to

$$R = \left(\left(\frac{a_0 + a_2}{2}\right)^2 + \left(\frac{a_1 + a_3}{2}\right)^2\right)^{1/2}.$$

The radius ρ of this circle is equal to

$$\rho = \left(\left(\frac{a_0 - a_2}{2}\right)^2 + \left(\frac{a_1 - a_3}{2}\right)^2\right)^{1/2}.$$

Since $a_0 \neq a_2$ or $a_1 \neq a_3$, we have $\rho \neq 0$. Since $|\sigma(m)| > 2$, we have $a_0a_2 + a_1a_3 \neq 0$. Hence, $R > \rho$. So there are infinitely many points (α_0, α_1) of the circle (11) for which the conditions $0 < \alpha_0 < a_0 + a_2$, $0 < \alpha_1 < a_1 + a_3$ are valid. Therefore system (8) has infinitely many solutions and $m \notin TEC(\mathbb{Z}_4)$.

The case $\alpha_0 - \alpha_1 + \alpha_2 - \alpha_3 = -a_0 + a_1 - a_2 + a_3$ is considered similarly. $\square$

In order to construct new examples of measures with a trivial equivalence class we use the following statement. If H is a subgroup of the group G then all measures on G with $\sigma(m) \subset H$ such that $m \in TEC(H)$ are from $TEC(G)$. The validity of this statement follows from Proposition 2.5 in [9].

By means of this remark we get the following corollaries.

Corollary 1. *If the measure* $m \in M^1(\mathbb{Z}_{2ls})$, $l, s \in \mathbb{N}$, *satisfies the conditions*

$$m(\{2js\}) = a, \quad m(\{(2j+1)s\}) = b, \quad a + b = \frac{1}{l}, j = 0, 1, \ldots, l - 1,$$

then $m \in TEC(\mathbb{Z}_{2ls})$.

Corollary 2. *If the measure* $m \in M^1(\mathbb{Z}_{4s})$, $s \in \mathbb{N}$, *satisfies the conditions*

$$\sigma(m) = \{0, s, 2s, 3s\}, \quad m(\{0\}) = m(\{2s\}), \quad m(\{s\}) = m(\{3s\}),$$

then $m \in TEC(\mathbb{Z}_{4s})$.

Corollary 1 follows from Theorem 2 and Corollary 2 follows from Theorem 3.

Proof of Theorem 4. We can assume, without restriction of generality, that the measure $m \in M^1(\mathbb{Z})$ has a support $\sigma(m) = \{0, n\}$, $n \in \mathbb{Z}$, $n \neq 0$. Let $\mu \in M^1(\mathbb{Z})$ and $\mu \sim m$. Denote $a_k = m(\{k\})$, $\alpha_k = \mu(\{k\})$. Equality (2) may be written in the form

$$\sum_{k \in \mathbb{Z}} \alpha_k \alpha_{k+j} = \sum_{k \in \mathbb{Z}} a_k a_{k+j}, \quad j \in \mathbb{Z}. \tag{12}$$

We assume that $\alpha_0 \neq 0$. Since $\sigma(m) = \{0, n\}$, we have $\sum_{k \in \mathbb{Z}} \alpha_k \alpha_{k+j} = 0, j \neq \pm n$. Hence, $\alpha_j = 0$ for $j \neq \pm n$. For this reason $\sigma(\mu) \subset \{-n, 0, n\}$. Therefore system (12) has a form

$$\begin{cases} \alpha_{-n}^2 + \alpha_0^2 + \alpha_n^2 = a_0^2 + a_n^2, \\ \alpha_{-n}\alpha_0 + \alpha_0\alpha_n = a_0 a_n, \\ \alpha_{-n}\alpha_n = 0. \end{cases}$$

Suppose $\alpha_{-n} = 0$. The system

$$\begin{cases} \alpha_0^2 + \alpha_n^2 = a_0^2 + a_n^2, \\ \alpha_0\alpha_n = a_0 a_n \end{cases}$$

has two solutions: $\alpha_0 = a_0$, $\alpha_n = a_n$ and $\alpha_0 = a_n$, $\alpha_n = a_0$. So $\mu = m$ in the first case and $\mu = \widetilde{m} * \delta_n$ in the second case.

If $\alpha_n = 0$ then

$$\begin{cases} \alpha_0^2 + \alpha_{-n}^2 = a_0^2 + a_n^2, \\ \alpha_0\alpha_{-n} = a_0 a_n. \end{cases}$$

Hence $\alpha_0 = a_0$, $\alpha_{-n} = a_n$ or $\alpha_0 = a_n$, $\alpha_{-n} = a_0$ and $\mu = \widetilde{m}$ or $\mu = m * \delta_{-n}$. Therefore $m \in TEC(\mathbf{Z})$. $\qquad\square$

REFERENCES

1. Rosenblatt J., *Phase retrieval,* Comm. Math. Phys., **95** (1984), 317–343.
2. Carnal H., Dozzi M., *On a decomposition problem for multivariate probability measures*, J. Multivar. Anal., **31** (1989), 165–177.

3. Carnal H., Fel'dman G.M., *Phase retrieval for probability measures on abelian groups*, I. J.Theor. Probab., **8** (1995), №3, 717–725.
4. Carnal H., Fel'dman G.M., *Phase retrieval for probability measures on abelian groups*, II. J.Theor. Probab., **10** (1997), №4, 1065–1074.
5. Carnal H., Feldman G.M., *On a property of entire characteristic functions of finite order with real zeros*, Doklady RAN, **366** (1999), 162–163. (in Russian)
6. Carnal H., Feldman G.M., *A stability property for probability measures on Abelian groups,* Statistics and probability Letters, **49** (2000) 39–44.
7. Il'inskaya I.P., *Phase retrieval for probability measures on the character group of Cantor-Walsh group*, Dopovidi NAN Ukraine, (2003), №8, 11–14. (in Russian)
8. Il'inskaya I.P., Neguritsa D.S., *On probability measures on the group of Walsh functions with a trivial equivalence class*, Ukrainian Mathematical Journal, **65** (2013), №5, 717–721. (in Russian)
9. Fel'dman G.M., Arithmetic of Probability Distributions and Characterization Problems on Abelian Groups, AMS, Providence, RI, 1993.

Kharkov Karazin National University
iljinskii@univer.kharkov.ua