Phase Retrieval for Nilpotent Groups

Hartmut Führ[1] 🆔 · **Vignon Oussa**[2] 🆔

Abstract

We study the phase retrieval property for orbits of general irreducible representations of nilpotent groups, for the classes of simply connected Lie groups, and for finite groups. We prove by induction that in the Lie group case, all irreducible representations do phase retrieval. For the finite group case, we mostly focus on p-groups. Here our main result states that every irreducible representation of an arbitrary p-group with exponent p and size $\leq p^{2+p/2}$ does phase retrieval. Despite the fundamental differences between the two settings, our inductive proof methods are very similar.

1 Introduction

Phase retrieval originated in the Fourier-analytic treatment of questions arising in crystallography. The phase retrieval problem for (finite) frames as a problem in mathematical signal processing was introduced in [3], with motivation stemming from applications such as speech recognition. Since its introduction phase retrieval has developed into a legitimate branch of applied mathematics, with links to diverse subjects such as harmonic analysis, algebraic geometry, optimization, numerical analysis, etc. We refer to the review papers [8, 10] and their extensive lists of references.

✉ Hartmut Führ
  fuehr@mathga.rwth-aachen.de

  Vignon Oussa
  vignon.oussa@bridgew.edu

1 Lehrstuhl für Geometrie und Analysis, RWTH Aachen University, 52056 Aachen, Germany

2 Department of Mathematics, Bridgewater State University, Bridgewater, MA 02234, USA

Despite the general interest in the problem, sources containing explicit constructions of frames with guaranteed phase retrieval properties are still relatively scarce. In this paper, we study the construction of such systems using strongly continuous, unitary representations of locally compact groups. Precisely, let π be a continuous unitary representation of a locally compact group G acting in some Hilbert space $\mathcal{H}_\pi$. Fixing a vector $\eta \in \mathcal{H}_\pi$, we define a continuous linear map $V_\eta : \mathcal{H}_\pi \to C(G)$ as $V_\eta(\psi)(g) = \langle \psi, \pi(g)\eta \rangle$. Next, let $\mathbb{T}$ denote the group of complex numbers of modulus one, and let $\mathcal{H}_\pi/\mathbb{T}$ denote the orbit space of $\mathcal{H}_\pi$ modulo the canonical scalar action of $\mathbb{T}$. We say that η *does phase retrieval* if the map

$$\mathcal{A}_\eta : \mathcal{H}_\pi/\mathbb{T} \to C(G), \ \mathcal{A}_\eta(\mathbb{T} \cdot f)(x) = |V_\eta f(x)|, \ x \in G$$

is injective. Similarly, we say that π *does phase retrieval* if there exists a vector $\eta \in \mathcal{H}_\pi$ that does phase retrieval. It is worth noting that if $\eta \in \mathcal{H}_\pi$ does phase retrieval for π then the linear map V_η is necessarily injective. When this is the case, V_η defines a linear bijection onto a subspace $\mathcal{C}_\eta \subset C(G)$, and the phase retrieval problem is equivalent to the statement that each $F \in \mathcal{C}_\eta$ can be recovered from $|F|$ up to a scalar. This observation serves as motivation for the name 'phase retrieval'; the phase of $F \in \mathcal{C}_\eta$ can be recovered from its modulus.

Even though the phase retrieval problem for finite frames has been studied for almost two decades, the bulk of the literature addressing this problem for group frames has only been devoted to some specific classes of groups, such as the finite Heisenberg groups [2, 5, 10]. The literature also contains a treatment of the affine Lie group (also known as the ax+b group) over the reals [1, 15] as well as the finite ax+b group defined over prime fields [4]. Recently, the results of [5] were extended to the case of projective unitary representations of finite abelian groups [12]. To the best of our knowledge, this is the largest class of general group representations for which the phase retrieval property has been studied. The present work aims to significantly expand the class of available representations. Precisely, we show that the class of groups admitting representations for which phase retrieval is possible includes all simply connected, connected nilpotent Lie groups, as well as all sufficiently small p-groups with exponent p, for an arbitrary prime p.

The following examples describe the group representations that are probably understood best so far, namely the Schrödinger representations of (finite or Lie) Heisenberg groups. These will turn out to be the cornerstones of our general inductive approach. Throughout the paper, we let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be the finite cyclic group of order n, and denote elements of $\mathbb{Z}_n$ (by slight abuse of notation) by $k = 0, \ldots, n-1$.

Example 1 (The finite Heisenberg group) Fix $n \in \mathbb{N}$, $n \geq 2$, and define the associated finite Heisenberg group by

$$\mathbb{H}_n = \mathbb{Z}_n^3 \tag{1}$$

with group law

$$(k, l, m) \cdot (k', l', m') = (k + k', l + l', m + m' - l'k), \tag{2}$$

and arithmetic operations taken modulo n. The center of this group is given by $Z(\mathbb{H}) = \{0\} \times \{0\} \times \mathbb{Z}_n$, and $\mathbb{H}/Z(\mathbb{H}) \cong \mathbb{Z}_n \times \mathbb{Z}_n$. Next, define the *Schrödinger representation* of $\mathbb{H}_n$ acting on $\mathbb{C}^n$ by first introducing the translation and modulation operators T_k, M_l respectively as

$$(T_k f)(y) = f(y - k), \ (M_l f)(y) = e^{2\pi i l y/n} f(y).$$

Let $\pi(k, l, m) = e^{2\pi i m/n} M_l T_k$. Explicitly,

$$(\pi(k, l, m)f)(y) = e^{2\pi i m/n} e^{2\pi i l y/n} f(y - k), \ k, l, m, y \in \{0, \ldots, n - 1\}.$$

This representation is known to be irreducible and also does phase retrieval [5]. To construct a vector η that does phase retrieval for the representation π, define the *ambiguity function* of η, as follows:

$$A_\eta(k, l) = \langle \eta, M_l T_k \eta \rangle.$$

It is shown in [5, 12] that any vector η for which the zero set of the matrix coefficient $A\eta$ is empty does phase retrieval.

Note that the existence of vectors with nonvanishing ambiguity function is established in Proposition 2.1 of [5].

Example 2 (The Heisenberg Lie group) Define the three-dimensional Heisenberg Lie group $\mathbb{H}$ as $\mathbb{H} = \mathbb{R}^3$, with group law

$$(p, q, r)(p', q', r') = (p + p', q + q', r + r' + pq'). \tag{3}$$

$\mathbb{H}$ is a simply connected, connected Lie group with center $\{0\} \times \{0\} \times \mathbb{R} \subset \mathbb{H}$. If we define the continuous-domain translation and modulation operators as $(T_p f)(y) = f(y - p)$, $(M_q f)(y) = e^{2\pi i q y} f(y)$, acting on $f \in L^2(\mathbb{R})$, then $\pi(p, q, r) = e^{2\pi i r} M_q T_p$ defines an irreducible, unitary representation π of $\mathbb{H}$ on $L^2(\mathbb{R})$. The representation π is often referred to as the *Schrödinger representation*, and as its finite counterpart, it does phase retrieval, with an analogous sufficient criterion for vectors guaranteeing that property: Defining the ambiguity function of $\eta \in L^2(\mathbb{R})$ as

$$A_\eta(p, q) = \langle \eta, \pi(p, q, 0)\eta \rangle,$$

we have that η does phase retrieval if A_η vanishes only on a set of Lebesgue measure zero. A prominent example of a window g with that property is provided by the Gaussian.

1.1 Main Contributions of Our Paper

In this paper, we intend to address the problem of phase retrieval for general irreducible representations of nilpotent groups. Our main results in this direction are the following.

- Any irreducible representation of an arbitrary simply connected, connected nilpotent Lie group does phase retrieval (Theorem 12).
- There exist explicitly checkable sufficient criteria for the phase retrieval property of irreducible representations of p-groups (Corollary 33).
- As a corollary to the previous result: Any irreducible representation of an arbitrary p-group with exponent p and size $\leq p^{2+p/2}$ does phase retrieval (Corollary 34).

The techniques we use to establish these results seem of potentially independent interest. In particular, the treatment of the p-group case is surprisingly analogous to the Lie group case, due to a p-group version of Kirillov's lemma that appears to be new (Lemma 22), and an associated explicit construction method for irreducible representations (Lemma 26). Under suitable assumptions on the underlying groups, this approach establishes a close relationship between irreducible representations of p-groups and finite Schrödinger representations that we systematically exploit for the study of phase retrieval.

As a second technical novelty of potential independent interest, we introduce the quantity $p_0(\pi)$ (see Definition 16), which is an upper bound on the proportion of zeros in a nonzero matrix coefficient associated to π. Our results estimating $p_0(\pi)$, specifically Lemma 32, serve as further illustration of the usefulness of the p-group analog of the Kirillov lemma and its representation-theoretic ramifications.

2 Nilpotent Lie Groups

This section establishes phase retrieval for irreducible representations of simply connected, connected nilpotent Lie groups. Before we turn to groups and representations, we first state a few basic observations and ideas regarding phase retrieval, which will be repeatedly useful. We expect them to be well-known, but include short arguments for lack of a handy reference.

Definition 3 Let $\mathcal{H}$ denote a Hilbert space. We say that $(x_i)_{i \in I} \subset \mathcal{H}$ *does phase retrieval* if

$$\forall f, g \in \mathcal{H} : \ (\forall i \in I : |\langle f, x_i \rangle| = |\langle g, x_i \rangle|) \Leftrightarrow f \in \mathbb{T} \cdot g.$$

With this definition, a unitary representation π of a locally compact group does phase retrieval iff there exists a vector $\eta \in \mathcal{H}_\pi$ such that $(\pi(x)\eta)_{x \in G}$ does phase retrieval. Part (b) of the following lemma has been observed e.g. in [6].

Lemma 4 *Let $\mathcal{H}$ denote a Hilbert space and $(x_i)_{i \in I} \subset \mathcal{H}$.*

(a) *If $(x_i)_{i \in I}$ does phase retrieval, then it has dense span in $\mathcal{H}$.*
(b) *If $(x_i)_{i \in I}$ does phase retrieval, and $f, g \in \mathcal{H} \backslash \{0\}$ are arbitrary, there exists $i \in I$ such that*

$$\langle f, x_i \rangle \langle g, x_i \rangle \neq 0.$$

(c) *Let $(y_j)_{j \in J}$ be related to $(x_i)_{i \in I}$ by the following property: There exists a map $\kappa : J \to I$ such that for all $j \in J$*

$$y_j \in \mathbb{T} x_{\kappa(j)}$$

and in addition,

$$\forall i \in I \exists j \in J : x_i \in \mathbb{T} x_{\kappa(j)}.$$

Then $(x_i)_{i \in I}$ does phase retrieval iff $(y_j)_{j \in J}$ does.

Proof Part (a) follows from the fact that any f orthogonal to all x_i must be in $\mathbb{T} \cdot 0 = \{0\}$. For part (b), assuming the existence of $f, g \in \mathcal{H} \setminus \{0\}$ with

$$\forall i \in I : \langle f, x_i \rangle \langle g, x_i \rangle = 0,$$

we first note that by part (a), the fact that f, g are both nonzero implies that the associated coefficient families $(\langle f, x_i \rangle)_{i \in I}$ and $(\langle g, x_i \rangle)_{i \in I}$ are nonzero as well. By assumption, these coefficient families are disjointly supported. Hence they are linearly independent, and accordingly, f and g are linearly independent. In particular, $f + g \notin \mathbb{T}(f - g)$. On the other hand, the disjointness assumption entails for all $i \in I$

$$|\langle f + g, x_i \rangle| = |\langle f, x_i \rangle| + |\langle g, x_i \rangle| = |\langle f - g, x_i \rangle|,$$

which contradicts the phase retrieval property.

For part (c) we note that the assumptions on the two families allow to recover the coefficient family $(\langle f, x_i \rangle)_{i \in I}$ from the coefficient family $(\langle f, y_j \rangle)_{j \in J}$, and the same holds for the families of coefficient moduli. Also, these observations remain true if the families $(x_i)_{i \in I}$ and $(y_j)_{j \in J}$ are interchanged. These facts then imply the equivalence in (c). $\qquad\qquad\square$

We next turn to Hilbert space tensor products and their realization via Hilbert–Schmidt operators. First some notation. Let $\mathcal{H}_1, \mathcal{H}_2$ denote nontrivial Hilbert spaces, and $HS(\mathcal{H}_2, \mathcal{H}_1)$ the space of Hilbert–Schmidt operators $A : \mathcal{H}_2 \to \mathcal{H}_1$, endowed with the usual scalar product

$$\langle A, B \rangle = \text{trace}(AB^*).$$

Given $x \in \mathcal{H}_1, y \in \mathcal{H}_2$, let

$$x \otimes y \in HS(\mathcal{H}_2, \mathcal{H}_1) : \mathcal{H}_2 \ni z \mapsto \langle z, y \rangle x.$$

With this terminology in place, we can formulate the following basic observation.

Lemma 5 *Let $(x_i)_{i \in I} \subset \mathcal{H}_1$, $(y_j)_{j \in J} \subset \mathcal{H}_2$ denote two systems of vectors with the phase retrieval property. Then $(x_i \otimes y_j)_{(i,j) \in I \times J}$ has the phase retrieval property for $HS(\mathcal{H}_2, \mathcal{H}_1)$.*

Proof Let $A, B \in HS(\mathcal{H}_2, \mathcal{H}_1)$ with

$$\forall (i, j) \in I \times j : \ |\langle A, x_i \otimes y_j \rangle| = |\langle B, x_i \otimes y_j \rangle|$$

Note that the operator scalar products are computed as

$$\langle A, x_i \otimes y_j \rangle = \langle A y_j, x_i \rangle.$$

Fixing $j \in J$, this gives for all $i \in I$:

$$|\langle A y_j, x_i \rangle| = |\langle B y_j, x_i \rangle|.$$

The phase retrieval property for $(x_i)_{i \in I}$ then entails

$$A y_j = v(j) B y_j, \ \forall j \in J, \tag{4}$$

with suitable $v(j) \in \mathbb{T}$. We next prove that v is constant on the set

$$S = \{j \in J : \ A y_j \neq 0\}.$$

To see this, we fix $i \in I$, and get for all $j \in J$ that

$$|\langle y_j, A^* x_i \rangle| = |\langle y_j, B^* x_i \rangle|.$$

Hence the phase retrieval property of $(y_j)_{j \in J}$ furnishes a map $u : I \to \mathbb{T}$ with

$$A^* x_i = u(i) B^* x_i, \ \forall i \in I. \tag{5}$$

Now assume that $j, j' \in S$ are given. Then there exists $i \in I$ such that

$$\langle A y_j, x_i \rangle \langle A y_{j'}, x_i \rangle \neq 0, \tag{6}$$

by Lemma 4 (b), and definition of S. This entails

$$\langle A y_j, x_i \rangle = v(j) \langle B y_j, x_i \rangle = v(j) u(i) \langle A y_j, x_i \rangle,$$

and the choice of i allows to cancel $\langle A y_j, x_i \rangle$ from this equation to obtain $v(j) = \overline{u(i)}$. The same reasoning can be applied to $v(j')$, leading to $v(j') = \overline{u(i)} = v(j)$. Hence v is a constant map. Plugging this observation into Eq. (4) provides $v \in \mathbb{T}$ satisfying

$$\forall j \in J : \ A y_j = v B y_j$$

and Lemma 4 (a) now applies to yield $A = vB$. □

We now turn to groups and representations. Before we state the main result of this section, we highlight several representation-theoretic facts relevant to the problem at hand; see Remark 6 and Lemma 8. Given a locally compact group G, we let $\widehat{G}$ denote its unitary dual, i.e. the set of equivalence classes of irreducible unitary representations, and $\pi \in \widehat{G}$ will be shorthand for "π is irreducible". Throughout the paper, we will repeatedly factor out suitably chosen normal subgroups. One such subgroup of particular interest is the *projective kernel* of a unitary representation π, which is given by

$$K_\pi = \{x \in G : \pi(x) \in \mathbb{T} \cdot \mathrm{id}_{\mathcal{H}_\pi}\}.$$

This is a closed normal subgroup of G containing the kernel of π.

Remark 6 Let G denote a locally compact group, and let π be a unitary representation of G. Assume that $K \lhd G$ is a normal subgroup contained in the projective kernel of π. Then π induces a projective representation $\overline{\pi}$ of the quotient group G/K, by picking a cross-section $\sigma : G/K \to G$ and letting $\overline{\pi}(xK) = \pi(\sigma(xK))$. Now Lemma 4(c) shows that the system $(\pi(x)\eta)_{x \in G}$ does phase retrieval iff the system $(\pi(\sigma(x))_{xK \in G/K}$ does.

This observation applies to two cases of particular interest: Firstly, and trivially, we may always factor out normal subgroups H contained in the kernel, and pass the action down to a representation of G/H. Moreover, if π is irreducible and $Z < G$ is a central subgroup, then $\pi(Z) \subset \mathbb{T} \cdot \mathrm{id}_{\mathcal{H}_\pi}$ follows by Schur's lemma. Therefore π does phase retrieval iff the associated projective representation of G/Z does.

Remark 7 At this point, let us shortly explain why we focus on irreducible representations. This focus has a long tradition in representation theory, due to the fact that typically, an understanding of the irreducible cases is fundamental to an understanding of more complex representations. The general intuition is that a decomposition into irreducible subrepresentations allows to reduce the general problem into a family of subproblems, which can then be addressed independently.

In the context of phase retrieval, this intuition works to a limited degree. If $(\pi, \mathcal{H}_\pi)$ is a representation, and $\mathcal{H}_\pi$ decomposes into two closed invariant subspaces, $\mathcal{H}_\pi = \mathcal{K}_1 \oplus \mathcal{K}_2$, then any vector $\eta \in \mathcal{H}_\pi$ doing phase retrieval for π gives rise to two vectors $\eta_1 \in \mathcal{K}_1$, $\eta_2 \in \mathcal{K}_2$ such that the restriction of π to $\mathcal{K}_i$ does phase retrieval for $\mathcal{K}_i$, by taking η_i to be the orthogonal projection of η onto $\mathcal{K}_i$.

The standard representation-theoretic intuition would suggest that this observation also works for the converse direction, at least under suitable assumptions on the subrepresentations associated to the $\mathcal{K}_i$. Specifically, assuming that the subrepresentations are irreducible and inequivalent, one might be tempted to expect that a vector η_i doing phase retrieval for each $\mathcal{K}_i$ gives rise to a vector $\eta = \eta_1 + \eta_2$ that does phase retrieval for $\mathcal{H}_\pi$. This is generally false, as the following example illustrates.

Pick an irreducible representation σ such that the contragredient representation $\overline{\sigma}$ is inequivalent to σ. Such representations exist, e.g. for the Heisenberg groups from Examples 1 (when $n > 2$) and 2. Assume that $\eta_1 \in \mathcal{H}_\sigma$ is a vector doing phase retrieval for σ. If we then realize $\overline{\sigma}$ on $\mathcal{H}_\sigma$ in the canonical manner, the associated

matrix coefficients are related by

$$V_\eta^{\overline{\sigma}} f = \overline{V_\eta^\sigma f};$$

this can be understood as the defining relation of the contragredient representation. On the one hand, this shows that η also does phase retrieval for $\overline{\sigma}$. However, if we now define $\pi = \sigma \oplus \overline{\sigma}$, and use the vector $\eta_0 = \eta \oplus \eta$, we get

$$\left| V_{\eta_0}^\pi (f \oplus 0) \right| = \left| V_\eta^\sigma f \right| = \left| V_{\eta_0}^\pi (0 \oplus f) \right|,$$

hence η_0 does not do phase retrieval.

To summarize: Understanding the phase retrieval problem for irreducible representations will not lead to automatic solutions for arbitrary representations, but it remains a fundamental first step, that we address in the following for nilpotent groups.

We next need a representation-theoretic lemma that is quite probably folklore. It can be proved by direct calculations using the realization of induced representations via cross-sections, see e.g. page 79 of [11].

Lemma 8 *Let $Z < N < G$ be locally compact groups, with N normal and closed in G, and Z central and closed in G. Let τ be a representation of N with the property that the restriction $\tau|_Z$ is a multiple of a character $\chi \in \widehat{Z}$. Then the restriction $\left(\mathrm{ind}_N^G \tau \right)|_Z$ is also a multiple of χ.*

We aim to prove the existence of vectors doing phase retrieval, for an irreducible representation π of a simply connected, connected nilpotent Lie group G. The basic idea is to use induction over $\dim(G)$, and to employ Mackey's theory of induced representations in the process. For the induction step to work, we need a somewhat stronger induction hypothesis on the vectors doing phase retrieval. The relevant additional property is defined next:

Definition 9 Let π denote a unitary representation of the locally compact group G. $\eta \in \mathcal{H}_\pi$ has the *full support property* if for all $0 \neq f \in \mathcal{H}_\pi$ the set

$$\{ x \in G : V_\eta f(x) = 0 \} \subset G$$

has Haar measure zero.

Remark 10 Just as for the case of phase retrieval in Remark 6, the full support property can equivalently be verified for the associated projective representation $\overline{\pi}$ of G/K, where K is any normal subgroup contained in the projective kernel of π. This observation makes use of the fact that the Haar measures of G/K and G are related by Weil's integral formula.

Remark 11 While the full support property has a strictly auxiliary role in our considerations, it seems of independent representation-theoretic interest. We are currently not aware of any sources investigating this property in any systematic way.

As the prime example of a vector with the full support property, we mention the Gaussian window

$$\eta(x) = e^{-\pi x^2}, \quad (x \in \mathbb{R}).$$

It is well-known that the image of the short-time Fourier transform $STFT_\eta$ associated to η, defined by

$$STFT_\eta f(x + iy) = \langle f, M_y T_x \eta \rangle,$$

consists of functions whose product with a suitable, fixed choice of two-dimensional Gaussian is entire (see e.g. Proposition 3.4.1 of [9]). But clearly $STFT_\eta f(x + iy) = V_\eta f(x, y, 0)$, where the right-hand side denotes the matrix coefficient associated to the Schrödinger representation. Hence the fact that nonzero entire functions are nonzero a.e. (together with Remark 10) allows to conclude that η has the full support property for the Schrödinger representation.

Note also that any vector η with the full support property for the Schrödinger representation automatically does phase retrieval; recall from Example 2 that a.e. nonvanishing of $V_\eta \eta$ was sufficient for the latter. Hence the Gaussian has both desired properties.

We are now in position to establish the first main result of this paper.

Theorem 12 *Let G denote a simply connected, connected nilpotent Lie group, and π an irreducible representation of G. Then there exists a vector $\eta \in \mathcal{H}_\pi$ that does phase retrieval, and has the full support property. In particular, π does phase retrieval.*

Proof We proceed by induction over $\dim(G)$. Noting first that the abelian case is trivial, and secondly, that the case of the Heisenberg group is settled, we may assume that G is a nonabelian group of dimension $n > 3$.

Furthermore, we may assume that $K = \text{Ker}(\pi)$ is a zero-dimensional subgroup of G. Otherwise, the Lie algebra $\mathfrak{k}$ of K has positive dimension, and the connected component of the identity $K_0 = \exp(\mathfrak{k})$ in K is a normal subgroup of positive dimension. Now the inductive hypothesis yields a vector with phase retrieval and full support property for the associated representation of the quotient group G/K, and thus for π (see Remarks 6, 10.)

Hence from now on the kernel of π is assumed to be zero-dimensional. This implies that the center $Z(G)$ of G is necessarily one-dimensional. Pick $Z \in \mathfrak{g}$ such that $\exp(\mathbb{R}Z) = Z(G)$. By Kirillov's lemma [7, Lemma 1.1.12], there exist $X, Y \in \mathfrak{g}$ with the following properties: $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathbb{R}X$, $[X, Y] = Z$, $\mathfrak{g}_0$ is an ideal in $\mathfrak{g}$, and it is the centralizer of Y. In particular, the associated subgroup $G_0 = \exp(\mathfrak{g}_0)$ is a normal subgroup, with $G = G_0 \exp(\mathbb{R}X)$. Furthermore, $A = \exp(\mathbb{R}Y) \exp(\mathbb{R}Z)$ is central in G_0, and normal in G.

For better readability, the remainder of the proof is structured into several steps.

Step 1 *There exists an irreducible representation τ of G_0 such that $\pi \simeq \text{ind}_{G_0}^G(\tau)$.*

To see this, consider the dual action of G on the dual group $\widehat{A}$, defined for arbitrary $g \in G$ and $a \in A$, by $[g \star \chi](a) = \chi(g^{-1}ag)$. Let $G_\chi = \{g \in G : g \star \chi = \chi\}$ be the

stabilizer of χ and let

$$\widetilde{G}_\chi = \left\{ \tau \in \widehat{G}_\chi : \tau|_A \text{ is a multiple of } \chi \right\}.$$

For $\tau \in \widetilde{G}_\chi$, $\pi_\tau = \mathrm{ind}_{G_\chi}^G (\tau)$ is an irreducible representation of G. In fact, according to the theory of Mackey [11, Theorem 4.22], every irreducible representation of G is of this form. Hence, since π is assumed to be irreducible, there exists τ, such that $\pi \simeq \mathrm{ind}_{G_\chi}^G (\tau)$ for suitable $\chi \in \widehat{A}$ and $\tau \in \widetilde{G}_\chi$. τ is irreducible, since π is. To complete the proof of Step 1, it suffices to show that $G_\chi = G_0$. Since A is central in G_0, the conjugation action of G_0 on A is trivial. The same then holds for the dual action of G_0 on $\widehat{A}$, and this establishes $G_0 \subset G_\chi$. Moreover, since π is irreducible, $\pi|_{\exp(\mathbb{R}Z)}$ is the multiple of a character, and by assumptions on the kernel of π, this character is necessarily nontrivial. Furthermore, Lemma 8 implies that this character coincides with χ on $Z(G)$. Hence, by suitably normalizing Z and Y, when necessary, we may assume without loss of generality that $\pi(\exp(zZ)) = e^{2\pi i z}$. The relation $[X, Y] = Z$ then entails

$$\exp(-xX)\exp(yY)\exp(xX) = \exp(yY)\exp(-xyZ),$$

and this leads to the following string of equalities:

$$(\exp(xX)\star\chi)(\exp(yY)) = \chi(\exp(yY)\exp(-xyZ)) = e^{-2\pi i xy}\chi(\exp(yY)).$$

These observations imply that $\exp(xX)\star\chi = \chi$ can only hold for $x = 0$. Since every $g \in G$ can be factored uniquely as $g = \exp(xX)g_0$, with $g_0 \in G_0 \subset G_\chi$ and $x \in \mathbb{R}$, we derive finally that $G_0 = G_\chi$.

Step 2 *Choosing an explicit realization of* π We will now introduce coordinates on G, and express π more explicitly in terms of these coordinates, and a suitable choice of realization. Thus far, we have shown that $\pi \simeq \mathrm{ind}_{G_0}^G(\tau)$, where $G_0 \lhd G$, and τ is an irreducible representation, restricting to a multiple of a character χ on $A = \exp(\mathbb{R}Y)\exp(\mathbb{R}Z)$. Furthermore, $\chi(\exp(zZ)) = e^{2\pi i z}$. Let $\mathfrak{g}_0 \subset \mathfrak{g}$ denote the Lie algebra of G_0, and let $W \subset \mathfrak{g}_0$ denote a vector space complement to $\mathbb{R}X \oplus \mathbb{R}Y \subset \mathfrak{g}_0$. Then every $g \in G$ has the unique factorization

$$g = \exp(zZ)\exp(yY)\exp(w)\exp(xX),$$

with $x, y, z \in \mathbb{R}$ and $w \in W$. Consequently, every element in the closed and normal subgroup G_0 also admits a unique factorization of the type $g_0 = \exp(zZ)\exp(yY)\exp(w)$.

As a consequence of the factorizations, we obtain that G is the inner semidirect product $G = G_0 \rtimes \exp(\mathbb{R}X)$, which allows to use a specific realization of induced representations (see e.g. page 79 of [11], *Realization III for Semidirect Products*). The representation space can be taken as $\mathcal{H}_\pi = L^2(\mathbb{R}, \mathcal{H}_\tau)$, the space of weakly Borel-measurable $\mathcal{H}_\tau$-valued functions on $\mathbb{R}$ with square-integrable norms, and the

cited source provides the following explicit formulae

$$
[\pi\,(g)\,f]\,(t) = \begin{cases} f\,(t-x) \text{ if } g = \exp\,(xX) \\ e^{-2\pi i t y}\,f\,(t) \text{ if } g = \exp\,(yY) \\ \tau\left(\exp\left(e^{ad(-tX)}w\right)\right)f\,(t) \text{ if } g = \exp\,(w)\,,\,w \in W \end{cases} \qquad . \qquad (7)
$$

It is worth noting that π acts partially like a Schrödinger representation via $\exp(xX)$ and $\exp(yY)$.

Step 3 *Fixing the vector η* By Remark 11, there exists $\eta_1 \in L^2(\mathbb{R})$ with full support and phase retrieval properties for the Schrödinger representation. Furthermore, the inductive hypothesis provides $\eta_2 \in \mathcal{H}_\tau$ with full support and phase retrieval properties for τ. We then define $\eta \in L^2(\mathbb{R}, \mathcal{H}_\tau)$ by $\eta(t) = \eta_1(t)\eta_2$, and claim that it has the full support and phase retrieval properties for π.

Step 4 *Explicit formulae for matrix coefficients* Fix any nonzero $f \in L^2(\mathbb{R}, \mathcal{H}_\tau)$. By abuse of notation, we will systematically use

$$
V_\eta f(y, w, x),\ (y, w, x) \in \mathbb{R} \times W \times \mathbb{R}
$$

instead of

$$
V_\eta(\exp(yY)\exp(w)\exp(xX))
$$

We will also omit the central variable zZ from our discussion, in view of Remarks 6 and 10.

We then get from (7) that

$$
\begin{aligned}
V_\eta f(y, w, x) &= \langle f, \pi(\exp(yY)\exp(w)\exp(xX))\eta\rangle \\
&= \int_\mathbb{R} \left\langle f\,(t),\tau\left(\exp\left(e^{-ad(tX)}w\right)\right)\eta\,(t-x)\right\rangle e^{2\pi i y t}\,dt \\
&= \int_\mathbb{R} \left\langle f\,(t),\tau\left(\exp\left(e^{-ad(tX)}w\right)\right)\eta_2\right\rangle \overline{e^{2\pi i y t}\eta_1(t-x)}\,dt \\
&= \int_\mathbb{R} \langle f\,(t),\tau\,(\exp(-tX)\exp(w)\exp(tX))\,\eta_2\rangle\,\overline{e^{2\pi i y t}\eta_1(t-x)}\,dt.
\end{aligned}
$$

Now, using ϱ to denote the Schrödinger representation, as well as

$$
F : W \times \mathbb{R} \to \mathbb{C},\ F(w, t) = \langle f\,(t),\tau\,(\exp(-tX)\exp(w)\exp(tX))\,\eta_2\rangle \qquad (8)
$$

we may rewrite this formula as

$$
(V_\eta f)(y, w, x) = \left(V_{\eta_1}^\varrho F(w, \cdot)\right)(y, x). \qquad (9)
$$

In addition, we make the observation that

$$
F(w, t) = \left(V_{\eta_2}^\tau f(t)\right)(\exp(-tX)\exp(w)\exp(tX)). \qquad (10)
$$

Step 5 η *does phase retrieval* Now assume that $f, h \in L^2(\mathbb{R}, \mathcal{H}_\tau)$ are such that $|V_\eta f| = |V_\eta h|$ holds. With F from (8) and H defined analogously as

$$H : W \times \mathbb{R} \to \mathbb{C}, \; H(w, t) = \langle h(t), \tau(\exp(-tX)\exp(w)\exp(tX))\eta_2 \rangle$$

Equation (9) gives for all $w \in W$

$$\left| V_{\eta_1}^\varrho (F(w, \cdot)) \right| = \left| V_{\eta_1}^\varrho (H(w, \cdot)) \right|.$$

Since η_1 does phase retrieval, this implies the existence of a map

$$u : W \to \mathbb{T}, \; H(w, \cdot) = u(w)F(w, \cdot) \;\; \forall w \in W. \tag{11}$$

It follows for almost all $t \in \mathbb{R}$ that

$$|H(\cdot, t)| = |F(\cdot, t)|.$$

By construction, $\exp(W) \subset G_0$ is a system of representatives modulo the central subgroup $\exp(\mathbb{R}Z)\exp(\mathbb{R}Y)$ of G_0, which is contained in the projective kernel of τ. Hence Eq. (10) (and its analog for H) allows to rewrite the previous equation as follows, for almost all $t \in \mathbb{R}$:

$$\forall g_0 \in G_0 : \; \left| V_{\eta_2}^\tau (f(t))(\exp(-tX)g_0 \exp(tX)) \right| = \left| V_{\eta_2}^\tau (h(t))(\exp(-tX)g_0 \exp(tX)) \right|.$$

For fixed $t \in \mathbb{R}$, conjugation by $\exp(tX)$ is a bijection of G_0 onto itself, hence we may simplify this equation to

$$\left| V_{\eta_2}^\tau (f(t)) \right| \equiv \left| V_{\eta_2}^\tau (h(t)) \right|.$$

Now we can appeal to the phase retrieval property of η_2 to conclude the existence of a map

$$v : \mathbb{R} \to \mathbb{T}, \; h(t) = v(t)f(t) \tag{12}$$

with the equality holding for almost every $t \in \mathbb{R}$. Note that this also entails, for almost every t, that

$$H(\cdot, t) = v(t)G(\cdot, t).$$

Defining the Borel set

$$C_f = \{t \in \mathbb{R} : f(t) \neq 0\} \subset \mathbb{R}, \tag{13}$$

(12) shows that the proof of phase retrieval boils down to showing that v is constant on C_f. Note that by removing a set of measure zero from C_f we can assume that (12) holds for all $t \in C_f$.

At this point the full support property of η_2 enters the picture. Picking any $t \in C_f$, Eq. (8) and the full support property of η_2 implies that the set

$$W_f(t) = \{w \in W : F(w, t) \neq 0\}$$

has full measure. Note that this step also used the fact that the automorphism of G_0 induced by conjugation with $\exp(tX)$ preserves the Haar measure of G_0, and Remark 10.

Hence, picking $t_1, t_2 \in C_f$ and any w in $W_f(t_1) \cap W_f(t_2)$ (which is of full measure, hence nonempty), we obtain from (11)

$$v(t_i)F(w, t_i) = H(w, t_i) = u(w)F(w, t_i).$$

By choice of w, we may cancel $F(w, t_i)$ on both sides, to obtain $v(t_1) = u(w) = v(t_2)$. This concludes the proof of phase retrieval.

Step 6 η *has the full support property* Let $0 \neq f \in L^2(\mathbb{R}, \mathcal{H}_\tau)$ be given, and let C_f be as in (13). We will prove that the set

$$\big\{(y, w, x) \in \mathbb{R} \times W \times \mathbb{R} : V_\eta f(y, w, x) = 0\big\}$$

has measure zero. Then an appeal to Remark 10 finishes the proof.

Given any $w \in W$, Eq. (9) together with the full support property of η_1 shows that

$$\big\{(y, x) \in \mathbb{R} \times \mathbb{R} : V_\eta f(y, w, x) = 0\big\}$$

has measure zero iff

$$\|F(w, \cdot)\|_{L^2(\mathbb{R})} \neq 0,$$

with the function F from (8).

Thus by Fubini's theorem, the full support property for η is shown once we establish that

$$\left\{w \in W : \int_{\mathbb{R}} |F(w, t)|^2 dt = 0\right\}$$

has measure zero. For this purpose, introduce the set

$$B_f = \{(w, t) \in W \times C_f : F(w, t) = 0\},$$

with C_f defined in Step 5. We also introduce the auxiliary function

$$\tilde{F}(w, t) = \left(V_{\eta_2}^\tau f(t)\right)(\exp(w))$$

and associated set

$$\tilde{B}_f = \{(w, t) \in W \times C_f : \tilde{F}(w, t) = 0\}.$$

Given $t \in \mathbb{R}$, consider the map $\alpha(t) : W \to W$ defined as

$$\alpha(t)(w) = P_W \left(e^{-ad(tX)} w \right)$$

where P_W is the projection onto W inside $\mathfrak{g}_0$, along the complement $\mathbb{R}Z \oplus \mathbb{R}Y$. Then by definition of $\alpha(t)$, we have

$$\exp(\alpha(t)w)^{-1} \exp(-tX) \exp(w) \exp(tX) \in Z(G_0),$$

and since τ restricted to $Z(G_0)$ is a character, this gives rise to the equation

$$|F(w, t)| = |\tilde{F}(\alpha(t)w, t)|.$$

We also note that $\alpha(t)$ is a diffeomorphism, with inverse map given by $\alpha(-t)$.

These observations allow to write

$$B_f = \{(w, t) \in W \times C_f : (\alpha(t)w, t) \in \tilde{B}_f\}. \tag{14}$$

The whole point of introducing $\tilde{B}_f$ was that the assumption that η_2 has the full support property, and the definition of C_f, imply that $\tilde{B}_f$ is a set of measure zero, by Fubini's theorem. It then follows by (14), a change of variable involving the $\alpha(t)$, and yet another application of Fubini's theorem, that B_f has measure zero. A final application of Fubini's theorem then yields a set $W' \subset W$ of full measure such that $F(w, \cdot)$ vanishes almost nowhere on C_f, for all $w \in W'$. Since C_f is of positive measure, this finally implies

$$\int_{\mathbb{R}} |F(w, t)|^2 dt > 0$$

for all $w \in W'$, and the proof is finished. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

3 Finite Nilpotent Groups

This section is devoted to establishing analogs of Theorem 12 for finite nilpotent groups. While we will not be able to cover all finite nilpotent groups, we will exhibit large classes of such groups, for which an analog can be formulated and proved, using an inductive method that is quite similar to that employed for Lie groups.

The following theorem contains the largest previously known class of finite groups for which phase retrieval is established:

Theorem 13 *Let G denote a finite nilpotent group of nilpotency class 2, which means that G is nonabelian, and $G/Z(G)$ is abelian. Then every irreducible representation of G does phase retrieval.*

This theorem is a consequence of Theorem 1.7 from [12], which states that every projective irreducible representation of a finite abelian group does phase retrieval, combined with the natural correspondence between projective representations of finite abelian groups and unitary representations of class 2 nilpotent groups. Our results will significantly extend this class of examples.

Recall that a *p*-group is a group G with cardinality p^r, for some positive exponent $r > 0$ and prime number p. If p^k is the highest power of some prime number p dividing the order of G, then a subgroup of G of order p^k is called a *p*-Sylow subgroup of G. The *exponent* of a group G is the smallest integer n satisfying $x^n = e$ for all $x \in G$. Clearly, the exponent of a *p*-group is again a power of p.

The treatment of general finite nilpotent groups is easily reduced to that of *p*-groups, by the following well-known observation (see e.g. Theorems 5.2.4 and 8.4.2 of [16]).

Theorem 14 *Every finite nilpotent group G is the direct product of its p-Sylow subgroups. As a consequence, every irreducible representation of G is the outer tensor product of irreducible representations of its p-Sylow subgroups.*

The following Lemma is a direct consequence of Lemma 5, which immediately gives a solution for the phase retrieval problem for tensor product representations in terms of solutions for the factors. Since it directly generalizes to finitely many tensor factors, this lemma reduces the phase retrieval problem for irreducible representation of general finite nilpotent groups to the *p*-group case, on which we shall subsequently concentrate.

Lemma 15 *For $k = 1, 2$, let π_k be a unitary representation of some finite group G_k and suppose that each π_k does phase retrieval and is realized is some Hilbert space $\mathcal{H}_{\pi_k}$. Next, let $\pi = \pi_1 \otimes \pi_2$ be the outer tensor product of π_1 and π_2. If η_1 does phase retrieval for π_1 and if η_2 does phase retrieval for π_2 then $\eta_1 \otimes \eta_2 \in \mathcal{H}$ does phase retrieval for π.*

Before we turn to the study of phase retrieval properties for *p*-groups, we will need to establish several auxiliary notions and results. To a large part, these notions are motivated by the desire to adapt the inductive approach developed for the Lie group case to the *p*-group setting. They mostly concern the inductive construction of irreducible representations. But we will also need a finite group analog to the full support property, which is necessarily of a more quantitative nature. We start by formulating this analog:

Definition 16 Let $(\pi, \mathcal{H}_\pi)$ denote a unitary representation of a finite group G. Given a vector $\eta \in \mathcal{H}_\pi$, we let

$$p_0(\pi, \eta) = \max_{f \in \mathcal{H}_\pi \setminus \{0\}} \left(1 - \frac{|\operatorname{supp}(V_\eta f)|}{|G|} \right)$$

as well as

$$p_0(\pi) = \min\{p_0(\pi, \eta) : \eta \in \mathcal{H}_\pi \setminus \{0\}\}.$$

The following remark formulates an analog to Remark 6 for the quantity p_0:

Remark 17 Let π be a representation of a finite group G, and $K \lhd G$ is a normal subgroup contained in the projective kernel of π. Picking any system $W \subset G$ of representatives modulo K, it is easy to see that

$$p_0(\pi, \eta) = \max_{f \in \mathcal{H}_\pi \setminus \{0\}} \left(1 - \frac{\left|\operatorname{supp}\left((V_\eta f)|_W\right)\right|}{|W|} \right)$$

Remark 18 $p_0(\pi, \eta)$ can be interpreted as the maximal proportion of zeros occurring in the matrix coefficients $V_\eta f$ for an arbitrary nonzero vector f. This quantity is therefore related to sampling sets: For any set $A \subset G$ satisfying $|A| > p_0(\pi, \eta)|G|$, the sampled coefficient map

$$V_\eta|_A : f \mapsto (V_\eta f)|_A$$

has trivial kernel by definition of $p_0(\pi, \eta)$, hence it is injective.

This property is also related to the full spark property, studied in the representation theoretic context in [13, 14]. In fact, for any representation π having the full spark property, one can derive

$$p_0(\pi) = \frac{d_\pi - 1}{|G|}.$$

A related result was derived by Malikiosis in [13], who showed that, for suitable choices of $\eta \in \mathbb{C}^n$ the system $(\pi(k, l, 0)\eta)_{k,l \in \mathbb{Z}_n}$ has the full spark property, where π is the Schrödinger representation from Example 1, associated to the finite cyclic group $\mathbb{Z}_n$ of order n. Since $W = \{(k, l, 0) : k, l = 0, \ldots, n-1\} \subset \mathbb{H}_n$ is a system of representatives modulo the center of $\mathbb{H}$, which is contained in the projective kernel of π, Remark 17 allows to determine

$$p_0(\pi) = \frac{n-1}{n^2}. \tag{15}$$

Remark 19 In our subsequent arguments (see Lemma 29 below), an upper estimate for the quantity $p_0(\tau)$ for a certain representation of a suitably chosen subgroup G_0 of G will play an important role, as a sufficient condition for phase retrieval. It is noteworthy that the phase retrieval property of π entails a necessary upper estimate for $p_0(\pi)$, as follows: Assuming that the vector $\eta \in \mathcal{H}_\pi$ does phase retrieval for π, Lemma 4(b) implies that for any nonzero $f, g \in \mathcal{H}_\pi$, the pointwise product $(V_\eta f) \cdot (V_\eta g)$ is not identically zero. Letting $A = \operatorname{supp}(V_\eta f) \subset G$ and $g = \pi(y)f$ for $y \in G$ yields via

$$V_\eta g(x) = \langle \pi(y)f, \pi(x)\eta \rangle = V_\eta f(y^{-1}x)$$

that $yA \cap A \neq \emptyset$, or equivalently: $y \in A \cdot A^{-1}$. Hence we have shown

$$A \cdot A^{-1} = G,$$

for the support A of any nonzero matrix coefficient $V_\eta f$. This observation, together with Remark 18, allows to derive the estimate

$$p_0(\pi, \eta) \leq 1 - |G/K|^{-1/2},$$

where $K \lhd G$ denotes the projective kernel of π.

It should be noted however that this bound is generally much weaker than the upper bound of $1/2$ that will become relevant below.

For the formulation of the next lemma, we introduce a new piece of terminology: Given a finite dimensional complex Hilbert space $\mathcal{H}$, we call a set $M \subset \mathcal{H}$ *real Zariski closed* if there exist mappings

$$f_1, \ldots, f_k : \mathcal{H} \to \mathbb{R}$$

that depend polynomially on the real and imaginary parts of arbitrarily chosen complex linear coordinates on $\mathcal{H}$, and such that

$$M = \{x \in \mathcal{H} : f_1(x) = \ldots = f_k(x) = 0\}.$$

We call M *real Zariski open* if its complement is real Zariski closed.

Lemma 20 *Let $(\pi, \mathcal{H}_\pi)$ denote a finite-dimensional representation of the finite group G. Let*

$$M_1 = \{\eta \in \mathcal{H}_\pi : \eta \text{ does phase retrieval }\}$$

and

$$M_2 = \{\eta \in \mathcal{H}_\pi : p_0(\pi, \eta) = p_0(\pi)\}.$$

Then M_1 and M_2 are real Zariski open. If π does phase retrieval, then $M_1 \cap M_2$ is nonempty and real Zariski open. In particular $M_1 \cap M_2 \subset \mathcal{H}_\pi$ is of full Lebesgue measure.

Proof For the statement concerning M_1 we refer to Lemma 2.5 of [4]. For M_2, we identify $\mathcal{H}_\pi$ with $\mathbb{C}^{d_\pi}$ (using any choice of basis in $\mathcal{H}_\pi$), identify $\mathbb{C}^G$ with $\mathbb{C}^{|G|}$ by a similar procedure, and use these identifications to associate to the linear operator $V_\eta : \mathbb{C}^{d_\pi} \to \mathbb{C}^G$ the describing matrix $\mathcal{A}_\eta \in \mathbb{C}^{|G| \times d_\pi}$. Given any matrix $\mathcal{A} \in \mathbb{C}^{|G| \times d_\pi}$, and an arbitrary set $B \subset \{1, \ldots, |G|\}$, we let $\mathcal{A}^B$ denote the submatrix obtained by picking the lines of $\mathcal{A}$ corresponding to indices contained in B. Then

$$p_0(\pi, \eta) \leq \frac{k}{|G|}$$

is equivalent to the statement that, for arbitrary sets $B \subset \{1, \ldots, |G|\}$ of cardinality $k + 1$, the submatrix $\mathcal{A}_\eta^B$ has rank d_π. But the set

$$\mathcal{Z}_k = \left\{ \mathcal{A} \in \mathbb{C}^{|G| \times d_\pi} : \forall B \subset \{1, \ldots, |G|\} \text{ with } |B| = k + 1, \ \text{rank}(\mathcal{A}^B) = d_\pi \right\}$$

can be described in terms of $d_\pi \times d_\pi$-subdeterminants, hence is real Zariski-open. Now we have that

$$p_0(\pi, \eta) = p_0(\pi) \Leftrightarrow p_0(\pi, \eta) \leq p_0(\pi)$$
$$\Leftrightarrow \mathcal{A}_\eta \in \mathcal{Z}_{\pi_0(\pi)|G|}.$$

Since the map $\eta \mapsto A_\eta$ is conjugate linear, we see that M_2 is the conjugate linear preimage of a real Zariski open set, hence real Zariski open itself. Now if π does phase retrieval, then M_1 is nonempty, whereas M_2 is nonempty by definition. Nonempty real Zariski open sets are open and dense in the standard topology; in fact they are of full Lebesgue measure. Then $M_1 \cap M_2$ is nonempty, and real Zariski-open, hence it inherits the remaining properties as well. □

We will now start to introduce the central device of our treatment of p-groups, namely a version of Kirillov's lemma for this class of groups. For this purpose, we introduce further notation. Let G denote a nonabelian p-group. Let $[w, y] = w^{-1}y^{-1}wy$ be the commutator of $w, y \in G$. Furthermore, write $w^y = y^{-1}wy$ for the conjugation product of w and y. We then have the well-known relations

$$[xz, y] = [x, y]^z[z, y], \quad [x, zy] = [x, y][x, z]^y, \tag{16}$$

which can be verified by direct calculation.

We introduce

$$Z_1(G) = \{y \in G : yZ(G) \in Z(G/Z(G))\}.$$

Since G is nilpotent, $G/Z(G)$ is as well. In particular, $G/Z(G)$ has nontrivial center, which implies that $Z(G) \subsetneq Z_1(G)$, unless G is abelian. The following elementary lemma will be used repeatedly:

Lemma 21 *The mapping*

$$[\cdot, \cdot] : G \times Z_1(G) \to Z(G), \quad (x, y) \mapsto [x, y]$$

is a well-defined bihomomorphism, i.e., for all $x \in G$, $y \in Z_1(G)$, the maps $[x, \cdot]$ and $[\cdot, y]$ are homomorphisms into $Z(G)$.

Proof Let $x \in G$, $y \in Z_1(G)$. The fact that $yZ(G)$ is central in $G/Z(G)$ implies

$$[x, y]Z(G) = [xZ(G), yZ(G)] = e_G Z(G),$$

hence $[x, y] \in Z(G)$, and $[\cdot, \cdot] : G \times Z_1(G) \to Z(G)$ is well-defined. Furthermore, (16) yields for $x, z \in G$

$$[xz, y] = [x, y]^z [z, y] = [x, y][z, y],$$

since the conjugation action is trivial on $[x, y] \in Z(G)$. If $z \in Z_1(G)$, we similarly get

$$[x, zy] = [x, y][x, z]^y = [x, y][x, z] = [x, z][x, y],$$

since $Z(G)$ is abelian. $\square$

The following is the announced p-group analog of Kirillov's lemma for nilpotent Lie groups [7, Lemma 1.1.12].

Lemma 22 *Let G be a non-abelian p-group with cyclic center $Z(G)$. Then there exist $z \in Z(G)$, $y \in Z_1(G)$ and $x \in G$ as well as an integer $r \geq 1$ such that the following hold:*

(a) $z = [x, y]$, $\langle z \rangle$ *is a subgroup of $Z(G)$ with* $\langle z \rangle = [G, y] \cong \mathbb{Z}_{p^r}$.
(b) $A = \langle y, Z(G) \rangle$ *is an abelian normal subgroup of G with* $A/Z(G) = \langle yZ(G) \rangle \cong \mathbb{Z}_{p^r}$.
(c) *Define* $G_0 = \{w : [w, y] = e_G\}$. *Then G_0 is a normal subgroup of G with* $G/G_0 = \langle xG_0 \rangle \cong \mathbb{Z}_{p^r}$. $A < G_0$ *is central.*

Proof Proof of Part (a): Pick any $y \in Z_1(G) \setminus Z(G)$. By Lemma 21, $[G, y]$ is a subgroup contained in the center $Z(G)$. Since the center of G is assumed to be cyclic, $[G, y]$ is cyclic as well, hence $[G, y] \cong \mathbb{Z}_{p^r}$ for some natural number r, since G is a p-group. The case $r = 0$ is equivalent to $[G, y] = \{e\}$, or $y \in Z(G)$, contrary to the choice of y. The existence of z and x is then obvious.

Proof of Part (b): It is clear that A is an abelian subgroup of G. Fixing $w \in G$, and appealing to Lemma 21, we obtain

$$w^{-1}yw = \left[w, y^{-1}\right]y = \underbrace{[w, y]^{-1}}_{\in Z(G)} y \in A.$$

This implies that $\langle y, Z(G) \rangle$ is normal. To complete the proof of Part (b), we show that $yZ(G)$ has order p^r in $G/Z(G)$. In order to see this, we use Lemma 21 to compute $[x, y^l] = [x, y]^l = z^l \neq e_G$ for $1 \leq l < p^r$, by choice of z. This shows in particular $y^l \notin Z(G)$.

On the other hand, assuming $y^{p^r} \notin Z(G)$ would entail the existence of $w \in G$ with $e_G \neq [w, y^{p^r}] = [w, y]^{p^r}$. This would imply that $[w, y] \in [G, y]$ has order $> p^r$, which contradicts (a).

Proof of Part (c): Note that by definition, G_0 is the kernel of the homomorphism $[\cdot, y] : G \to Z(G)$, which has image $[G, y]$, generated by $z = [x, y]$. Hence G_0 is a normal subgroup, and $\langle xG_0 \rangle = G/G_0 \cong \langle z \rangle \cong \mathbb{Z}_{p^r}$ follows by the first homomorphism theorem. y is central in G_0 by definition of the latter, and $Z(G) \subset G_0$ is central even in G, hence $A = \langle y, Z(G) \rangle$ is central in G_0. $\square$

Remark 23 We note that the case $[G, y] \subsetneq Z(G)$ may well occur. For a concrete example, fix a prime number p and consider $G = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$, with group law

$$(k, l, m) \cdot (k', l', m') = (k + k', l + l', m + m' - pl'k).$$

The center of this group is given by $\{0\} \times \{0\} \times \mathbb{Z}_{p^2}$, whereas $[G, y] = \langle (0, 0, p) \rangle$.

The notation of the lemma suggests that the group $H = \langle x, y, z \rangle$, for x, y, z from Lemma 22 is isomorphic to a Heisenberg group. Note that the analogous statement in the Lie group case, i.e. that the closed subgroup associated to the Lie subalgebra generated by X, Y, Z is isomorphic to the three-dimensional Heisenberg group, holds true. The next example shows however that the p-group case is more diverse. Nevertheless the Schrödinger representations from Example 1 constitute important basic building blocks in our inductive strategy to establish phase retrieval for more general p-groups, and the following example is intended to shed some light on this phenomenon.

Example 24 Let $H = \mathbb{H}_{p^r}$ denote a finite Heisenberg group associated to the cyclic group $\mathbb{Z}_{p^r}$, as given by (1) and (2). Define $x = (1, 0, 0)$, $y = (0, 1, 0)$ and $z = (0, 0, -1)$. Then one has $Z(H) = \langle z \rangle = Z_0$,

$$Z_1(H) = H = \langle x, y, z \rangle = \langle x, y \rangle,$$

and $[x, y] = z$, as well as all the other properties from Lemma 22. It is tempting to assume that the relations in this lemma already characterize H up to isomorphism.

But this is not the case. For the construction of a counterexample, fix a prime number p and an integer $r \geq 1$. Consider the group $G = \mathbb{Z}_{p^{2r}} \times \mathbb{Z}_{p^r}$, with group law

$$(k, l)(k', l') = (k + (1 - lp^r)k', l + l'), \ 0 \leq k, k' < p^{2r}, \ 0 \leq l, l' < p^r, \quad (17)$$

where the operations on the right-hand side are taken modulo p^{2r}, p^r, respectively. Using

$$(1 - lp^r)(1 - l'p^r) \equiv 1 - (l + l')p^r \mod p^{2r},$$

one easily verifies that (17) is a well-defined group law. We let $x = (0, 1)$, $y = (1, 0)$ and $z = (p^r, 0)$, and obtain that $Z(G) = \langle z \rangle = Z_0$,

$$Z_1(G) = G = \langle x, y, z \rangle = \langle x, y \rangle = \langle y \rangle \rtimes \langle x \rangle,$$

as well as $[x, y] = z$.

Again, all remaining properties noted in Lemma 22 hold for x, y, z also. Nonetheless, G is clearly not isomorphic to the Heisenberg group H, since it contains elements of order p^{2r}.

In order to exhibit similarities of the newly constructed group to the Heisenberg group case, we now determine certain irreducible unitary representations of G. Letting

$A = \langle y, z \rangle = \mathbb{Z}_{p^{2r}} \times \{0\} \cong \mathbb{Z}_{p^{2r}}$, we let $\xi \in \mathbb{T}$ be a root of unity of order p^{2r}, and define the associated character $\chi_\xi \in \widehat{A}$ as

$$\chi_\xi(k, 0) = \xi^k, \ k = 0, \dots, p^{2r} - 1.$$

The dual action of x on the characters is given by

$$x^l * \chi_\xi(k, 0) = \chi_\xi((0, -l)(k, 0)(0, l)) = \xi^{k(1 + lp^r)} = \chi_{\xi^{1+lp^r}}(k, 0).$$

Now let ξ_0 denote an arbitrary *primitive root of order p^{2r}*. Then we have for $0 \leq l < p^r$ that

$$\xi_0^{(1+lp^r)} = \xi_0 \Longleftrightarrow \xi_0^{lp^r} = 1 \Longleftrightarrow l = 0,$$

i.e., the stabilizer of ξ_0 under the dual action is trivial.

We now consider $\pi = \mathrm{ind}_A^G \chi_{\xi_0}$. By Mackey's theorem, π is an irreducible representation, and since $\langle y, z \rangle$ is a normal subgroup, we can realize π on $l^2(G/A) = l^2(\langle x \rangle)$ by the formula from page 79 of [11], which yields

$$\left[\pi(y^k x^l) \varphi \right](x^j) = \chi_{\xi_0}(x^{-j} y^k x^j) \varphi(x^{j-l}).$$

Since $[x, y] = z$, $x^{-j}(y^k) x^j = y^k z^{-kj}$, and we obtain

$$\left[\pi(y^k x^l) \varphi \right](x^j) = \chi_{\xi_0}(y^k z^{-kj}) \varphi(x^{j-l})$$
$$= \xi_0^k \xi_1^{-kj} \varphi(x^{j-l})$$

where $\xi_1 = \xi_0^{p^r}$ is a *primitive root of order p^r*. This observation may be rephrased as

$$\pi(y^k x^l) = \alpha(k, l) M_k T_l,$$

with $\alpha(k, l) \in \mathbb{T}$. This shows that, even though G and H are clearly non-isomorphic, the operators in the realization of π differ from a Schrödinger representation only by scalar factors, and Lemma 4 (c) entails that the vectors doing phase retrieval for π are precisely the ones that do phase retrieval for the Schrödinger representation.

The next definition introduces a bookkeeping device, intended to describe the construction of an arbitrary irreducible representations by repeated induction steps.

Definition 25 Let G denote a p-group, and π an irreducible, faithful representation of G. (G_0, r, τ) is called a *K-triple for π* if $r \in \mathbb{N}$, $G_0 \lhd G$, τ is a representation of G_0 such that $\pi \simeq \mathrm{ind}_{G_0}^G \tau$, and there exist $x \in G$, $y \in Z_1(G) \backslash Z(G)$ and $z \in Z(G)$ with the following properties:

  (i) $[x, y] = z$, and $\langle z \rangle = [G, y] \cong \mathbb{Z}_{p^r}$.
  (ii) G_0 is the centralizer of y.

(iii) $G/G_0 = \langle xG_0 \rangle \cong \mathbb{Z}_{p^r}$.

The K-triple is called *split*, if x can be chosen such that $x^{p^r} = e$.

It is easy to see that a K-triple (G_0, r, τ) is split if and only if the short exact sequence

$$1 \rightarrow G_0 \rightarrow G \rightarrow G/G_0 \rightarrow 1$$

splits, i.e. when G is the inner semidirect product $G_0 \rtimes \langle x' \rangle$ for a suitable choice of x'. Here the "only if"-part is clear. For the converse, assume that a K-triple (G_0, r, τ) is given, and that in addition $G = G_0 \rtimes \langle x' \rangle$ for a suitable choice of x'. This entails in particular that x' has order p^r. Since G_0 is by definition the kernel of the homomorphism $[\cdot, y] : G \rightarrow \langle z \rangle$, we get that $s \mapsto [(x')^s, y] \in \langle z \rangle$ is onto, hence $z' = [x', y]$ fulfills $\langle z' \rangle = \langle z \rangle$. This shows that $x', y, z' \in G$ have the properties required of x, y, z in Definition 25 to show that (G_0, r, τ) is a split K-triple.

The following lemma provides a central result for our inductive approach. It is the p-group analog to Step 1 in the proof of Theorem 12, and its proof is remarkably similar to the proof for the Lie group setting.

Lemma 26 *Let G denote a nonabelian p-group, and π a faithful irreducible representation of G. Then there exists a K-triple for π.*

Proof Since π is irreducible, $\pi(Z(G))$ is a (finite) subgroup of the torus. It follows that $\pi(Z(G))$ is cyclic, and by faithfulness of π, this entails that $Z(G)$ is cyclic. Hence Lemma 22 is applicable, and we obtain the group elements x, y, z, as well as the normal subgroup G_0 and $r \in \mathbb{N}$ such that the properties (i)–(iii) from Definition 25 are fulfilled. It therefore remains to prove the existence of τ. Note that G_0 is the centralizer of y by its definition in part (c) of the lemma.

Let $A = \langle y, Z(G) \rangle$. Then A is an abelian normal subgroup of G. Note that this fact can be concluded from the choice according to Lemma 22, but it also follows from $z = [x, y] \in Z(G)$ and the choice of G_0 as centralizer of y. In a similar way, A is seen to be central in G_0.

For any given unitary character χ of A, G acts on χ via the dual action which is defined as follows. For arbitrary $g \in G$ and $a \in A$, $[g \star \chi](a) = \chi(g^{-1}ag)$. Let $G_\chi = \{g \in G : g \star \chi = \chi\}$ be the stabilizer of χ and let

$$\widetilde{G}_\chi = \left\{ \tau \in \widehat{G_\chi} : \tau|_A \text{ is a multiple of } \chi \right\},$$

where $\widehat{G}_\chi$ denotes the set of (equivalence classes of) irreducible representations of G_χ. For $\tau \in \widetilde{G}_\chi$, $\pi_\tau = \mathrm{ind}_{G_\chi}^G (\tau)$ is an irreducible representation of G. In fact, according to the theory of Mackey [11, Theorem 4.22], every irreducible representation of G is of this form.

Hence $\pi \simeq \mathrm{ind}_{G_\chi}^G (\tau)$ for suitable $\chi \in \widehat{A}$ and $\tau \in \widetilde{G}_\chi$. The proof is finished when we have shown that $G_\chi = G_0$. By condition (ii), A is central in G_0, which means that the conjugation action of G_0 on A is trivial. The same then follows for the dual action on $\widehat{A}$, which establishes $G_0 \subset G_\chi$.

In order to show the reverse inclusion, we take a closer look at the dual action of x and its powers. By Lemma 8 applied with $Z = Z(G)$ and $N = G_0$, the characters obtained by restricting either π or τ to $Z(G)$ must coincide. By assumption, π is faithful, hence $\tau|_{Z_0}$ is faithful. Since $Z_0 = \langle z \rangle$, we get that $\tau(z^k) = \xi^k$, for a suitable p^r th root of unity $\xi \in \mathbb{T}$. In fact, faithfulness requires that ξ is a *primitive root of unity of order p^r*, i.e. $\xi^k = 1$ holds iff p^r divides k, for all $k \in \mathbb{Z}$.

Since $y \in Z_1(G)$, we can appeal to Lemma 21 to compute $x^{-m} y x^m = [x^m, y^{-1}] y = z^{-m} y$ which leads to

$$(x^m \star \chi)(y) = \chi(z^{-m})\chi(y) = \xi^{-m} \chi(y).$$

Hence $x^m \star \chi = \chi$ entails $\xi^{-m} = 1$, and since ξ is a primitive root of order p^r, this only happens for $m \in p^r \mathbb{Z}$.

By (iii), every $g \in G$ can be factored uniquely as $g = x^m g_0$, with $g_0 \in G_0 \subset G_\chi$ and $0 \leq m < p^r$. This implies that

$$\chi = g \star \chi = x^m \star \chi$$

holds iff $m = 0$, or equivalently, iff $g \in G_0$. This proves $G_0 = G_\chi$ and thus $\pi \simeq \mathrm{ind}_{G_0}^G \tau$. $\qquad\square$

We next provide an explicit description of the representation π in terms of the data provided by a K-triple. It is again quite analogous to the Lie group case, but this time the analogy requires an additional assumption (which is automatic in the Lie group setting), namely that the group extension $1 \to G_0 \to G \to G/G_0 \to 1$ splits.

Lemma 27 *Let G denote a p-group, and π an irreducible, faithful representation of G, with a split K-triple (G_0, r, τ). Let $x, y, z \in G$ denote the group elements associated to the triple according to Definition 25, with the property $x^{p^r} = e$.*

(a) *Let $W \subset G_0$ denote a system of representatives modulo $\langle \{y\} \cup Z(G) \rangle$. Then every element $g \in G$ has a unique factorization*

$$g = z' y^k w x^l, \ z' \in Z(G), \ k, l \in \{0, \ldots p^r - 1\}, \ w \in W.$$

(b) *The representation $\mathrm{ind}_{G_0}^G \tau$ acts in the Hilbert space $l^2\left(\mathbb{Z}_{p^r}, \mathcal{H}_\tau\right)$ by the formula*

$$\left[\pi\left(y^k w x^l\right)\varphi\right](j) = \xi_1^k \xi_2^{-kj} \tau\left(x^{-j} w x^j\right)\varphi(j - l),$$

where $\xi_1 \in \mathbb{T}$ is a suitable root of unity, and ξ_2 is a primitive root of unity of order p^r.

Proof Part (a) follows from properties (i)–(iii), and the choice of W.

For part (b), we use the semidirect product structure $G = G_0 \rtimes \langle x \rangle$, and again appeal to the realization of induced representations for semidirect products, elaborated on [11, p. 79]. We identify the quotient G/G_0 with the cyclic group $\mathbb{Z}_{p^r}$, using the

identification $x^j G_0 \mapsto j$. Letting $w \in W$ and $\varphi \in l^2\left(\mathbb{Z}_{p^r}, \mathcal{H}_\tau\right)$, we get by the cited result that

$$\left[\pi\left(y^k w x^l\right)\varphi\right](j) = \tau\left(x^{-j}\left(y^k w\right)x^j\right)\varphi(j-l)$$

for $(k, w, l) \in \mathbb{Z}_{p^r} \times W \times \mathbb{Z}_{p^r}$, $j \in \mathbb{Z}_{p^r}$. Since $[x, y] = z$, we get $x^{-j}y^k x^j = y^k z^{-kj}$ and

$$\begin{aligned}
\pi\left(y^k w x^l\right)\varphi\left(x^j\right) &= \tau\left(x^{-j}y^k x^j\right)\circ\tau\left(x^{-j}w x^j\right)\varphi(j-l)\\
&= \chi\left(y^k z^{-kj}\right)\cdot\tau\left(x^{-j}(w)x^j\right)\varphi(j-l)\\
&= \chi\left(y^k\right)\cdot\chi\left(z^{-kj}\right)\cdot\tau\left(x^{-j}w x^j\right)\varphi(j-l). \quad (18)
\end{aligned}$$

Here $\chi : A \to \mathbb{T}$ denotes the character obtained by restricting the irreducible representation τ to the central subgroup A. Since π is faithful, Lemma 8 implies that τ is faithful on $Z(G)$. Hence, as z has order p^r, there exists a primitive root of unity ξ_2 of order p^r such that

$$\tau(z^l) = \xi_2^l.$$

Furthermore $\chi\left(y^k\right) = \xi_1^k$ for a suitable root of unity, whose order is at most the order of y. $\qquad\square$

Lemma 28 *Let G denote a p-group, and π an irreducible, faithful representation of G, with K-triple (G_0, r, τ). Let $W \subset G_0$ denote a system of representatives modulo $\langle\{y\} \cup Z(G)\rangle$, where $y \in Z_1(G)$ denotes the group element associated to the triple according to Definition 25. Then there exist mappings $\alpha_j : W \to W$ and $\beta_j : W \to \langle\{y\} \cup Z(G)\rangle$, $j = 0, \ldots, p^r - 1$ such that*

$$\forall j = 0, \ldots, p^r - 1, \ \forall w \in W : \ x^{-j}w x^j = \beta_j(w)\alpha_j(w).$$

In addition, α_j is bijective.

Proof Since $\langle y, z\rangle$ is normal in G, it is invariant under conjugation with x^j. Hence this conjugation induces an automorphism of the quotient group $G_0/\langle\{y\} \cup Z(G)\rangle$. This in turn yields the factorization stated in the lemma, with a bijection α_j. $\qquad\square$

We can now formulate a sufficient criterion for π to do phase retrieval, based on suitable assumptions on the associated K-triple. The reasoning is rather similar to Step 5 in the proof of Theorem 12.

Lemma 29 *Let G denote a p-group, and π an irreducible, faithful representation of G, with a split K-triple (G_0, r, τ). Assume that τ does phase retrieval, and that π is given by the realization from Lemma 27.*

(a) *Assume that $p_0(\tau) < 1/2$. If $\eta_1 \in l^2(\mathbb{Z}_{p^r})$ has the phase retrieval property for the Schrödinger representation, and $\eta_2 \in \mathcal{H}_\tau$ has the phase retrieval property for τ, and additionally $p_0(\tau, \eta_2) < 1/2$, the vector*

$$\eta \in l^2\left(\mathbb{Z}_{p^r}, \mathcal{H}_\tau\right), \ \eta(j) = \eta_1(j) \cdot \eta_2$$

does phase retrieval property for π. Such vectors exist.

(b) *Pick any system $W \subset G_0$ of representatives modulo $\langle\{y\} \cup Z(G)\rangle$, where $x, y \in G$ are associated to the K-triple according to Definition 25. Assume that*

$$\forall w \in W : \ \alpha_1(w) = w$$

holds, where $\alpha_1 : W \to W$ is the bijection from Lemma 28. If $\eta_1 \in l^2(\mathbb{Z}_{p^r})$ has the phase retrieval property for the Schrödinger representation, and $\eta_2 \in \mathcal{H}_\tau$ has the phase retrieval property for τ, the vector

$$\eta \in l^2\left(\mathbb{Z}_{p^r}, \mathcal{H}_\tau\right), \ \eta(j) = \eta_1(j) \cdot \eta_2$$

has the phase retrieval property for π.

Proof We first derive formulae for matrix coefficients, which are valid for both cases under consideration. Given $\eta = \eta_1 \cdot \eta_2$ with $\eta_1 \in l^2(\mathbb{Z}_{p^r})$ and $\eta_2 \in \mathcal{H}_\tau$, the matrix coefficient of $f \in l^2(\mathbb{Z}_{p^r}, \mathcal{H}_\tau)$ is computed in the following two-step procedure: Using Lemma 27 for all $k, l = 0, \ldots, p^r - 1$, with suitable choices of $x, y, z \in G$ and $W \subset G_0$ as in the cited lemma, we have for all $w \in W$ and all $k, l = 0, \ldots, p^r - 1$,

$$V_\eta f(y^k w x^l) = \sum_{j=0}^{p^r - 1} \left\langle f(j), \tau(x^{-j} w x^j)\eta_2 \right\rangle \xi_1^{-k} \xi_2^{kj} \overline{\eta_1(j - l)}. \tag{19}$$

This can be rephrased as the result of consecutive computations of matrix coefficients with respect to τ and a (slightly modified version of) the Schrödinger representation. For this purpose, we let

$$F : W \times \mathbb{Z}_{p^r} \to \mathbb{C}, \ F(w, j) = \langle f(j), \tau(x^{-j} w x^j)\eta_2 \rangle \tag{20}$$

and note that

$$F(w, j) = V_{\eta_2}^\tau \big(f(j)\big)\big(x^{-j} w x^j\big). \tag{21}$$

Then Eq. (19) can be rewritten as

$$V_\eta f\big(y^k w x^l\big) = V_{\eta_1}^\varrho \left(F(w, \cdot)\right)(k, l) \tag{22}$$

where

$$V_{\eta_1}^{\varrho} g(k, l) = \sum_{j=0}^{p^r - 1} g(j) \xi_1^{-k} \xi_2^{kj} \overline{\eta_1(j - l)}.$$

This is just a matrix coefficient with respect to the Schrödinger representation from Example 1, modified by multiplication with ξ_1^{-k}, and by replacing the powers of the standard primitive p^rth root of unity, given by $e^{2\pi i / p^r}$, by powers of ξ_2, which is a primitive root of order p^r as well, by Lemma 27(b). Hence, $V_{\eta_1}^{\varrho} g$ coincides with the windowed Fourier transform of g with respect to η_1 up to phase factors (independent of g) and a permutation of coefficients. By Lemma 4(c), these operations do not affect the phase retrieval property, hence our choice of η_1 guarantees the phase retrieval property for $V_{\eta_1}^{\varrho}$ as well.

Now assume that $f, h \in l^2(\mathbb{Z}_p^r, \mathcal{H}_\tau)$ are such that $|V_\eta f| \equiv |V_\eta g|$ holds. We use F from (20) and define H analogously as

$$H : W \times \mathbb{Z}_{p^r} \to \mathbb{C}, \; H(w, j) = \langle h(j), \tau(x^{-j} w x^j) \eta_2 \rangle \tag{23}$$

Equation (22) gives for all $w \in W$

$$\left| V_{\eta_1}^{\varrho} (F(w, \cdot)) \right| = \left| V_{\eta_1}^{\varrho} (H(w, \cdot)) \right|.$$

Since η_1 does phase retrieval, we obtain the existence of a map

$$u : W \to \mathbb{T}, \; H(w, \cdot) = u(w) F(w, \cdot), \; \forall w \in W.$$

This implies for all $j \in \mathbb{Z}_{p^r}$ that

$$|H(\cdot, j)| \equiv |F(\cdot, j)|.$$

$W \subset G_0$ is a system of representatives modulo the central subgroup $\langle \{y\} \cup Z(G) \rangle$ of G_0, and the latter is contained in the projective kernel of τ. Hence Eq. (21) (and its analog for H) allows to rewrite the previous equation as follows, for all $j \in \mathbb{Z}_{p^r}$:

$$\forall g_0 \in G_0 : \; \left| V_{\eta_2}^{\tau} (f(j))(x^{-j} g_0 x^j) \right| = \left| V_{\eta_2}^{\tau} (h(j))(x^{-j} g_0 x^j) \right|.$$

For fixed $j \in \mathbb{Z}_{p^r}$, conjugation by x^j is an automorphism of G_0, hence we may simplify this equation to

$$\left| V_{\eta_2}^{\tau} (f(j)) \right| = \left| V_{\eta_2}^{\tau} (h(j)) \right|.$$

Now the phase retrieval property of η_2 implies the existence of a map

$$v : \mathbb{Z}_{p^r} \to \mathbb{T}, \; \forall j \in \mathbb{Z}_{p^r} : \; h(j) = v(j) f(j). \tag{24}$$

Note that this also entails, for all j, that

$$H(\cdot, j) \equiv v(j) F(\cdot, j).$$

Defining the set

$$C_f = \{j \in \mathbb{Z}_{p^r} : f(j) \neq 0\}, \tag{25}$$

(24) shows that the proof of phase retrieval boils down to showing that v is constant on C_f. This is achieved if we can show that for all $j, j' \in C_f$ there exists $w \in W$ such that

$$F(w, j) \cdot F(w, j') \neq 0,$$

since then the reasoning finishing Step 5 in the proof of Theorem 12 can be easily adapted to the finite setting: We obtain that

$$v(j) F(w, j) = H(w, j) = u(w) F(w, j), \ \ v(j') F(w, j') = u(w) F(w, j')$$

and $F(w, j)$, $F(w, j')$ can be cancelled to give $v(j) = u(w) = v(j')$.

It is only at this stage that we need to distinguish the parts (a) and (b) of the lemma. In the case of part (a), we recall that $F(\cdot, j)$ is the restriction to W of a matrix coefficient with respect to the action of the representation τ on η_1. By choice of W and η_1, and in view of Remark 17, the proportions of zero entries in $F(\cdot, j)$ and $F(\cdot, j')$ is therefore $< 1/2$, for $j, j' \in C_f$. Hence the pigeonhole principle yields the desired $w \in W$ with $F(w, j) F(w, j') \neq 0$.

In case (b) we have $\alpha_j(w) = w$ for all $j \in \mathbb{Z}_{p^r}$. Here all $F(\cdot, j)$ are restrictions of matrix coefficients to W, with respect to the action of τ on η_2. Now the phase retrieval property of $V_{\eta_2}^\tau$ entails via Lemma 4(b) that $F(\cdot, j) \cdot F(\cdot, j') \not\equiv 0$ holds for $j, j' \in C_f$.

We close the proof by observing that in case (a), the existence of a vector η_2 fulfilling the assumptions of (a) is guaranteed by Lemma 20. $\qquad \square$

The next definition extends the bookkeeping device provided by K-triples, in order to account for repeated applications of Lemma 29.

Definition 30 Let G be a p-group, and π an irreducible representation. A *full sequence of K-triples associated to* π is a sequence of triples (H_i, r_i, τ_i) with the following properties: Let $\tau_0 = \pi$, $K_0 = \ker(\pi_0)$, $H_0 = G/K_0$, as well as $K_i = \ker(\tau_i)$ for $i = 1, \ldots, k$. Then, for all $0 \leq i < k$, $(H_{i+1}, r_{i+1}, \tau_{i+1})$ is a K-triple for the representation $\overline{\tau}_i$ of H_i/K_i induced by τ_i, and H_k/K_k is abelian.

Remark 31 Repeated application of Lemma 26 shows that every irreducible representation π has an associated full sequence of K-triples.

The sizes of the quotient groups are related by the estimate

$$|H_{i+1}/K_{i+1}| \leq |H_{i+1}| = p^{-r_{i+1}} |H_i/K_i|,$$

which results from the fact that $H_{i+1} < H_i/K_i$ has index $p^{r_{i+1}}$. We further note that H_k must be nontrivial: Recall that $\bar{\tau}_{k-1} \simeq \operatorname{ind}_{H_k}^{H_{k-1}/K_{k-1}} \tau_k$ is required to be irreducible. In the case of a trivial subgroup H_k, this representation is just the left regular representation of the (nontrivial) group H_{k-1}/K_{k-1}, which is never irreducible.

Hence H_k has cardinality at least p. As a consequence we get that the length k of a full sequence of K-triples fulfills

$$1 + k \leq \log_p |G|. \tag{26}$$

Repeated applications of Lemma 29 requires control over properties of the associated matrix coefficients, as quantified in $p_0(\pi)$. Since the quantity $p_0(\pi)$ is of independent interest (see Remark 18), the following lemma is as well.

Lemma 32 *Let G denote a nonabelian p-group, and π a faithful, irreducible representation of G. Let (G_0, r, τ) denote a split K-triple associated to π. Then we have the estimate*

$$p_0(\pi) \leq p_0(\tau) + \frac{p^r - 1}{p^{2r}}.$$

Proof We use the realization of π from Lemma 27. Fix a system $W \subset G_0$ of representatives modulo $\langle\{y\} \cup Z(G)\rangle$. Given a nonzero $f \in l^2(\mathbb{Z}_{p^r}, \mathcal{H}_\tau)$, we intend to estimate the proportions of zeros in the family $(V_\eta f(y^k w x^l))_{k,l=0,\ldots,p^r-1, w \in W}$. Since this is the restriction of $V_\eta f$ to a system of representatives modulo the center of G, the proportion of zeros of $V_\eta f$ coincides with this quantity.

We pick $\eta_1 \in l^2(\mathbb{Z}_{p^r})$ and $\eta_2 \in \mathcal{H}_\tau$, and let $\eta = \eta_1 \cdot \eta_2 \in l^2(\mathbb{Z}_{p^r}, \mathcal{H}_\tau)$. We recall some notations and observations from the proof of Lemma 29, specifically

$$F : W \times \mathbb{Z}_{p^r} \to \mathbb{C}, \quad F(w, j) = \langle f(j), \tau(x^{-j} w x^j)\eta_2\rangle \tag{27}$$

and the related formulas

$$F(w, j) = V_{\eta_2}^\tau (f(j))(x^{-j} w x^j), \tag{28}$$

and

$$V_\eta f(y^k w x^l) = V_{\eta_1}^\varrho (F(w, \cdot))(k, l). \tag{29}$$

We assume that η_1, η_2 are chosen such that

$$p_0(\sigma, \eta_1) = p_0(\sigma) = \frac{p^r - 1}{p^{2r}}, \quad p_0(\tau, \eta_2) = p_0(\tau),$$

where σ denotes the Schrödinger representation from Example 1, and the second equality for $p_0(\sigma)$ follows by Eq. (15). Note that this quantity is also an upper bound for the proportion of zeros in $V_{\eta_1}^\varrho(g)$ for any nonzero vector $g \in l^2(\mathbb{Z}_{p^r})$, by the same reasoning as in the proof of Lemma 29: The matrix coefficients $V_{\eta_1}^\varrho g$ and $V_{\eta_1}^\sigma g$ differ

up to a multiplication with phase factors and a permutation, none of which affects the proportion of zeros.

Let

$$c_0 = \frac{|\{w \in W : F(w, \cdot) \equiv 0\}|}{|W|}.$$

In view of (28) and (29) we have that

$$V_\eta^\pi f(y^k w x^l) = 0$$

may occur for fixed $w \in W$ and suitable k, l either if $F(w, \cdot) \equiv 0$, in which case it holds for all $k, l \in \mathbb{Z}_{p^r}$, or if $F(w, \cdot) \not\equiv 0$ holds. In the latter case, the proportion of zeros in $V_\eta^\pi f(y^k w x^l)$ for fixed w can be bounded using $p_0(\eta_2, \sigma)$. These observations lead to the overall estimate

$$|\{(k, w, l) : V_\eta^\pi f(y^k w x^l) = 0\}|$$
$$\leq |\{w \in W : F(w, \cdot) \equiv 0\}| \cdot p^{2r} + |\{w \in W : F(w, \cdot) \not\equiv 0\}| \cdot p^{2r} p_0(\eta_2, \sigma).$$

Dividing both sides of this inequality by $|G/Z(G)| = |W| p^{2r}$ yields

$$\frac{|\{(k, w, l) : V_\eta^\pi f(y^k w x^l) = 0\}|}{|G/Z(G)|} \leq c_0 + (1 - c_0) \frac{p^r - 1}{p^{2r}} \leq c_0 + \frac{p^r - 1}{p^{2r}}.$$

It therefore remains to prove

$$c_0 \leq p_0(\tau, \eta_2) = p_0(\tau). \tag{30}$$

To see this, pick any $j_0 \in \mathbb{Z}_{p^r}$ such that $f(j_0) \neq 0$; j_0 exists since we assume f to be nonzero. We can then estimate

$$
\begin{aligned}
|\{w \in W : F(w, \cdot) \equiv 0\}| &\leq |\{w \in W : F(w, j_0) = 0\}| \\
&= |\{w \in W : V_{\eta_2}^\tau(f(j_0))(x^{-j_0} w x^{j_0}) = 0\}| \\
&\leq |W| \cdot p_0(\tau, \eta_2),
\end{aligned}
$$

which proves (30), and finishes the proof of the lemma. $\qquad\square$

A straightforward inductive application of Lemma 29 now gives the following result, which formulates a sufficient criterion for phase retrieval that can be checked using a full sequence of K-triples.

Corollary 33 *Let G denote a p-group. Assume that π is an irreducible representation of G possessing a full sequence of K-triples (H_i, r_i, τ_i), for $i = 1, \ldots, k$, that are all split. If*

$$\sum_{i=2}^k \frac{p^{r_i} - 1}{p^{2r_i}} < \frac{1}{2},$$

then π does phase retrieval.

Proof A downwards induction establishes

$$p_0(\tau_j) \le \sum_{i=j+1}^{k} \frac{p^{r_i} - 1}{p^{2r_i}} < \frac{1}{2},$$

for all $j = 1, \ldots, k$. Hence Lemma 29 (a) can be applied k times, and yields the desired statement. □

As an application of the corollary, we show that a simple size estimate on $|G|$ suffices to guarantee phase retrieval for all irreducible representations of G, if G has exponent p.

Corollary 34 *Assume that the p-group G has exponent p and fulfills $|G| \le p^{2+p/2}$. Then every irreducible representation of G does phase retrieval.*

Proof First note that, p being a prime, the exponent p property is equivalent to stating that every nontrivial group element has order p. Clearly this property is inherited by quotients and subgroups. As a consequence, every K-triple is split and of type $(G_0, 1, \tau)$, and this observation extends to all K-triples occurring in a full sequence associated to an irreducible representation π.

Let k denote the length of such a full sequence of K-triples. By Eq. (26) and the assumption on $|G|$ we have

$$k \le \log_p |G| - 1 \le 1 + p/2.$$

Using that all exponents in the sequence of K-triples equal one, the computation

$$\sum_{i=2}^{k} \frac{p-1}{p^2} = (k-1) \frac{p-1}{p^2}$$

$$\le (\log_p |G| - 2) \cdot \frac{p-1}{p^2} \le \frac{p}{2} \cdot \frac{p-1}{p^2} < \frac{1}{2}.$$

shows that Corollary 33 applies, and yields the result. □

Remark 35 It is quite possible that the requirement concerning split K-triples reflects a shortcoming of our proof method, rather than being an objective obstacle for the phase retrieval property. Understanding the precise relationship between these properties remains to be investigated in future work.

Given that it is currently unclear which irreducible representations π of a general p-group have an associated sequences of K-triples that are also split, the true scope of Corollary 33 is not yet fully understood. However, Corollary 34 exhibits one general class to which Corollary 33 applies, and it is already quite sizeable: According to [17],

the number of p-groups of order p^8 and exponent p, for primes $p > 7$, is given by the formula

$$p^4 + 2p^3 + 20p^2 + 147p + (3p + 29) \gcd(p - 1, 3) + 5 \gcd(p - 1, 4) + 1246,$$

and Corollary 34 guarantees the phase retrieval properties for arbitrary irreducible representations of these groups, as soon as $p \geq 13$. The enumeration and systematic construction of p-groups with specific properties is still an ongoing endeavour, and therefore the emergence of further general classes which can be treated with Corollary 33 seems quite plausible.

In any case, we expect that Corollary 33 can be employed for the systematic construction of p-groups and associated representations with particular interesting properties. One such property is the nilpotency class of G: Observe that the size restriction $|G| \leq p^{2+p/2}$ entails a restriction on the length of the central series, and therefore on the nilpotency class of G. However, we conjecture that for any prime number p there exist p-groups G of arbitrarily large nilpotency class and/or size, and irreducible representations of G doing phase retrieval. A proof of this conjecture via Corollary 33 would be achieved by constructing sequences of split K-triples of arbitrary length k, with sufficiently large exponents $r_1, \ldots, r_k$.

Concluding Remarks

While the statements of our main results were *existence results* for vectors doing phase retrieval, the inductive methods employed to prove these results provide access to the explicit construction of such vectors.

In the Lie group case, this can be formulated in a rather satisfactory way. If one follows the inductive construction of an arbitrary irreducible representation by repeated applications of Kirillov's lemma and induction of representations, the canonical identification of Hilbert spaces $L^2(\mathbb{R}, L^2(\mathbb{R}^k)) \cong L^2(\mathbb{R}^{k+1})$ ultimately provides a realization of π on $\mathbb{R}^m$ for a suitable $m \geq 1$. By tracing the inductive construction of the vector η doing phase retrieval in Step 3, one can employ a Gaussian for η_1 at each step. In the identification $L^2(\mathbb{R}, L^2(\mathbb{R}^k)) \cong L^2(\mathbb{R}^{k+1})$ one obtains $\eta(t, u) = \eta_1(t)\eta_2(u)$, and a simple induction yields that η is a Gaussian, as well.

This leads to the fundamental observation that every irreducible representation of an arbitrary simply connected, connected nilpotent Lie group has an explicitly computable realization on $L^2(\mathbb{R}^m)$, for suitable m, in which Gaussian vectors do phase retrieval.

In the finite group case, the setting is somewhat more involved, even assuming that all elements in a full sequences of K-triples are already known to be split: Note that the corresponding induction step in Lemma 29 requires choosing a vector η_2 that guarantees phase retrieval *and* $p_0(\tau, \eta_2) < 1/2$, and combining it with a vector η_1 doing phase retrieval for the Schrödinger representation. Here the proof of Lemma 32 estimating $p_0(\tau, \eta_2)$ relies on the same procedure to construct η from η_1 and η_2. That means that the vectors η simultaneously guaranteeing the estimates in Lemma 32 and phase retrieval can be constructed inductively as well, as soon as one can solve the following, currently open problem: Are there explicit constructions of vectors η for

the Schrödinger representation which simultaneously have the phase retrieval and full spark property?

References

1. Alaifari, R., Bartolucci, F., Wellershoff, M.: Phase retrieval of bandlimited functions for the wavelet transform. Appl. Comp. Harm. Anal. **64**, 102–117 (2023)
2. Alaifari, R., Wellershoff, M.: Stability estimates for phase retrieval from discrete Gabor measurements. J. Fourier Anal. Appl. **27**(2), 31, 6 (2021)
3. Balan, R., Casazza, P., Edidin, D.: On signal reconstruction without phase. Appl. Comput. Harmon. Anal. **20**(3), 345–356 (2006)
4. Bartusel, D., Führ, H., Oussa, V.: Phase retrieval for affine groups over prime fields (Preprint, 2021)
5. Bojarovska, I., Flinth, A.: Phase retrieval from Gabor measurements. J. Fourier Anal. Appl. **22**(3), 542–567 (2016)
6. Chen, Y., Cheng, C., Sun, Q., Wang, H.: Phase retrieval of real-valued signals in a shift-invariant space. Appl. Comput. Harmon. Anal. **49**(1), 56–73 (2020)
7. Corwin, L.J., Greenleaf, F.P.: Representations of Nilpotent Lie Groups and Their Applications. Part I, Volume 18 of Cambridge Studies in Advanced Mathematics. Basic Theory and Examples. Cambridge University Press, Cambridge (1990)
8. Fannjiang, A., Strohmer, T.: The numerics of phase retrieval. Acta Numer. **29**, 125–228 (2020)
9. Gröchenig, K.: Foundations of Time–Frequency Analysis. Applied and Numerical Harmonic Analysis. Birkhäuser Boston Inc, Boston (2001)
10. Grohs, P., Koppensteiner, S., Rathmair, M.: Phase retrieval: uniqueness and stability. SIAM Rev. **62**(2), 301–350 (2020)
11. Kaniuth, E., Taylor, K.F.: Induced Representations of Locally Compact Groups (Cambridge Tracts in Mathematics), vol. 197. Cambridge University Press, Cambridge (2013)
12. Li, L., Juste, T., Brennan, J., Cheng, C., Han, D.: Phase retrievable projective representation frames for finite abelian groups. J. Fourier Anal. Appl. **25**(1), 86–100 (2019)
13. Malikiosis, R.-D.: A note on Gabor frames in finite dimensions. Appl. Comput. Harmon. Anal. **38**(2), 318–330 (2015)
14. Malikiosis, R.D., Oussa, V.: Full spark frames in the orbit of a representation. Appl. Comput. Harmon. Anal. **49**(3), 791–814 (2020)
15. Mallat, S., Waldspurger, I.: Phase retrieval for the Cauchy wavelet transform. J. Fourier Anal. Appl. **21**(6), 1251–1309 (2015)
16. Robinson, D.J.S.: A Course in the Theory of Groups (Graduate Texts in Mathematics), vol. 80. Springer-Verlag, New York, Berlin (1982)
17. Vaughan-Lee, M.: Groups of order p^8 and exponent p. Int. J. Group Theory **4**(4), 25–42 (2015)