Phase Retrieval from $4N-4$ Measurements: A Proof for Injectivity

Friedrich Philipp

1 Technische Universität Berlin, Institut für Mathematik, MA 4-1, Straße des 17. Juni 136, D-10623 Berlin, Germany

We prove by means of elementary methods that phase retrieval of complex polynomials $p$ of degree less than $N$ is possible with $4N-4$ phaseless Fourier measurements of $p$ and $p'$.

1 Introduction

Phase retrieval is the recovery (up to a global phase factor) of signals from intensity measurements, i.e. from the absolute values of (scalar) linear measurements of the signal. This problem is motivated by applications in, e.g., X-ray crystallography [8], optical design [5], and quantum mechanics [7]. In many applications it is usually the Fourier transform of the signal from which the phase gets lost. While in practice one tries to overcome the resulting under-determination by exploiting a priori information on the phase, mathematicians and engineers are also interested in the question whether phase retrieval (without prior knowledge) is possible when the number of measurements is increased.

One of the most challenging problems in phase retrieval today is the question of how many intensity measurements are necessary and that a “generic” system consisting of $4N-4$ vectors allows for phase retrieval of every signal in $\mathbb{C}^N$. And indeed, the latter was confirmed very recently in [4].

However, in order to understand the full picture, one seeks for structured measurement systems with $4N-4$ vectors allowing for phase retrieval. The first example of this kind was given by Bodmann and Hammen in [3]. They constructed a system of $4N-4$ vectors in the $N$-dimensional linear space $\mathbb{C}^N$ of complex polynomials of degree less than $N$ and proved that it allows for phase retrieval, cf. [3, Theorem 2.3]. Another measurement ensemble consisting of $4N-4$ vectors and allowing for phase retrieval was recently provided in [6]. A recovery algorithm was presented as well.

In the present contribution, we will prove a variant of the main theorem in [3]. The measurements in [3] are in fact intensities of polynomial evaluations at points on the unit circle $\mathbb{T}$ and on another circle intersecting $\mathbb{T}$. Our main theorem is as follows.

**Theorem 1.1** Let $p$ be a polynomial with complex coefficients of degree at most $N-1$, and let

$$w_1, \ldots, w_{2N-1} \in \mathbb{T}$$

be mutually distinct points on the unit circle, respectively. Then the $4N-4$ intensity measurements

$$|p(w_j)|, \quad j = 1, \ldots, 2N-1$$

and

$$|p'(z_k)|, \quad k = 1, \ldots, 2N-3,$$

determine $p$ uniquely, up to a global phase factor.

Theorem 1.1 bears two advantages over Theorem 2.3 in [3]. First, its proof (given in Section 2) is self-contained and simpler than that of [3, Theorem 2.3]. Second, the linear measurements in Theorem 1.1 are evaluations of polynomials at points on the unit circle only and hence correspond to Fourier measurements$^1$ in $\mathbb{C}^N$. However, we remark that the second set of measurements in Theorem 1.1 consists of Fourier measurements of $p'$ and not of $p$ itself. We also mention that a recovery algorithm based on the above measurements can be found in [9].

2 Proof of Theorem 1.1

Recall that a trigonometric polynomial of degree at most $m$ has the form

$$f(t) = \sum_{n=-m}^{m} \alpha_n e^{int} = \sum_{n=1}^{m} \alpha_{-n} e^{-int} + \alpha_0 + \sum_{n=1}^{m} \alpha_n e^{int}, \quad t \in \mathbb{R},$$

where $\alpha_n \in \mathbb{C}$, $n = -m, \ldots, m$. The trigonometric polynomial $f$ is said to be real if $\alpha_{-n} = \overline{\alpha_n}$ for $n = 0, \ldots, m$. For the proof of Theorem 1.1 we only need the following two well known lemmas.

---

$^*$ Corresponding author: e-mail philipp@math.tu-berlin.de, phone +49 999 999 999, fax +49 999 999 9999

$^1$ Hereby, we mean the scalar product in $\mathbb{C}^N$ with a vector $(1, \omega^3, \omega^{2j}, \ldots, \omega^{2(N-1)})^T$, where $|\omega| = 1$.  

Copyright line will be provided by the publisher.
Lemma 2.1 A trigonometric polynomial \( f \) of degree at most \( m \) is uniquely determined by any \( 2m + 1 \) evaluations of \( f \) at mutually distinct points in \([0, 2\pi)\).

Lemma 2.2 Let \( f \) and \( g \) be two real trigonometric polynomials such that \(|f(t)| = |g(t)|\) for all \( t \in \mathbb{R} \). Then \( g = -f \) or \( g = f \).

Proof of Theorem 1.1. First of all, we observe that \( t \mapsto |p(e^{it})|^2 \) and \( t \mapsto |p'(e^{it})|^2 \) are trigonometric polynomials of degrees at most \( N-1 \) and \( N-2 \), respectively. Thus, by Lemma 2.1 the measurements in Theorem 1.1 uniquely determine the restrictions of \( |p| \) and \( |p'| \) to the unit circle. Hence, we have to prove that two polynomials \( p \in \mathcal{P}_N \) and \( q \in \mathcal{P}_N \) with

\[
|p(e^{it})| = |q(e^{it})| \quad \text{and} \quad |p'(e^{it})| = |q'(e^{it})|
\]

for all \( t \in \mathbb{R} \) (3)

must be linearly dependent. Without loss of generality we assume that both polynomials \( p \) and \( q \) do not vanish identically. Now, we define functions \( g_p, g_q : \mathbb{C} \to \mathbb{C} \) by

\[
g_p(z) := zp'(z)\overline{p(z)} \quad \text{and} \quad g_q(z) := zq'(z)\overline{q(z)}, \quad z \in \mathbb{C}.
\]

Then (3) implies \(|g_p(e^{it})| = |g_q(e^{it})|\) for all \( t \in \mathbb{R} \). But also \( \text{Im} g_p(e^{it}) = \text{Im} g_q(e^{it}) \) for all \( t \in \mathbb{R} \) since we have

\[
\frac{d}{dt} |p(e^{it})|^2 = 2 \text{Re} \left( ie^{it} p'(e^{it})\overline{p(e^{it})} \right) = -2 \text{Im} g_p(e^{it})
\]

and, similarly, \( \frac{d}{dt} |q(e^{it})|^2 = -2 \text{Im} g_q(e^{it}) \). Consequently, we obtain \( |\text{Re} g_p(e^{it})| = |\text{Re} g_q(e^{it})| \) for all \( t \in \mathbb{R} \). But \( \text{Re} g_p(e^{it}) \) and \( \text{Re} g_q(e^{it}) \) are real trigonometric polynomials in \( t \), so that Lemma 2.2 implies \( \text{Re} g_q(e^{it}) = \text{Re} g_p(e^{it}) \) for all \( t \in \mathbb{R} \) or \( \text{Re} g_q(e^{it}) = -\text{Re} g_p(e^{it}) \) for all \( t \in \mathbb{R} \). Combining this and the above, it follows that either

\[
g_p(e^{it}) = g_p(e^{it}) \quad \text{for} \quad t \in \mathbb{R} \quad \text{or} \quad g_q(e^{it}) = -g_p(e^{it}) \quad \text{for} \quad t \in \mathbb{R}.
\]

(4)

In the first case, we have \( p'(z)p(z) = q'(z)q(z) \) for all \( z \in \mathbb{T} \). Taking (3) into account, we see that multiplication with \( p(z)q(z) \) leads to

\[
p'(z)q(z) = q'(z)p(z)
\]

for all \( z \in \mathbb{T} \). This implies \( p'(z)q(z) = q'(z)p(z) \) for all \( z \in \mathbb{C} \) and thus \( \frac{p(z)}{q(z)}(z) \equiv 0 \). Consequently, \( p \) and \( q \) are linearly dependent.

Let us assume that the second case in (4) applies, i.e.

\[
e^{it} q'(e^{it})\overline{q(e^{it})} = -e^{-it} p'(e^{it})\overline{p(e^{it})}
\]

for all \( t \in \mathbb{R} \).

(5)

We will show that both \( p \) and \( q \) must be constant and therefore linearly dependent. For this, let

\[
p(z) = \sum_{k=0}^{N-1} \alpha_k z^k \quad \text{and} \quad q(z) = \sum_{k=0}^{N-1} \beta_k z^k.
\]

Then the relation (5) reads

\[
\sum_{k=0}^{N-1} \sum_{j=0}^{N-1} j\beta_j \overline{\alpha_k} e^{i(j-k)t} = - \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} j\alpha_j \overline{\beta_k} e^{i(k-j)t} \quad \text{for all} \quad t \in \mathbb{R}.
\]

If we now compare the zero-th coefficients (i.e. those for \( j = k \)) on right and left hand side of the previous equation, we obtain

\[
\sum_{j=0}^{N-1} j|\beta_j|^2 = - \sum_{j=0}^{N-1} j|\alpha_j|^2.
\]

Thus, \( \beta_1 = \ldots = \beta_{N-1} = \alpha_1 = \ldots = \alpha_{N-1} = 0 \), which implies \( p(z) = \alpha_0 \) and \( q(z) = \beta_0 \).

\[\square\]

References