DIPLOMARBEIT

PHASE ESTIMATION BASED ON LATTICE REDUCTION TECHNIQUES

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Diplomingenieurs

unter der Leitung von

Ao. Univ.-Prof. Dipl.-Ing. Dr.techn. Gerald Matz

Institut für Telekommunikation

eingereicht an der Technischen Universität Wien

Fakultät für Elektrotechnik und Informationstechnik

von

Moritz Gröger

Hauptstraße 74

2481 Achau

Achau, im September 2011 _____

—— To my grandparents ——

Abstract

This thesis gives an introduction to basic concepts of lattice theory, a theory that deals with periodic arrangements of discrete points. Furthermore, this concepts are applied to the estimation of signal phase. A powerful concept within lattice theory is lattice reduction, which is concerned with finding improved representations of a given lattice. It has been shown that solutions to the frequently occurring closest lattice point problem can be improved in terms of performance and complexity if they are preceded by lattice reduction.

In this diploma thesis we consider an estimator for uniformly sampled polynomial phase signals, the so-called angular least squares estimator. To estimate the signal parameters, we use phase unwrapping in a least squares manner. This leads to an integer least squares problem, which can be cast into a closest lattice point problem, and therefore be solved by lattice concepts. Furthermore, we formulate the angular least squares estimator for a case, where the polynomial phase signal is nonuniformly sampled. The fact that in this case we do not experience aliasing comes at the cost of poor performance in low-SNR scenarios. Subsequently, the angular least squares estimator is used to estimate phase parameters of a signal that is modeled by a Fourier basis. Numerically results show that the angular least squares estimator works well in every mentioned scenario provided the SNR is above a certain threshold.

Kurzfassung

Diese Diplomarbeit gibt eine Einführung in grundlegende Konzepte der Gittertheorie, eine Theorie, die sich mit periodischen Anordnungen diskreter Punkte beschäftigt. Weiters werden diese Konzepte für ein Phasenschätzproblem herangezogen. Ein leistungsfähiges Konzept innerhalb der Gittertheorie ist die so genannte Gitterreduktion. Ihr Ziel ist es, eine verbesserte Darstellung eines gegebenen Gitters zu finden. Es ist bekannt, dass die Suche nach dem nächsten Gitterpunkt betreffend Ergebnis und Komplexität verbessert werden kann, indem man zuvor eine Gitterreduktion anwendet.

In dieser Diplomarbeit betrachten wir einen Schätzer für Signale mit polynomialer Phase basierend auf „phase unwrapping“. Um eine kontinuierliche Phase zu erhalten wird hierbei der gemessene Hauptwert der Phase entsprechend verschoben aneinander gefügt. Dieser Ansatz führt zu einem ganzzahligen Problem kleinster Quadrate, welches mit Hilfe einer Suche nach dem nächsten Gitterpunkt gelöst werden kann. Neben gleichförmig abgetasteten Signalen betrachten wir auch zufällig abgetastete. In letztgenanntem Fall tritt bei niedrigem Signal-Rausch-Verhältnis ein größerer Schätzfehler auf. Schließlich wird der Phasenschätzer verwendet, um eine Phase zu schätzen, die durch eine Fourier-Basis modelliert wird.

Numerische Resultate zeigen, dass der Schätzer für alle oben genannten Szenarien gut funktioniert, solange das Signal-Rausch-Verhältnis einen bestimmten Schwellwert überschreitet.

Contents

1

Introduction

A lattice is a periodic arrangement of discrete points. First work on lattice theory has been done by Minkowski and Voronoi more than a century ago. Lattices found widespread use in mathematics, for example for the sphere packing problem, the problem of packing as many non-intersecting, n-dimensional hyperspheres into the smallest possible volume. Beside the use in pure mathematics, the theory of lattices has been applied to several other fields, such as cryptography and cryptanalysis, the geometry of numbers, diophantine approximations, crystalography and coding theory. More recently lattices have found applications in communication systems with multiple antennas.

In lattice theory a fundamental problem is the *closest lattice point problem* (also called the nearest lattice point problem). Given a lattice, it is the problem of finding the lattice point with minimal Euclidian distance to an arbitrarily given input point. To give an example in communication theory: assuming a lattice is used as a code for a Gaussian channel, maximum-likelihood decoding (optimum decoding) equals the closest lattice point search at the demodulator.

Efficient search algorithms exist to solve the closest point problem for many classical lattices [1]. When assuming a general lattice, that means there is no exploitable structure of the lattice, finding the closest point is exhaustive. However, there are algorithms

to solve this problem. A good overview about the closest lattice point problem is given in Agrell et al. [2].

There are fast algorithms approximating the closest lattice point. Babai [3] presented two such algorithms that are polynomial in time. One is based on a rounding-off procedure and the other one is known as *Babai's nearest plane algorithm*. The performance or complexity of algorithms obtaining or approximating the closest point strongly depends on the *basis matrix* of a lattice. A basis matrix is used to describe a lattice and is not unique. In order to achieve good performance regarding the closest point problem, the basis matrix should consist of fairly orthogonal and short basis vectors. The method for obtaining such a reduced basis is called *lattice reduction*.

The lattice reduction aided approach is the following:

1. Find an improved basis by using lattice reduction. The original and the reduced basis are related via a unimodular matrix.

2. Solve the closest point problem in the lattice described by the reduced basis matrix.

3. Transform the result back to the original domain using the unimodular matrix.

In this thesis the aforementioned approach is applied to an application in signal processing, the estimation of a polynomial phase signal and of a Fourier-based phase signal. Following the work of McKilliam [4], we extend the estimator to the nonuniform sampling case and furthermore to Fourier-based phase signals.

The text is structured as follows:

- **Chapter 1**: This introduction.
- **Chapter 2** introduces some basics of lattices theory. Furthermore lattice reduction and the closest point search are treated.
- **Chapter 3** shows a technique for estimating uniformly sampled polynomial phase signals. The parameters are estimated by performing phase unwrapping in a least squares manner. The obtained integer least squares problem is formulated as a closest lattice point problem, which we solve using Babai's nearest plane algorithm. Some numerical simulation results illustrating the performance of this estimator will be shown.
- **Chapter 4** extends the polynomial phase estimation approach from Chapter 3 to the more general case of nonuniform sampling. The chapter will be concluded by simulation results.
- **Chapter 5** tackles the phase estimation problem using a Fourier basis instead of a polynomial basis. As in earlier chapters, the corresponding simulation results are given.
- **Chapter 6** gives a summary and discusses open problems for future research.

2

Lattice Theory

Lattices are periodic arrangements of discrete points. In mathematics they provide solutions to several problems such as the sphere packing problem or the kissing number problem. Beside their mathematical use, lattices have found numerous applications in several fields such as coding theory, cryptography/cryptanalysis or diophantine approximations. More recently they found applications in wireless communications featuring multiple antennas, so called MIMO (multiple input multiple output) communications. In this thesis, lattices are used for the signal processing problem of phase estimation.

We first provide some basics of lattice theory. We give some examples of lattices and explain how they are described in terms of a basis (or generator) matrix. We will see that this description is non-unique, a property we capitalize on when applying lattice reduction. In Section 2.2, the principle of lattice reduction is given and we get to know a commonly used algorithm, the Lenstra-Lenstra-Lovász (LLL) reduction algorithm.

The final section gives an overview about the closest lattice point problem and provides *Babai's nearest plane algorithm*, a fast algorithm to compute an approximation for the closest lattice point in a lattice.

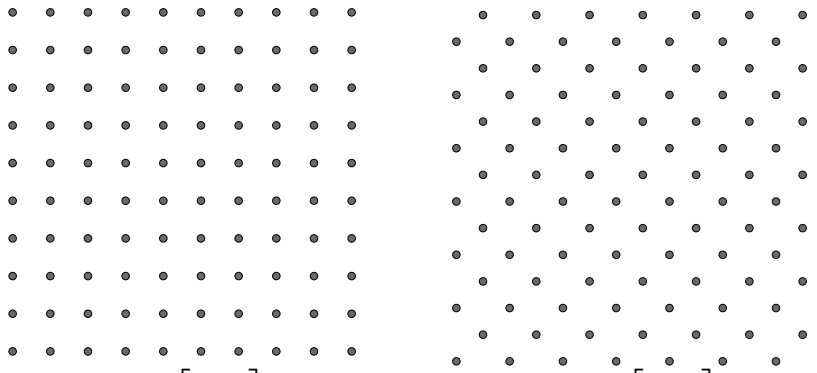

Figure 2.1: *Two-dimensional example lattices: (a) square and (b) rhombic.*

2.1 Lattice Description

A real-valued lattice $\mathcal{L}$ is a set of points in $\mathbb{R}^n$. In order to describe a lattice we use $m \leq n$ linearly independent basis (or generator) vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$, with $\mathbf{b}_\ell \in \mathbb{R}^n$ such that

$$\mathcal{L} \triangleq \left\{ \mathbf{x} \middle| \mathbf{x} = \sum_{\ell=1}^{m} z_\ell \mathbf{b}_\ell, z_\ell \in \mathbb{Z} \right\},$$

where m denotes the *rank* of the lattice and $\mathbb{Z}$ is the set of integers. Every single lattice point can be expressed by an integer linear combination of the basis vectors. Equivalently, we can characterize a lattice in a matrix notation by rearranging the basis vectors into a $n \times m$ matrix $\mathbf{B} = (\mathbf{b}_1 \ldots \mathbf{b}_m)$ called the generator matrix, as

$$\mathcal{L} \triangleq \left\{ \mathbf{x} \middle| \mathbf{x} = \mathbf{B}\mathbf{z}, \mathbf{z} \in \mathbb{Z}^m \right\}.$$

We will abbreviate the definition of a lattice above as $\mathcal{L} = \mathbf{B}\mathbb{Z}^m$. By assuming the basis vectors to be linear independent, $\mathbf{B}$ has full column rank, i.e., $\text{rank}(\mathbf{B}) = m$. Examples for two-dimensional lattices can be seen in Figure 2.1. The square lattice, shown in Figure 2.1(a), is obtained by choosing the generator matrix $\mathbf{B}$ as the two-dimensional identity matrix $\mathbf{I}_2$. The lattice then is denoted by $\mathcal{L} = \mathbb{Z}^2$.

The generator matrix need not necessarily be square. If the generator matrix $\mathbf{B}$ is

a tall matrix (has more rows than columns), i.e., $m < n$, then the lattice points lie in a m-dimensional subspace of $\mathbb{R}^n$. In the case of a square generator matrix, i.e., $m = n$, the lattice points span $\mathbb{R}^n$ and we say the lattice is of full rank.

A generator matrix for a lattice is not unique. The generators $\mathbf{B}$ and $\mathbf{BT}$ span the same lattice $\mathcal{L}$ if the transformation matrix $\mathbf{T}$ is an $m \times m$ matrix with integer elements such that $|\det(\mathbf{T}) = 1|$. Matrices with these properties are called *unimodular*. The fact that two generator matrices $\mathbf{B}$ and $\mathbf{BT}$ lead to the same lattice $\mathcal{L}$ can be written as $\mathbf{B}\mathbb{Z}^m = \mathbf{BT}\mathbb{Z}^m$ and thus $\mathbb{Z}^m = \mathbf{T}\mathbb{Z}^m$. The last equality can hold only if $\mathbf{T}$ is invertible and $\mathbf{T}$ and $\mathbf{T}^{-1}$ have integer elements. The restriction on the determinant of the integer-valued matrix $\mathbf{T}$, i.e., $|\det(\mathbf{T}) = 1|$, guarantees the existence of the inverse and the inverse matrix to be integer.

The *fundamental parallelotope* of a lattice basis is the parallelotope constructed from the basis vectors of the lattice as

$$\mathcal{P}(\mathbf{B}) \triangleq \left\{ \mathbf{x} \middle| \mathbf{x} = \sum_{\ell=1}^{m} \theta_\ell \mathbf{b}_\ell, 0 \leq \theta_\ell < 1 \right\}.$$

As the generator matrix is not unique, neither is the fundamental parallelotope. In Figure 2.2 we see two examples of fundamental parallelotopes for a lattice which can be described by the generator matrix

$$\mathbf{B} = \begin{bmatrix} 1 & 0.1 \\ 0.1 & 1 \end{bmatrix}. \tag{2.1}$$

Furthermore we can see in this figure that the union of $\mathcal{P}(\mathbf{B})$ shifted to all lattice points covers the complete space $\mathbb{R}^n$ and any two shifted parallelotopes don't intersect, i.e.,

$$\bigcup_{\mathbf{x} \in \mathcal{L}} \mathcal{P}(\mathbf{B}) + \mathbf{x} = \mathbb{R}^n \qquad \text{and} \tag{2.2}$$

$$(\mathcal{P}(\mathbf{B}) + \mathbf{x}) \cap (\mathcal{P}(\mathbf{B}) + \mathbf{y}) = \emptyset \quad \forall \mathbf{x}, \mathbf{y} \in \mathcal{L}, \quad \mathbf{x} \neq \mathbf{y}. \tag{2.3}$$

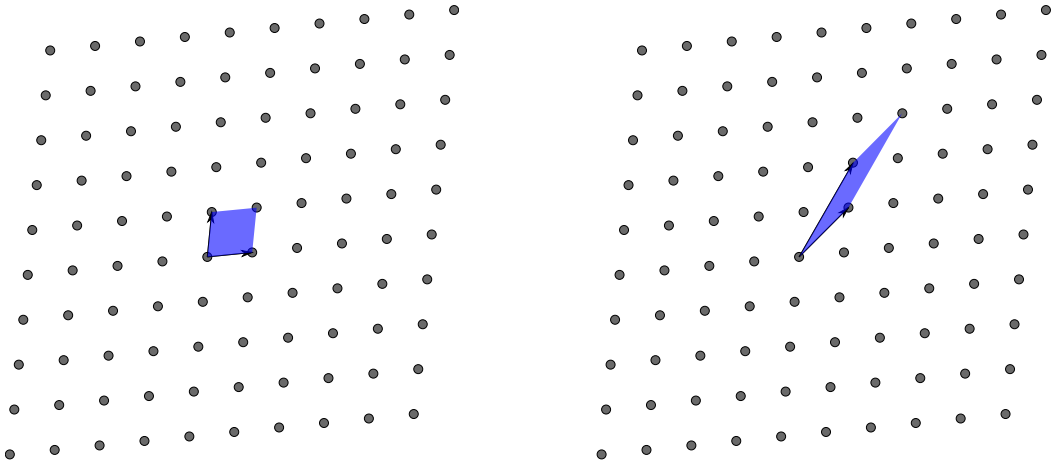

Figure 2.2: *Two examples of fundamental parallelotopes for a lattice given by the generator matrix in* (2.1)*. In (a) the fundamental parallelotope corresponds to the basis vectors* $[1, 0.1]^T$ *and* $[0.1, 1]^T$*. In (b) the underlying basis vectors are* $[1.1, 1.1]^T$ *and* $[1.2, 2.1]^T$*.*

Fulfilling (2.2) and (2.3), $\mathcal{P}(\mathbf{B})$ is a so-called fundamental region.

The *Voronoi region* $\mathcal{V}(\mathcal{L})$ is a subset of $\mathbb{R}^n$ containing all the points which are closer, according to a given norm, to the lattice point at the origin than to any other lattice point, i.e.,

$$\mathcal{V}(\mathcal{L}) \triangleq \left\{ \mathbf{y} \middle| \|\mathbf{y}\| \leq \|\mathbf{y} - \mathbf{z}\| \quad \text{for all} \quad \mathbf{z} \in \mathcal{L} \right\}. \tag{2.4}$$

The norm we will use throughout this thesis is the 2-norm, which means that the Voronoi region is the set of points with Euclidian distance smaller to the origin than to any other point. In Figure 2.3 we see an examples of a Voronoi region. By shifting $\mathcal{V}(\mathcal{L})$ to another lattice point $\mathbf{x} \in \mathcal{L}$, $\mathcal{V}(\mathcal{L}) + \mathbf{x}$ describes the set of points closest to $\mathbf{x}$. From (2.4) we see that the faces of the Voronoi region are closed. In order to make the Voronoi region satisfy (2.2) and (2.3) we have to define half of the faces to be closed and the corresponding opposing faces to be open. With this modification the Voronoi region is a fundamental region which tessellates the space $\mathbb{R}^n$. The Voronoi region is independent of the choice of the lattice basis.

Given a lattice $\mathcal{L}$ with lattice basis $\mathbf{B}$, the so-called *lattice determinant* is defined

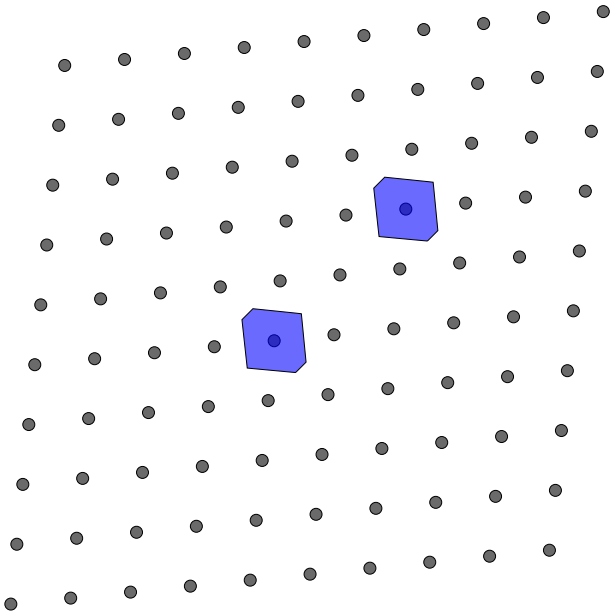

Figure 2.3: *The Voronoi region* $\mathcal{V}(\mathcal{L})$ *and a shifted version* $\mathcal{V}(\mathcal{L})+\mathbf{x}$ *for a lattice with generator matrix from* (2.1).

as the square-root of the determinant of the Gram matrix $\mathbf{B}^T\mathbf{B}$,

$$\det(\mathcal{L}) = \sqrt{\det(\mathbf{B}^T\mathbf{B})}. \tag{2.5}$$

Assuming the lattice is of full rank, i.e., $m = n$, the lattice determinant simplifies to $\det(\mathcal{L}) = |\det(\mathbf{B})|$ and is equal to the volume of the fundamental parallelotope, which is the same for any basis for a given lattice. Generally, every fundamental region has a volume equal to the lattice determinant, since every volume correspond to exactly one lattice point and together they cover the whole space spanned by the lattice. The Voronoi region $\mathcal{V}(\mathcal{L})$ is such a fundamental region, therefore its volume is equal to the lattice determinant. If a lattice is not of full rank, i.e., $m < n$, the lattice determinant equals the volume of the intersection of the m-dimensional subspace spanned by the lattice with the fundamental region.

A measure for the orthogonality of a lattice is the so-called *orthogonality defect*, defined as

$$\delta(\mathbf{B}) = \frac{\prod_{\ell=1}^{m} \|\mathbf{b}_\ell\|}{\det(\mathcal{L})}. \tag{2.6}$$

In the numerator we have the product of the basis vector lengths. The Hadamard inequality $|\det(\mathbf{B})| \leq \prod_{\ell=1}^{m} \|\mathbf{b}_\ell\|$ states that an m-dimensional volume spanned by the m vectors is upper bounded by the product of the corresponding vector lengths, with equality if and only if the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$ are mutually orthogonal. By applying this inequality to (2.6) we see that the orthogonality defect is lower bounded by 1, i.e., $\delta(\mathbf{B}) \geq 1$, with equality if and only if the lattice basis vectors are orthogonal.

Another way to illustrate the orthogonality of the lattice basis is achieved by the *QR-decomposition*. As mentioned earlier, we have an $n \times m$ basis matrix $\mathbf{B}$ with full column rank, i.e., $\text{rank}(\mathbf{B}) = m$. The QR-decomposition

$$\mathbf{B} = \mathbf{QR} = \begin{bmatrix} \mathbf{q}_1 & \ldots & \mathbf{q}_m \end{bmatrix} \begin{bmatrix} r_{11} & r_{12} & r_{13} & \ldots & r_{1m} \\ & r_{22} & r_{23} & \ldots & r_{2m} \\ & & r_{33} & \ldots & r_{3m} \\ & & & \ddots & \vdots \\ & & & & r_{mm} \end{bmatrix} \tag{2.7}$$

expresses the lattice basis in terms of an $n \times m$ orthonormal matrix $\mathbf{Q}$ and an $m \times m$ upper triangular matrix $\mathbf{R}$. The columns $\mathbf{q}_1, \ldots, \mathbf{q}_m$ of $\mathbf{Q}$ are orthogonal and of unit length ($\mathbf{Q}^T\mathbf{Q} = \mathbf{I}_m$). Since the lattice basis $\mathbf{B}$ is of full rank m and we require that the diagonal elements of $\mathbf{R}$ are positive, the QR-decomposition is unique. From (2.7) we see that each basis vector $\mathbf{b}_\ell$ can be described by the sum $\sum_{k=1}^{\ell} r_{k,\ell}\mathbf{q}_k$. The vector $\mathbf{q}_\ell$ of unit length is pointing into the direction of the basis vector $\mathbf{b}_\ell$ perpendicular to the space spanned by $\mathbf{q}_1, \ldots, \mathbf{q}_{\ell-1}$. The diagonal element $r_{\ell,\ell} = \mathbf{q}_\ell^T\mathbf{b}_\ell$ characterizes the length of $\mathbf{b}_\ell$ into the direction of this orthonormal vector $\mathbf{q}_\ell$. The components of $\mathbf{b}_\ell$ projected onto each orthonormal vector $\mathbf{q}_k$ with $1 \leq k < \ell$ are described by the regarding element $r_{k,\ell} = \mathbf{q}_k^T\mathbf{b}_\ell$. If these off-diagonal elements of $\mathbf{R}$ are close to zero the lattice with the basis $\mathbf{B}$ can be considered as roughly orthogonal. In case the upper triangular matrix $\mathbf{R}$ is a diagonal matrix, every basis vector $\mathbf{b}_l$ is a multiple of the orthogonal vector $\mathbf{q}_\ell$

and therefore the basis matrix is orthogonal.

2.2 Lattice Reduction

Any lattice can be described by many different lattice bases. Given a lattice $\mathcal{L}$, the aim of lattice reduction is to find a lattice basis with "good" properties which usually means it consists of short and roughly orthogonal vectors. What "good" exactly means depends on the lattice reduction method, which is not unique. There are several lattice reduction methods, such as Minkowski reduction [5], Hermite-Korkin-Zolotarev reduction [6] [7], Gauss reduction [8], Lenstra-Lenstra-Lovász reduction [9], and Seysen reduction [10], each with a more or less stringent reduction criterion. Minkowski reduction and Hermite-Korkin-Zolotarev reduction have strict conditions but their computational complexity is very high. Currently there is no polynomial-time algorithm known for finding such a reduced basis. A reduction method where there exists a polynomial-time algorithm is the Lenstra-Lenstra-Lovász (LLL) algorithm which will be described later in this chapter.

As mentioned in Section 2.1, the basis $\mathbf{BT}$ and $\mathbf{B}$ span the same lattice as long the transformation matrix $\mathbf{T}$ is an unimodular matrix. The goal of lattice reduction algorithms is to find a matrix $\mathbf{T}$ transforming the old basis $\mathbf{B}$ into a new basis $\tilde{\mathbf{B}}=\mathbf{BT}$ which fulfills the underlying reduction criterion. In order to achieve such a reduced basis $\tilde{\mathbf{B}}$ the algorithms use several elementary column operations on the basis matrix $\mathbf{B}$ until the requirements of the lattice reduction method are fulfilled [11]. These elementary column operations are:

- *Reflection:* A specific basis matrix column is multiplied by -1. The corresponding unimodular matrix is denoted as $\mathbf{T}_R^{(\ell)}=\mathbf{I}-2\mathbf{e}_\ell\mathbf{e}_\ell^T$. Transforming the basis matrix $\mathbf{B}$ according to $\tilde{\mathbf{B}}=\mathbf{B}\mathbf{T}_R^{(\ell)}$ yields a new basis with a reflected column vector $\tilde{\mathbf{b}}_\ell=-\mathbf{b}_\ell$ whereas the remaining column vectors are unchanged.

- *Swap:* Two columns are interchanged. Written in terms of basis vectors k and ℓ this reads as $\tilde{\mathbf{b}}_\ell = \mathbf{b}_k$ and $\tilde{\mathbf{b}}_k = \mathbf{b}_\ell$. The unimodular transformation matrix for a swap of columns k and ℓ is $\mathbf{T}_S^{(k,\ell)} = \mathbf{I} - \mathbf{e}_k\mathbf{e}_k^T - \mathbf{e}_\ell\mathbf{e}_\ell^T + \mathbf{e}_k\mathbf{e}_\ell^T + \mathbf{e}_\ell\mathbf{e}_k^T$.

- *Translation:* The μth multiple of the kth column is added to the ℓth column of the basis matrix. The resulting vector builds the ℓth column of the new lattice basis, i.e., $\tilde{\mathbf{b}}_\ell = \mathbf{b}_\ell + \mu\mathbf{b}_k$, where $\mu \in \mathbb{Z}$. The unimodular matrix here is given by $[\mathbf{T}_T^{(k,\ell)}]^\mu = \mathbf{I} + \mu\mathbf{e}_k\mathbf{e}_\ell^T$.

A sequence of the above mentioned elementary column operations forms the unimodular matrix $\mathbf{T}$, which transforms the given basis $\mathbf{B}$ into the reduced basis $\tilde{\mathbf{B}}$.

LLL Reduction

In 1982, Lenstra, Lenstra, and Lovász [9] presented their famous LLL reduction algorithm, which produces from any given lattice basis the so-called LLL-reduced basis in polynomial time. A lattice basis $\tilde{\mathbf{B}}$ is called LLL-reduced with parameter $\delta \in (\frac{1}{4}, 1]$ if the two following conditions are fulfilled:

$$|\tilde{r}_{k,\ell}| \leq \tfrac{1}{2}|\tilde{r}_{k,k}|, \quad \text{for } 1 \leq k < \ell \leq m, \tag{2.8a}$$

$$\delta\,|\tilde{r}_{\ell-1,\ell-1}|^2 \leq |\tilde{r}_{\ell,\ell}|^2 + |\tilde{r}_{\ell-1,\ell}|^2, \quad \text{for } \ell = 2, \ldots, m. \tag{2.8b}$$

Here, $\tilde{r}_{k,\ell}$ denotes the elements of the upper triangular matrix $\tilde{\mathbf{R}}$, where $\tilde{\mathbf{B}} = \tilde{\mathbf{Q}}\tilde{\mathbf{R}}$.

The first inequality is the condition for *size-reduction*. It states that the component of any vector $\tilde{\mathbf{b}}_\ell$ with $\ell > k$ into the direction of $\tilde{\mathbf{q}}_k$ is not larger than half the length of the component of $\tilde{\mathbf{b}}_k$ into the same direction. To see the involved entries of $\tilde{\mathbf{R}}$ for a fixed k, for example $k = 2$, we write

$$\begin{bmatrix} \tilde{\mathbf{b}}_1 & \tilde{\mathbf{b}}_2 & \tilde{\mathbf{b}}_3 & \dots & \tilde{\mathbf{b}}_m \end{bmatrix} = \begin{bmatrix} \tilde{\mathbf{q}}_1 & \boxed{\tilde{\mathbf{q}}_2} & \dots & \tilde{\mathbf{q}}_m \end{bmatrix} \begin{bmatrix} \tilde{r}_{11} & \tilde{r}_{12} & \tilde{r}_{13} & \dots & \tilde{r}_{1m} \\ & \tilde{r}_{22} & \tilde{r}_{23} & \dots & \tilde{r}_{2m} \\ & & \tilde{r}_{33} & \dots & \tilde{r}_{3m} \\ & & & \ddots & \vdots \\ & & & & \tilde{r}_{mm} \end{bmatrix}.$$

The basis vectors $\tilde{\mathbf{b}}_2, \dots, \tilde{\mathbf{b}}_m$ and their regarding components into the direction of $\tilde{\mathbf{q}}_2$ are highlighted here. The off-diagonal entries (shown in blue) have to be smaller than the half of the corresponding diagonal element (shown in red).

If this condition is fulfilled for every row, i.e., for $1 \leq k \leq m$, the lattice basis $\tilde{\mathbf{B}}$ is size-reduced. Whenever an off-diagonal element $\tilde{r}_{k,\ell}$ is not fulfilling the size-reduction condition (2.8a), the translation $\tilde{\mathbf{b}}_\ell \longleftarrow \tilde{\mathbf{b}}_\ell - \mu\tilde{\mathbf{b}}_k$ with $\mu = \lceil \tilde{r}_{k,\ell}/\tilde{r}_{k,k} \rfloor$ is performed, where $\lceil \cdot \rfloor$ denotes rounding to the nearest integer.

The second inequality (2.8b) is the so-called Lovász condition. The inequality relates the squared component of $\tilde{\mathbf{b}}_{\ell-1}$ orthogonal to the space spanned by the basis vectors $\tilde{\mathbf{b}}_1, \dots, \tilde{\mathbf{b}}_{\ell-2}$, i.e., $|\tilde{r}_{\ell-1,\ell-1}|^2$, to the sum of the squared components of $\tilde{\mathbf{b}}_\ell$ orthogonal to the same space, $|\tilde{r}_{\ell,\ell}|^2 + |\tilde{r}_{\ell-1,\ell}|^2$. For an example let us assume $\ell = 3$. According to

$$\begin{bmatrix} \tilde{\mathbf{b}}_1 & \tilde{\mathbf{b}}_2 & \tilde{\mathbf{b}}_3 & \dots & \tilde{\mathbf{b}}_m \end{bmatrix} = \begin{bmatrix} \tilde{\mathbf{q}}_1 & \tilde{\mathbf{q}}_2 & \dots & \tilde{\mathbf{q}}_m \end{bmatrix} \begin{bmatrix} \tilde{r}_{11} & \tilde{r}_{12} & \tilde{r}_{13} & \dots & \tilde{r}_{1m} \\ & \tilde{r}_{22} & \tilde{r}_{23} & \dots & \tilde{r}_{2m} \\ & & \tilde{r}_{33} & \dots & \tilde{r}_{3m} \\ & & & \ddots & \vdots \\ & & & & \tilde{r}_{mm} \end{bmatrix},$$

the Lovász condition compares the components of $\tilde{\mathbf{b}}_3$ orthogonal to $\text{span}\{\tilde{\mathbf{b}}_1\}$ (shown in blue) and the component of $\tilde{\mathbf{b}}_2$ orthogonal to $\text{span}\{\tilde{\mathbf{b}}_1\}$ (shown in red). The parameter δ provides a trade-off between the quality of the reduced basis and the computational

complexity of the algorithm to achieve this reduced basis. A larger δ increases the orthogonality of the obtained lattice basis. In [9] the parameter was originally chosen as $\delta = 3/4$. In case the Lovász condition is not fulfilled, the two involved vectors are swapped, i.e., $\tilde{\mathbf{b}}_{\ell-1} \longleftrightarrow \tilde{\mathbf{b}}_{\ell}$ which leads to a more orthogonal lattice basis.

After the swapping of basis vectors, the lattice basis may not be *size-reduced* any more, so again size-reduction is applied. These two processes, namely finding a shorter basis via size reduction for a given orthogonalization of the basis and finding a better orthogonalization via swapping of basis vectors for a given basis, are iteratively used by the LLL algorithm until both conditions, (2.8a) and (2.8b) are fulfilled.

Algorithm 1 shows the LLL algorithm provided by Wübben [12]. Given the QR-decomposition of $\mathbf{B}$ we get the QR-decomposition of the LLL-reduced basis $\tilde{\mathbf{B}}$ and the corresponding transformation matrix $\mathbf{T}$ as an output. In this algorithm the column swaps and translations are performed directly on the matrices $\tilde{\mathbf{R}}$ and $\mathbf{T}$. Therefore a QR-decomposition is not necessary after each basis update.

2.3 Closest Lattice Point Search

Given a point $\mathbf{y} \in \mathbb{R}^n$ and a lattice $\mathcal{L}$ lying in the same space, the goal of the closest lattice point search is to find the lattice point $\mathbf{x} \in \mathcal{L}$ that is closer to the point $\mathbf{y}$ than any other lattice point, i.e.

$$\|\mathbf{y} - \mathbf{x}\| \leq \|\mathbf{y} - \mathbf{z}\|, \quad \text{for all} \quad \mathbf{z} \in \mathcal{L}, \tag{2.9}$$

where $\|\cdot\|$ denotes the Euclidian norm. We will use $\mathrm{CPt}\{\mathbf{y}, \mathcal{L}\}$ to denote closest point search. With definition of the Voronoi region in (2.4) we can express the closest point search alternatively as

$$\mathbf{x} = \mathrm{CPt}\{\mathbf{y}, \mathcal{L}\} \quad \Longleftrightarrow \quad \mathbf{y} \in \mathcal{V}(\mathcal{L}) + \mathbf{x}, \tag{2.10}$$

Algorithm 1 LLL algorithm

Input: $\mathbf{Q}, \mathbf{R}$
Output: $\tilde{\mathbf{Q}}, \tilde{\mathbf{R}}, \mathbf{T}$

Initialization: $\tilde{\mathbf{Q}} := \mathbf{Q}, \tilde{\mathbf{R}} := \mathbf{R}, \mathbf{T} := \mathbf{I}_m$
$\ell = 2$
while $\ell \leq m$ **do**
  for $k = \ell - 1$ to 1 **do**
    $\mu = \lceil \tilde{\mathbf{R}}(k, \ell) / \tilde{\mathbf{R}}(k, k) \rfloor$
    if $\mu \neq 0$ **then**
      Translation:
      $\tilde{\mathbf{R}}(1 : k, \ell) := \tilde{\mathbf{R}}(1 : k, \ell) - \mu \tilde{\mathbf{R}}(1 : k, k)$
      $\mathbf{T}(:, \ell) := \mathbf{T}(:, \ell) - \mu \mathbf{T}(:, k)$
    end if
  end for
  if $\delta \tilde{\mathbf{R}}(\ell - 1, \ell - 1)^2 > \tilde{\mathbf{R}}(\ell, \ell)^2 + \tilde{\mathbf{R}}(\ell - 1, \ell)^2$ **then**
    Columnswap:
    $\tilde{\mathbf{R}}(:, \ell - 1) \longleftrightarrow \tilde{\mathbf{R}}(:, \ell)$
    $\mathbf{T}(:, \ell - 1) \longleftrightarrow \mathbf{T}(:, \ell)$
    Calculate Givens rotation matrix θ such that element $\tilde{\mathbf{R}}(\ell, \ell - 1)$ becomes zero:
    $\mathbf{\Theta} = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}$ with $\alpha = \frac{\tilde{\mathbf{R}}(\ell-1,\ell-1)}{||\tilde{\mathbf{R}}(\ell-1:\ell,\ell-1)||}$, $\beta = \frac{\tilde{\mathbf{R}}(\ell,\ell-1)}{||\tilde{\mathbf{R}}(\ell-1:\ell,\ell-1)||}$
    $\tilde{\mathbf{R}}(\ell - 1 : \ell, \ell - 1 : m) := \mathbf{\Theta} \tilde{\mathbf{R}}(\ell - 1 : \ell, \ell - 1 : m)$
    $\tilde{\mathbf{Q}}(:, \ell - 1 : \ell) := \tilde{\mathbf{Q}}(:, \ell - 1 : \ell) \mathbf{\Theta}^T$
    $\ell := \max\{\ell - 1, 2\}$
  else
    $\ell := \ell + 1$
  end if
end while

that is a search for the shifted Voronoi region the given point $\mathbf{y}$ is part of.

Solutions to the closest lattice point search have numerous applications. In the context of MIMO (multiple input-multiple output) communications, where we consider several transmit and receive antennas, the closest lattice point search provides a solution for maximum-likelihood (ML) detection. Another example is vector perturbation [13] where the closest point search is used for precoding in a wireless MIMO scenario. A field where the closest lattice point search is often required is cryptography/cryptanalysis. In signal processing, the closest lattice point search is potentially useful for integer programming problems, where within an optimization problem some or all variables are restricted to be integer. An example for solving an integer least squares problem in the context of global positioning system (GPS) is given in [14].

The closest lattice point search is known to be *NP-hard* for randomized reductions [15]. However, there are algorithms that compute the closest lattice point in reasonable time. A good survey on algorithms for the closest point search in lattices without a regular structure is given in [2]. The basic approach is to define a certain region in which the optimal lattice point must lie and then find all the lattice points inside this region. Many closest lattice point search algorithms are based on the Kannan or the Pohst strategy. A variant of the latter is known as the sphere decoder in the communication field [16].

There are fast approximate algorithms computing the closest point. Babai [3] presented two procedures computing an approximate closest lattice point. One is called the rounding off-procedure and the other one is known as Babai's nearest plane algorithm. Both are not guaranteed to find the closest point.

The performance of algorithms obtaining or approximating the closest point strongly depends on the *basis matrix* of a lattice. The best results to the closest point problem are obtained by searching in a lattice using short and orthogonal basis vectors. Therefore, it is advantageous to apply lattice reduction first. The approach is the following:

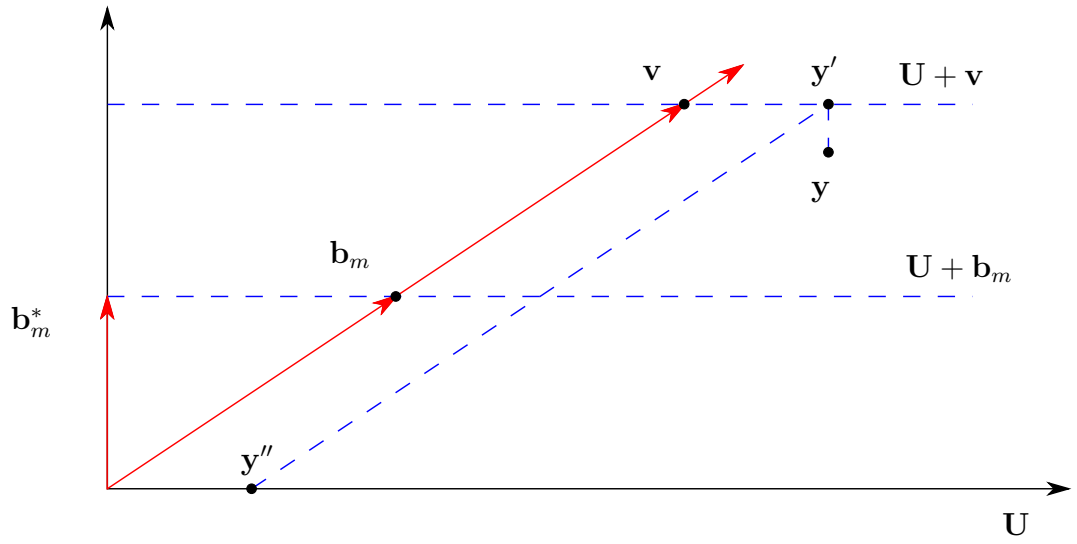

Figure 2.4: *Illustration of Babai's nearest plane method. The x-axis represents the m-1-dimensional subspace* **U** *and the y-axis is perpendicular to* **U**.

1. Find an improved basis by using lattice reduction. The original and the reduced basis are related via an unimodular matrix.

2. Solve the closest point problem in the lattice described by the reduced basis matrix.

3. Transform the result back to the original domain using the unimodular matrix.

A common strategy is to reduce the lattice according to the LLL-reduction method, because this method is only polynomial in time.

2.3.1 Babai's Nearest Plane Algorithm

Let $\mathcal{L}$ be a lattice of full rank and given by the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$. The nearest plane algorithm finds a point $\mathbf{w} \in \mathcal{L}$ that is close to a given point $\mathbf{y} \in \mathbb{R}^n$. The point obtained is not guaranteed to be the closest point to $\mathbf{y}$, but if the basis of the lattice $\mathcal{L}$ is LLL-reduced, $\|\mathbf{y} - \mathbf{w}\|$ is within an exponential factor of the minimum value. In the following the principle of the nearest plane algorithm is described. Figure 2.4 illustrates Babai's nearest plane method [17].

Let $\mathbf{U}$ be the linear subspace spanned by $\{\mathbf{b}_1, \ldots, \mathbf{b}_{m-1}\}$, i.e.,

$$\mathbf{U} = \sum_{\ell=1}^{m-1} r_\ell \mathbf{b}_\ell, r_\ell \in \mathbb{R}, \tag{2.11}$$

and the corresponding sublattice $\mathcal{L}' = \mathcal{L} \cap \mathbf{U}$ given by

$$\mathcal{L}' = \sum_{\ell=1}^{m-1} z_\ell \mathbf{b}_\ell, z_\ell \in \mathbb{Z}. \tag{2.12}$$

The algorithm finds $\mathbf{v} \in \mathcal{L}$ such that the distance between $\mathbf{y}$ and the plane $\mathbf{U} + \mathbf{v}$ is minimal. Let $\mathbf{y}'$ be the orthogonal projection of $\mathbf{y}$ onto the plane $\mathbf{U} + \mathbf{v}$. Let $\mathbf{y}'' = \mathbf{y}' - \mathbf{v}$ and therefore $\mathbf{y}'' \in \mathbf{U}$. Recursively, solve the closest point problem of $\mathbf{y}''$ to obtain $\mathbf{v}' \in \mathcal{L}'$. The result is given by $\mathbf{w} = \mathbf{v} + \mathbf{v}'$. To find $\mathbf{v}$ and the projected query point $\mathbf{y}'$ we proceed as follows. Let us write $\mathbf{y}$ as a linear combination of the orthogonalized basis, that is $\mathbf{y} = \sum_{\ell=1}^{m} \gamma_\ell \mathbf{b}_\ell^*$. Let $\lfloor \gamma_m \rceil$ denote the integer nearest to γ_m. Then $\mathbf{y}' = \sum_{\ell=1}^{m-1} \gamma_\ell \mathbf{b}_\ell^* + \lfloor \gamma_m \rceil \mathbf{b}_m^*$, and $\mathbf{v} = \lfloor \gamma_m \rceil \mathbf{b}_m$.

Algorithm 2 Babai nearest plane algorithm

Input: $\mathbf{y} \in \mathbb{R}^n, \mathbf{B} \in \mathbb{R}^{n \times m}$
Output: $\mathbf{x} \in \mathcal{L}(\mathbf{B})$
1: $[\mathbf{Q}, \mathbf{R}] = QR(\mathbf{B})$
2: $\mathbf{y}^* = \mathbf{Q}^T \mathbf{y}$
3: $\mathbf{c}(m) = \lceil \mathbf{y}^*(m) / \mathbf{R}(m, m) \rfloor$
4: **for** $k = m - 1$ to 1 **do**
5: $\quad \mathbf{c}(k) = \lceil (\mathbf{y}^*(k) - \mathbf{R}(k, k+1 : m)\mathbf{c}(k+1 : m)) / \mathbf{R}(k, k) \rfloor$
6: **end for**
7: $\mathbf{w} = \mathbf{B}\mathbf{c}$

Algorithm 2 shows a version of Babai's nearest plane algorithm that works with a QR-decomposition of the lattice basis $\mathbf{B}$. In line 3 we obtain the integer value for the mth layer describing the nearest plane to the query point. For the next layers with dimension $m - 1$ down to 1 we take into account previous decisions on higher layers and substract their influence on the layer under investigation.

In the field of MIMO detection, Babai's nearest plane algorithm is referred to as suc-

cessive interference cancelation (SIC) or decision feedback detection. The data symbols are detected successively by canceling the contribution of previously detected symbols. For the detection of a data symbol, yet undetected symbols are suppressed ("nulled out"). The fact that a decision on a specific layer will effect all subsequent decisions leads to error propagation whenever a wrong decision is made. Therefore it is advantageous to detect the most reliable layers first.

3

Uniformly Sampled Polynomial Phase Estimation

This chapter deals with the estimation of a uniformly sampled polynomial phase signal, which has several applications in electrical engineering, such as radar, sonar and telecommunications.

Considering the polynomial phase signal of order one, we have two coefficients to estimate, namely the phase and the frequency. This special case is better known as frequency estimation and well studied [18]. Polynomial phase signals of higher order occur in radar and sonar applications where they describe the motion of a target. Furthermore they are applicable to model sounds that are emitted by bats or dolphins for echo location [4].

First we present the angular least squares phase estimator. We will see that the estimation problem can be seen as a closest point search in a lattice. In Section 3.2 the identifiability of polynomial phase parameters is treated. Whenever there is the possibility that several sets of phase coefficients are mapped to the same signal we can't obtain a unique solution. Therefore a so-called identifiable region is introduced, which specifies a region in which the parameters have to lie in order to get a unique solution. Furthermore we will discuss a procedure that resolves aliasing.

In the concluding section, some results of Monte-Carlo simulations of the angular least squares estimator for uniformly sampled polynomial phase samples are shown.

3.1 Angular Least Squares Phase Unwrapping

In this section we describe an estimator for the phase parameters of a polynomial phase signal. The estimator is performing phase unwrapping in a least squares manner. The least squares problem can be solved by using the closest lattice point search. A polynomial phase signal of order m can be modeled in continuous time as

$$y(t) = A(t)e^{j2\pi(p_0+p_1t+\cdots+p_mt^m)} + w(t), \tag{3.1}$$

where $A(t)$ is the signal amplitude, $w(t)$ describes the additive complex noise and $p_0, \ldots, p_m$ denote the polynomial phase parameters. The estimation of the phase parameters is based on a set of samples of $y(t)$. Within this chapter we consider uniform sampling, where the sampling points $\{t_n\}_{n=1}^N$ are regularly spaced. The distance between two consecutive time instants is denoted as $\Delta = t_n - t_{n-1}$. By uniformly sampling the signal $y(t)$ at time instants $\{t_n\}_{n=1}^N$ we get the discrete model

$$y_n = A_n e^{j2\pi(p_0+p_1n\Delta+\cdots+p_m(n\Delta)^m)} + w_n, \tag{3.2}$$

where $n = 1, 2, \ldots, N$. Without loss of generality we will set $\Delta = 1$ here. The argument of the signal y_n, normalized by 2π, reads

$$\theta_n = \frac{\angle y_n}{2\pi} = \sum_{k=0}^{m} p_k n^k + v_n, \tag{3.3}$$

where v_n is the phase noise caused by the additive noise w_n and the signal amplitude A_n. In case the additive noise w_n is complex Gaussian and the signal amplitude A_n is constant, the probability density function (pdf) of the phase noise v_n is the projected

normal distribution (see (3.41) below). Let us rewrite (3.3) in vector form, i.e.,

$$\boldsymbol{\theta} = \mathbf{X}\mathbf{p} + \mathbf{v}, \tag{3.4}$$

where the phase vector with normalized phase entries is denoted by $\boldsymbol{\theta} = (\theta_1 \dots \theta_N)^T$, the phase noise vector by $\mathbf{v} = (v_1 \dots v_N)^T$, and the parameter vector of length m by $\mathbf{p} = (p_1 \dots p_m)^T$. The matrix $\mathbf{X}$ is the $N \times m$ Vandermonde matrix

$$\mathbf{X} = \left[\mathbf{n}^0 \dots \mathbf{n}^m\right] = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 2^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & N & \cdots & N^m \end{bmatrix}, \tag{3.5}$$

with $\mathbf{n}^k = (1^k \; 2^k \dots N^k)^T$.

If the phase $\boldsymbol{\theta}$ is given, the parameter vector $\mathbf{p}$ could be directly estimated according to a simple least squares approach, that is

$$\hat{\mathbf{p}} = \underset{\mathbf{p} \in \mathbb{R}^{m+1}}{\operatorname{argmin}} \|\boldsymbol{\theta} - \mathbf{X}\mathbf{p}\|^2. \tag{3.6}$$

Instead of the true phase $\boldsymbol{\theta}$, however, the measurements usually provide a wrapped version of $\boldsymbol{\theta}$, denoted as $\tilde{\boldsymbol{\theta}} = (\tilde{\theta}_1 \dots \tilde{\theta}_N)^T$. The entries of $\tilde{\boldsymbol{\theta}}$ are given by

$$\tilde{\theta}_n = \sum_{k=0}^{m} p_k n^k + v_n - \left\lfloor \sum_{k=0}^{m} p_k n^k + v_n \right\rceil, \tag{3.7}$$

where $\lfloor \cdot \rceil$ denotes rounding to the nearest integer. The range of the wrapped phase $\tilde{\theta}_n$ is $[-1/2, 1/2)$. The wrapping of the phase corresponds to the subtraction of the nearest integer in (3.7). It can be modeled by an integer variable $u_n = -\left\lfloor \sum_{k=0}^{m} p_k n^k + v_n \right\rceil$.

Therefore we can rewrite (3.7) as

$$\tilde{\theta}_n = \sum_{k=0}^{m} p_k n^k + u_n + v_n, \tag{3.8}$$

or in terms of vectors

$$\tilde{\boldsymbol{\theta}} = \mathbf{X}\mathbf{p} + \mathbf{u} + \mathbf{v}, \tag{3.9}$$

with $\mathbf{u} = (u_1 \dots u_N)^T$.

We see that the true phase of the signal $\boldsymbol{\theta}$ and the wrapped phase $\tilde{\boldsymbol{\theta}}$ are related via the integer vector $\mathbf{u}$ as

$$\tilde{\boldsymbol{\theta}} = \boldsymbol{\theta} + \mathbf{u}. \tag{3.10}$$

An illustration of the phase wrapping is provided in Figure 3.1.

To estimate the phase parameters based on the wrapped phase, we use an extended least squares approach. The parameter vector $\mathbf{p}$ and the unwrapping vector $\mathbf{u}$ are jointly estimated according to

$$(\hat{\mathbf{p}}, \hat{\mathbf{u}}) = \underset{\mathbf{p}\in\mathbb{R}^{m+1}, \mathbf{u}\in\mathbb{Z}^N}{\operatorname{argmin}} \|\tilde{\boldsymbol{\theta}} - \mathbf{X}\mathbf{p} - \mathbf{u}\|^2. \tag{3.11}$$

Fixing the unwrapping vector $\mathbf{u}$ and using linear regression for minimizing with respect to $\mathbf{p}$ we obtain

$$\hat{\mathbf{p}} = \mathbf{X}^{\#}(\tilde{\boldsymbol{\theta}} - \mathbf{u}), \tag{3.12}$$

where $\mathbf{X}^{\#} = (\mathbf{X}^H\mathbf{X})^{-1}\mathbf{X}^H$ is the left pseudoinverse of $\mathbf{X}$. Inserting $\hat{\mathbf{p}}$ into (3.11) yields

$$\hat{\mathbf{u}} = \underset{\mathbf{u}\in\mathbb{Z}^N}{\operatorname{argmin}} \|\mathbf{B}(\tilde{\boldsymbol{\theta}} - \mathbf{u})\|^2. \tag{3.13}$$

Here, $\mathbf{B} = \mathbf{I} - \mathbf{X}\mathbf{X}^{\#}$ is an orthogonal projection matrix. Equation (3.13) describes an integer least squares problem. In the case of uniform sampling, this integer least squares problem can be solved by using a closest point search in a lattice. Let the matrix $\mathbf{B}$

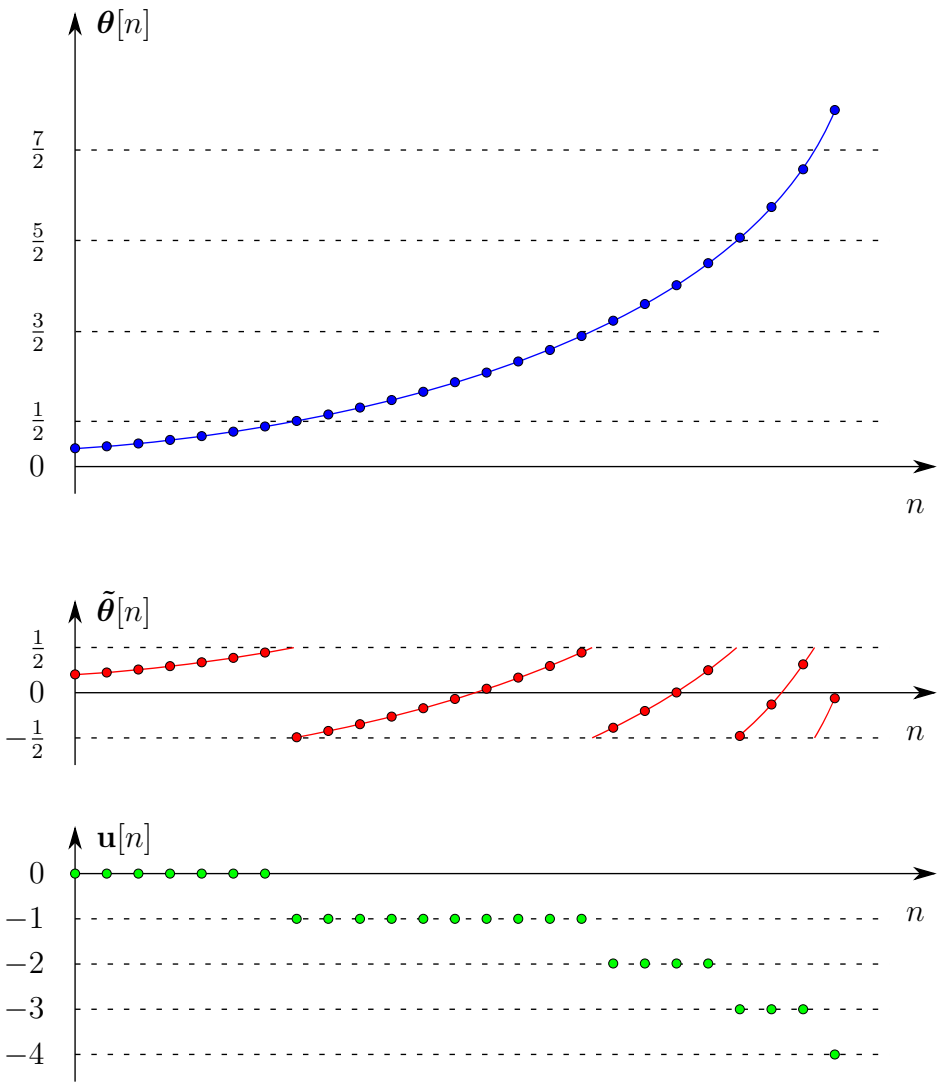

Figure 3.1: *Illustration of the phase wrapping. The unwrapped phase is shown in blue, the wrapped phase in red, and the corresponding unwrapping vector in green. The dots lie on the sampling points.*

be the generator of the lattice $\mathcal{L}$. Then the estimate of the unwrapping vector $\hat{\mathbf{u}}$ is obtained by finding the closest lattice point $\mathbf{B}\hat{\mathbf{u}}$ to the query point $\mathbf{B}\tilde{\boldsymbol{\theta}}$, i.e.,

$$\mathbf{B}\hat{\mathbf{u}} = \mathrm{CPt}\{\mathbf{B}\tilde{\boldsymbol{\theta}}, \mathcal{L}\}. \tag{3.14}$$

In order to get the desired polynomial phase estimate we have to substitute the estimated unwrapping vector $\hat{\mathbf{u}}$ for $\mathbf{u}$ in (3.12). This yields

$$\hat{\mathbf{p}} = \mathbf{X}^{\#}(\tilde{\boldsymbol{\theta}} - \hat{\mathbf{u}}). \tag{3.15}$$

There are many parameter vectors that correctly describe the sampled signal, but only one corresponds to the true signal. This effect is known as aliasing. The estimated parameter $\hat{\mathbf{p}}$ is potentially aliased. In order to get an unambiguous result for the polynomial phase we have to resolve aliasing. A procedure that resolves aliasing will be introduced in 3.2.1.

3.2 Identifiability of Polynomial Phase Parameters

In this section we discuss the effect of aliasing of polynomial phase signal parameters. In spite of the interest for estimation of polynomial phase parameters, aliasing has not been fully clarified. Some results on polynomial phase aliasing have been derived by Ängeby [19]. As a consequence of aliasing, several sets of parameters will be mapped to the same sampled signal.

The aim of polynomial phase estimators is to get a unique result of the phase parameters. We have to restrict the parameters to lie in a specific region, where they are uniquely identifiable and therefore aliasing doesn't occur. According to McKilliam [20], this region will be called identifiable region. With this restriction on the phase parameters we get to know a method how to resolve possibly aliased parameter estimates.

Furthermore we describe how to correctly compute the square error between the true parameters and the estimated parameters.

Let us consider a polynomial phase signal of order m,

$$s(t) = e^{j2\pi\psi(t)}, \quad \text{with} \quad \psi(t) = p_0 + p_1 t + p_2 t^2 + \cdots + p_m t^m. \tag{3.16}$$

Here, $\psi(t)$ is a polynomial of order m. As throughout this chapter, we consider uniform sampling, where the difference between two consecutive sampling points stays constant. The sampled polynomial phase signal then can be written as

$$s_n = e^{j2\pi(p_0 + p_1 n + \cdots + p_m n^m)}, \tag{3.17}$$

where n is an integer. Let $\mathbf{s} = (s_1 \dots s_N)^T$ be the vector of signal samples and $\mathbf{p} = (p_0 \dots p_m)^T$ the parameter vector. We are interested in unique mappings between the phase parameters and the signal samples. This means we have one and only one parameter vector $\mathbf{p}$ that generates the signal samples $\mathbf{s}$.

Let us consider the opposite: $\mathbf{p}$ and $\tilde{\mathbf{p}} = \mathbf{p} + \mathbf{d}$ are two distinct parameter vectors which both yield the same signal samples $\mathbf{s}$, that is

$$\begin{aligned} s_n &= \exp\left(j2\pi \sum_{k=0}^{m} p_k n^k\right) \\ &= \exp\left(j2\pi \sum_{k=0}^{m} (p_k + d_k) n^k\right) \\ &= \exp\left(j2\pi \sum_{k=0}^{m} p_k n^k\right) \exp\left(j2\pi \sum_{k=0}^{m} d_k n^k\right). \end{aligned} \tag{3.18}$$

This ambiguity of the parameters $\mathbf{p}$ and $\tilde{\mathbf{p}}$ occurs if and only if

$$\exp\left(j2\pi \sum_{k=0}^{m} d_k n^k\right) = 1, \tag{3.19}$$

which in turn is equivalent to

$$\sum_{k=0}^{m} d_k n^k \in \mathbb{Z}. \tag{3.20}$$

The set of all additive parameter vectors $\mathbf{d}$ which lead to aliasing is written as

$$D = \left\{ \mathbf{d} \in \mathbb{R}^{m+1} \;\middle|\; \sum_{k=0}^{m} d_k n^k \in \mathbb{Z}, n \in \mathbb{Z} \right\}. \tag{3.21}$$

Let $\mathcal{Z}$ be the set of polynomials of order m that take on integer values when they are evaluated at integer values. Then we can rewrite the set D as

$$D = \left\{ \mathbf{d} \in \text{coef}(z) \;\middle|\; z \in \mathcal{Z} \right\}, \tag{3.22}$$

where $\text{coef}(z)$ denotes the length $m+1$ vector containing the coefficients of z. An integer basis of $\mathcal{Z}$ is given by the integer-valued polynomials $P_k(n)$ [20] defined as

$$P_k(n) = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}, \tag{3.23}$$

with $P_0(n)=1$. That is, every element of $\mathcal{Z}$ can be uniquely written as

$$c_0 P_0(n) + c_1 P_1(n) + \cdots + c_m P_m(n) \quad \text{with} \quad c_i \in \mathbb{Z}. \tag{3.24}$$

Inserting (3.24) into (3.22) yields

$$\begin{aligned} D &= \left\{ \text{coef}\big(c_0 P_0(n) + c_1 P_1(n) + \cdots + c_m P_m(n)\big) \;\middle|\; c_i \in \mathbb{Z} \right\} \\ &= \left\{ c_0 \,\text{coef}\big(P_0(n)\big) + c_1 \,\text{coef}\big(P_1(n)\big) + \cdots + c_m \,\text{coef}\big(P_m(n)\big) \;\middle|\; c_i \in \mathbb{Z} \right\}. \end{aligned} \tag{3.25}$$

By defining the $m+1$ square basis $\bar{\mathbf{B}}$ according to

$$\bar{\mathbf{B}} = \Big[\text{coef}\big(P_0(n)\big) \;\; \text{coef}\big(P_1(n)\big) \;\; \dots \;\; \text{coef}\big(P_m(n)\big) \Big] \tag{3.26}$$

we can represent the set of all additive parameter vectors $\mathbf{d}$ where aliasing occurs in a terms of a lattice, i.e.,

$$D = \left\{ \mathbf{d} = \bar{\mathbf{B}}\mathbf{c} \,\middle|\, \mathbf{c} \in \mathbb{Z}^{m+1} \right\}. \tag{3.27}$$

An identifiable region, i.e., a region where a parameter can be uniquely described, is built by any tessellation region of the aforementioned lattice D. In the following the Voronoi region $\mathcal{V}(D)$ will be taken as a tessellation region. Considering a polynomial phase signal of order $m=3$, the integer valued polynomials are

$$\begin{aligned} P_0(n) &= 1 \\ P_1(n) &= n \\ P_2(n) &= \frac{n^2}{2} - \frac{n}{2} \\ P_3(n) &= \frac{n^3}{6} - \frac{n^2}{2} + \frac{n}{3}. \end{aligned} \tag{3.28}$$

The identifiable region is given by the Voronoi region $\mathcal{V}(D)$ of a lattice generated by the basis

$$\bar{\mathbf{B}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1/2 & 1/3 \\ 0 & 0 & 1/2 & -1/2 \\ 0 & 0 & 0 & 1/6 \end{bmatrix}. \tag{3.29}$$

3.2.1 Resolve Aliasing

Resolving aliasing means that given any polynomial coefficient vector $\tilde{\mathbf{p}}$, we find the equivalent coefficient vector within the identifiable region, denoted $\mathbf{p}$. This is done by

$$\mathbf{p} = \tilde{\mathbf{p}} - \mathrm{CPt}\{\tilde{\mathbf{p}}, D\}, \tag{3.30}$$

where the $\mathrm{CPt}\{\tilde{\mathbf{p}}, D\}$ denotes the closest point search in the lattice D. Since the order of the polynomial phase usually is not too large, the closest point can be computed by

a sphere decoder [2].

3.2.2 Computing Square Error

In the simulations, the performance of the estimator is measured in terms of the mean square error between true and estimated parameters. As McKilliam [20] suggested, the square error of the kth parameter should correctly be computed as ε_k^2, where ε_k is the kth entry of the vector

$$\boldsymbol{\varepsilon} = \mathbf{p} - \hat{\mathbf{p}} - \mathrm{CPt}\{\mathbf{p} - \hat{\mathbf{p}}, D\}. \tag{3.31}$$

Here, the vector of the true coefficients is denoted by $\mathbf{p} = (p_0 \dots p_m)^T$ and the estimated coefficients are written as $\hat{\mathbf{p}} = (\hat{p}_0 \dots \hat{p}_m)^T$.

3.3 Performance Bounds

3.3.1 Cramér-Rao Lower Bound

In estimation theory, the Cramér-Rao lower bound (CRB) is a lower bound on the variance of any unbiased estimator. This is useful, because any unbiased estimator can be compared against the CRB. An estimator achieving the CRB is called efficient.
Let us consider a uniformly sampled polynomial phase signal with amplitude 1 and an additive noise term w_n, i.e.,

$$y_n = e^{j2\pi(p_0 + p_1 n + \cdots + p_m n^m)} + w_n. \tag{3.32}$$

The noise is assumed complex Gaussian with independent real and imaginary part each with variance σ_c^2. The CRB for this scenario has been derived by Peleg and Porat [21]. An approximation for large N is given by

$$\mathrm{cov}\begin{bmatrix} N^{1/2}(p_0 - \hat{p}_0) & \dots & N^{(2m+1)/2}(p_m - \hat{p}_m) \end{bmatrix} \geq \frac{\sigma_c^2}{4\pi^2}\mathbf{H}^{-1}, \tag{3.33}$$

where cov[·] denotes the covariance matrix and $\mathbf{H}$ is the $(m+1)$-dimensional square Hilbert matrix. The elements of the inverse $\mathbf{H}^{-1}$ are given analytically by

$$[\mathbf{H}^{-1}]_{ij} = (-1)^{i+j}(i+j-1)\binom{n+i-1}{n-j}\binom{n+j-1}{n-i}\binom{i+j-2}{i-1}^2. \tag{3.34}$$

For sampling periods Δ different from 1, the CRB has to be adapted. The polynomial phase signal uniformly sampled with a sampling interval Δ is given by

$$y_n = e^{j2\pi(p_0+p_1 n\Delta+\cdots+p_m(n\Delta)^m)} + w_n. \tag{3.35}$$

The sampling rate ν equals $1/\Delta$ and therefore we can write the last equation as

$$y_n = e^{j2\pi(p_0+p_1 n/\nu+\cdots+p_m(n/\nu)^m)} + w_n. \tag{3.36}$$

With respect to the given sampling rate ν the CRB is derived as

$$\operatorname{cov}\left[N^{1/2}(p_0-\hat{p}_0)\ldots N^{(2m+1)/2}(p_m-\hat{p}_m)\right] \geq \frac{\sigma_c^2}{4\pi^2}\mathbf{S}\mathbf{H}^{-1}, \tag{3.37}$$

where

$$\mathbf{S} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \nu^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \nu^{2m} \end{bmatrix}. \tag{3.38}$$

The CRB determines a lower bound for the variance of the kth order parameter estimate. We see that a higher sampling rate ν leads to a higher lower bound for the kth order parameter due to weighting with ν^{2k}.

3.3.2 Asymptotic Variance of the Angular Least Squares Phase Unwrapping

The angular least squares unwrapping estimator has been derived in Section 3.1. Here, the asymptotic properties of this estimator are dealt with. McKilliam [4] stated a proof that the angular least squares estimator is strongly consistent and derived its central limit theorem.

As mentioned in Subsection 3.2.2, the dealiased difference between the true and the estimated parameters is given by $\boldsymbol{\varepsilon} = \mathbf{p} - \hat{\mathbf{p}} - \mathrm{CPt}\{\mathbf{p} - \hat{\mathbf{p}}, D\}$. The central limit theorem states that as N goes to infinity, the distribution of

$$\begin{bmatrix} N^{1/2}\varepsilon_0 & \dots & N^{(2m+1)/2}\varepsilon_m \end{bmatrix} \tag{3.39}$$

converges to normal distribution with zero mean and covariance matrix

$$\frac{\sigma^2}{\left(1 - f(-\frac{1}{2})\right)^2}\mathbf{H}^{-1}, \tag{3.40}$$

where σ^2 is the unwrapped variance of the projected circular random variables just explained. In Section 3.1 we have considered the additive noise term w_n to be complex Gaussian. The distribution of the complex argument of a complex Gaussian random variable is called the projected normal distribution.

Let us consider the special case of uncorrelated real and imaginary part with variance σ_N^2 each and the mean of the complex random noise equals 1. The corresponding pdf is given by Quinn [22] as

$$f(v) = e^{-\frac{1}{2\sigma_N^2}} + \cos(2\pi v) e^{-\frac{\sin^2(2\pi v)}{2\sigma_N^2}} \sqrt{\frac{\pi}{2\sigma_N^2}} \left(1 + \mathrm{erf}\left(\sqrt{\frac{1}{2\sigma_N^2}}\cos(2\pi v)\right)\right). \tag{3.41}$$

The unwrapped variance σ^2, which is used in (3.40), needs to be computed numerically

according to

$$\sigma^2 = \int_{-\frac{1}{2}}^{+\frac{1}{2}} v^2 f(v)\,\mathrm{d}v. \tag{3.42}$$

3.4 Numerical Simulations

In this section we evaluate the statistical performance of the angular least squares estimator using Monte Carlo simulations. The angular least squares estimator has been presented in Section 3.1. It has been shown that the estimation boils down to an integer least squares problem, which in turn is cast into the closest lattice point problem $\mathbf{B}\hat{\mathbf{u}} = \mathrm{CPt}\{\mathbf{B}\tilde{\boldsymbol{\theta}}, \mathcal{L}\}$. In our simulations the closest point problem is approached in the following way:

- The last $m+1$ columns of the lattice generated by $\mathbf{B} = \mathbf{I} - \mathbf{X}\mathbf{X}^{\#}$ are dropped. The new basis matrix is denoted by $\mathbf{B}_{N-m-1}$.
- The LLL algorithm (Algorithm 1) with parameter $\delta = 3/4$ is applied to the basis $\mathbf{B}_{N-m-1}$ resulting in the reduced basis $\tilde{\mathbf{B}}_{\mathrm{red}}$.
- The closest lattice point problem in the lattice with generator $\tilde{\mathbf{B}}_{\mathrm{red}}$ reads

$$\tilde{\mathbf{B}}_{\mathrm{red}}\hat{\mathbf{u}}_{\mathrm{red}} = \mathrm{CPt}\{\mathbf{B}\tilde{\boldsymbol{\theta}}, \tilde{\mathbf{B}}_{\mathrm{red}}\mathbb{Z}^m\}. \tag{3.43}$$

  We use Babai's nearest plane algorithm (Algorithm 2) to obtain an approximate solution for this problem.

- The result is transformed back to the original domain according to $\hat{\mathbf{u}}_{N-m-1} = \mathbf{T}\hat{\mathbf{u}}_{\mathrm{red}}$, where $\mathbf{T}$ is the unimodular transformation matrix derived by the LLL algorithm. We get the unwrapping vector $\hat{\mathbf{u}}$ by appending $m+1$ zeros to $\hat{\mathbf{u}}_{N-m-1}$.

The parameter estimates are then calculated as

$$\hat{\mathbf{p}} = \mathbf{X}^{\#}(\tilde{\boldsymbol{\theta}} - \hat{\mathbf{u}}).$$

As a consequence of the zero padding we might get an aliased version of the true estimate. Here, we resolve aliasing according to (3.30). In the simulations a polynomial phase signals of order $m=3$ is assumed. The noise term w_n is complex Gaussian with independent real and imaginary parts having variance σ_c^2. In this case the Cramér-Rao bound (see Subsection 3.3.1) is approximated by

$$\frac{\sigma_c^2}{4\pi^2}\mathbf{S}\mathbf{H}^{-1}, \tag{3.44}$$

where $\mathbf{S}$ takes into account the sampling rate. Also plotted next to the CRB is the asymptotic variance of the angular least squares estimator (ALS), derived in Subsection 3.3.2. In the simulations, the MSE of the estimator after 2500 trials is computed for each value of SNR $= 1/2\sigma_c^2$ in the range $[0\text{dB}, 20\text{dB}]$. The MSE is calculated according to (3.31). In the following figures the MSE for each parameter is plotted in comparison to the CRB and the ALS.

For Figure 3.2 the true parameters are given by $\mathbf{p}=(0.1, 0.5, 0.01, 0.005)'$. We vary the number of sampling points N on a constant observation interval of the polynomial phase signal ($T=50$). It can bee seen that the estimator performs close to optimum if the signal-to-noise ratio is sufficiently high. The SNR threshold appears around 10dB and moves just slightly as N increases. Furthermore, the threshold is more pronounced for large m. In Figure 3.3 we see how the estimator performs without the LLL algorithm. A rather significant penalty of about 3dB is paid in this case.

For Figure 3.4 the true parameters are uniformly distributed in the identifiable region. The parameters are generated via $\mathbf{p}=\text{CPt}\{\mathbf{u}, D\}$, where D (cf. (3.27)) is generated by the basis matrix in (3.29), and $\mathbf{u}$ is a vector whose elements are independent

and uniformly distributed on $[0, 1)$. Note that Figure 3.4 also shows a curve for $N = 20$ and $T = 50$; in this "undersampled" case the estimator fails.

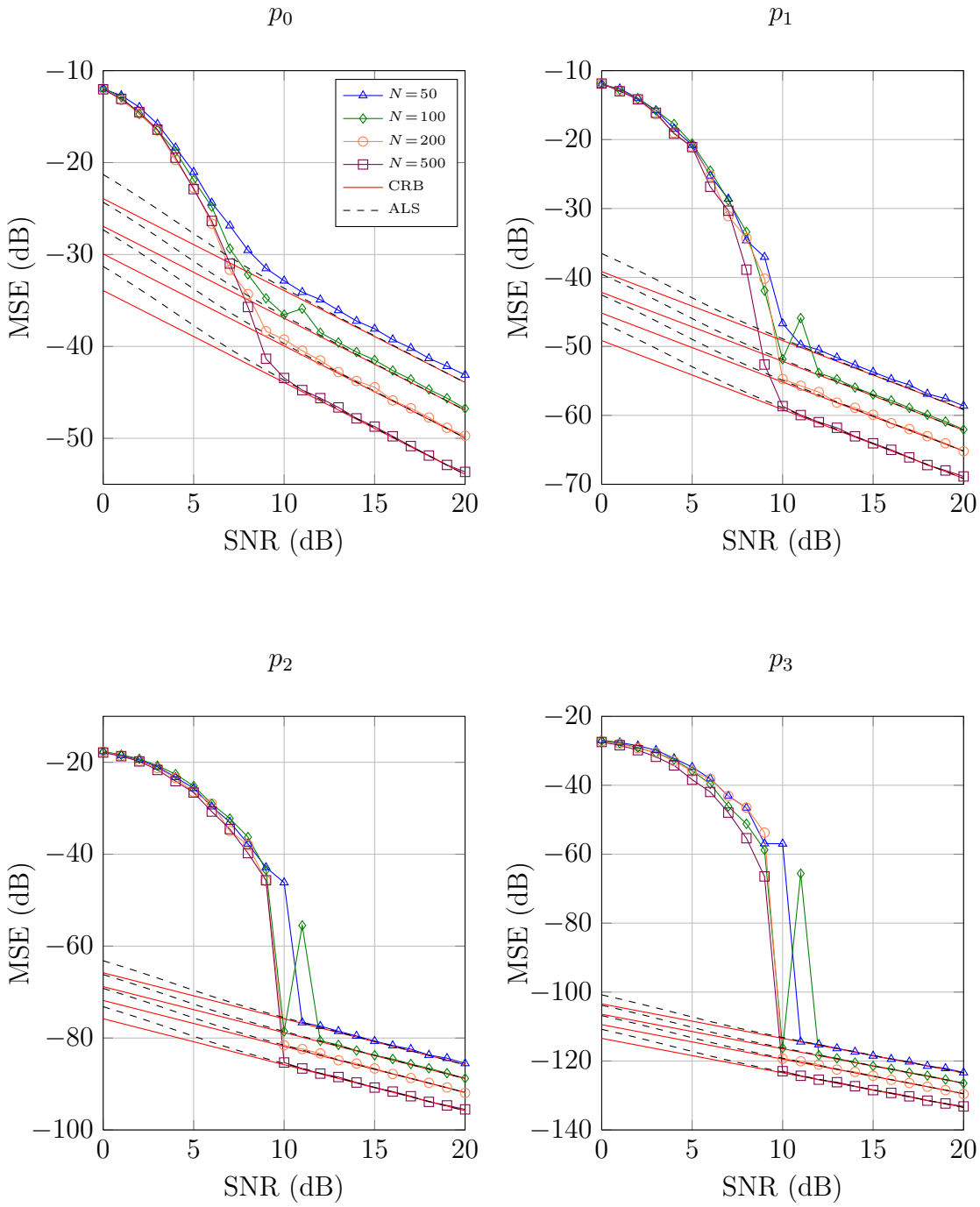

Figure 3.2: *Mean square error for each of the four parameters with* $T=50$ *and* $\mathbf{p}=(0.1, 0.5, 0.01, 0.005)'$.

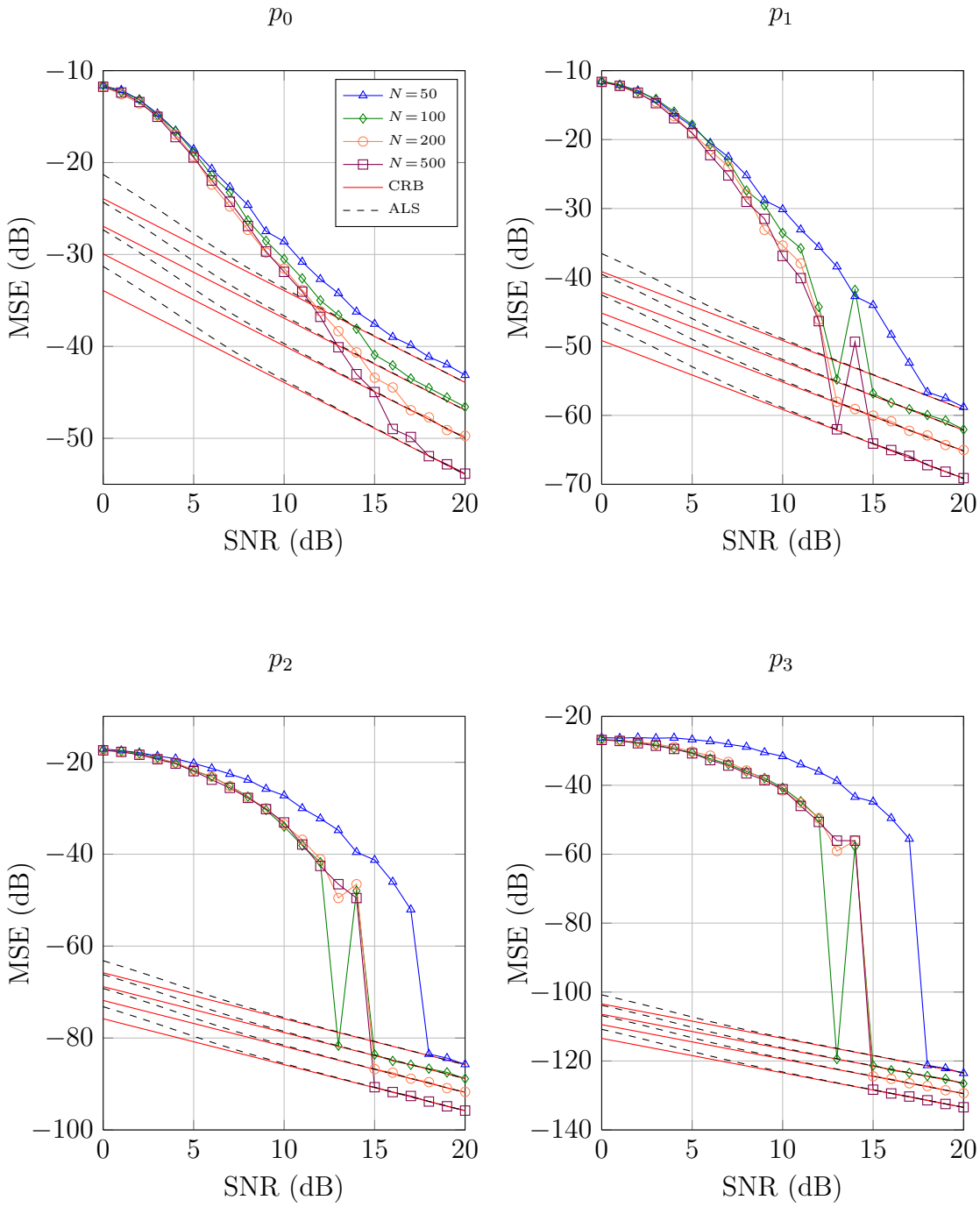

Figure 3.3: *Mean square error for each of the four parameters with* $T=50$ *and* $\mathbf{p}=(0.1, 0.5, 0.01, 0.005)'$. *No LLL algorithm is applied in this case.*

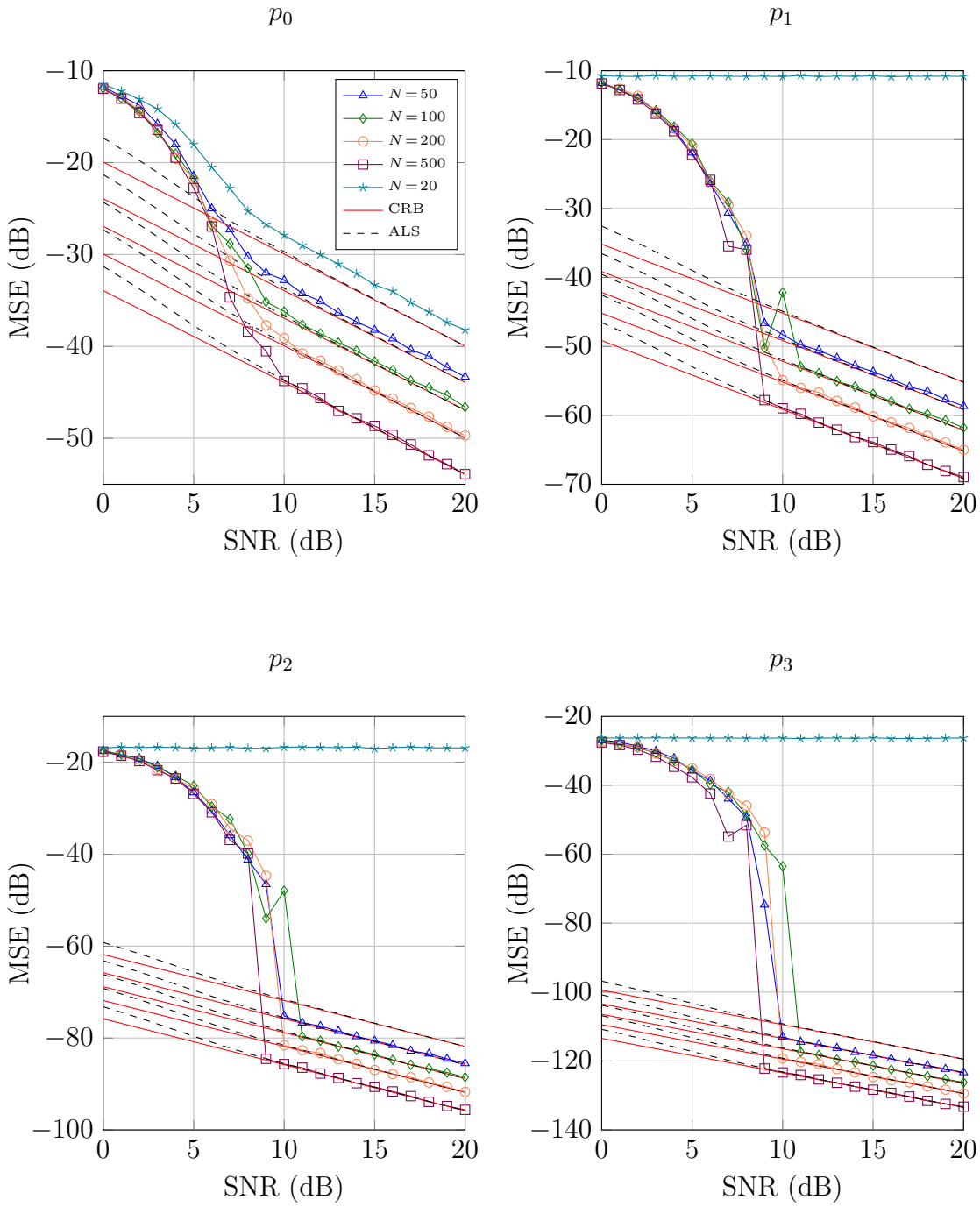

Figure 3.4: *Mean square error for each of the four parameters with* $T=50$ *and* $\mathbf{p}$ *uniformly distributed in the identifiable region.*

4

Nonuniformly Sampled Polynomial Phase Estimation

In this chapter we consider nonuniformly sampled phase estimation. Again we introduce the angular least squares estimator to get an estimate of a polynomial phase signal, but unlike in Chapter 3 the estimation is based on nonuniform samples of a signal.

The treatment of nonuniformly sampled signal phase estimation is motivated by Ängeby [19]. He suggests that aliasing can be avoided by nonuniform sampling, specifically, when the signal samples are irrationally spaced. This is the case when the sampling instants are randomly generated.

In Section 4.2 the identifiability of polynomial phase parameters in the nonuniform sampling scenario is considered. In Section 4.3 we present some simulation results for the nonuniformly sampled phase estimation based on the angular least squares approach.

4.1 Angular Least Squares Phase Unwrapping

Like in Chapter 3 we assume a polynomial phase signal of order m which is modeled in continuous time as

$$y(t) = A(t)e^{j2\pi(p_0+p_1t+\cdots+p_mt^m)} + w(t). \tag{4.1}$$

Here, $A(t)$ is the signal amplitude, $w(t)$ describes the additive complex noise, and $p_0, \ldots, p_m$ denote the polynomial phase parameters. Again the estimation of the phase parameters is based on a set of samples of $y(t)$, but unlike in Chapter 3, the sampling points $\{t_n\}_{n=1}^N$ are irregularly spaced. The sampled polynomial phase signal is written as

$$y(t_n) = A(t_n)e^{j2\pi(p_0+p_1t_n+\cdots+p_mt_n^m)} + w(t_n). \tag{4.2}$$

The sampled argument of the signal $y(t)$ is given by

$$\theta[n] = \frac{\angle y(t_n)}{2\pi} = \sum_{k=0}^{m} p_k t_n^k + v[n], \tag{4.3}$$

where $v[n]$ is the phase noise caused by the additive noise $w(t_n)$ and the signal amplitude $A(t_n)$. By assuming the additive noise to be complex Gaussian and the signal amplitude to be constant, the phase noise is distributed according to the projected normal distribution (3.41).

Let $\mathbf{v} = (v[1] \ldots v[N])^T$ denote the phase noise vector, $\boldsymbol{\theta} = (\theta[1] \ldots \theta[N])^T$ be the phase vector with normalized entries, and $\mathbf{p} = (p_1 \ldots p_m)^T$ be the parameter vector of length m. We express (4.3) in vector notation as

$$\boldsymbol{\theta} = \mathbf{L}\mathbf{p} + \mathbf{v}, \tag{4.4}$$

where $\mathbf{L}$ is the $N \times m$ matrix given by

$$\mathbf{L} = \left[\mathbf{l}^0 \dots \mathbf{l}^m\right] = \begin{bmatrix} 1 & t_1 & \cdots & t_1^m \\ 1 & t_2 & \cdots & t_2^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_N & \cdots & t_N^m \end{bmatrix}. \tag{4.5}$$

The length N vector $\mathbf{l} = (t_1 \dots t_N)^T$ denotes the vector of the nonuniform sampling points.

With the knowledge of the unwrapped phase $\boldsymbol{\theta}$, the parameter vector $\mathbf{p}$ could be directly estimated in a least squares manner, according to

$$\hat{\mathbf{p}} = \underset{\mathbf{p}\in\mathbb{R}^{m+1}}{\operatorname{argmin}} \|\boldsymbol{\theta} - \mathbf{L}\mathbf{p}\|^2. \tag{4.6}$$

Instead of the true phase $\boldsymbol{\theta}$, the measurements correspond to a wrapped version of the phase, where the phase values are given by

$$\tilde{\theta}[n] = \sum_{k=0}^{m} p_k t_n^k + v[n] - \left\lfloor \sum_{k=0}^{m} p_k t_n^k + v[n] \right\rceil, \tag{4.7}$$

and therefore lie in the interval $[-1/2, 1/2)$. The wrapped phases are stacked into the vector $\tilde{\boldsymbol{\theta}} = (\tilde{\theta}[1] \dots \tilde{\theta}[N])^T$. As done in the uniform sampling case, we model the wrapping by an integer vector $\mathbf{u} = (u_1 \dots u_N)^T$ whose entries are given by $u_n = -\left\lfloor \sum_{k=0}^{m} p_k t_n^k + v[n] \right\rceil$. The true phase $\boldsymbol{\theta}$ of the signal and the wrapped phase $\tilde{\boldsymbol{\theta}}$ are related via the integer vector $\mathbf{u}$ as

$$\tilde{\boldsymbol{\theta}} = \boldsymbol{\theta} + \mathbf{u}. \tag{4.8}$$

An illustration of the unwrapped phase $\boldsymbol{\theta}$, the wrapped phase $\tilde{\boldsymbol{\theta}}$ and the corresponding unwrapping vector $\mathbf{u}$ is given in Figure 4.1. Inserting (4.4) into (4.8) yields

$$\tilde{\boldsymbol{\theta}} = \mathbf{L}\mathbf{p} + \mathbf{u} + \mathbf{v}. \tag{4.9}$$

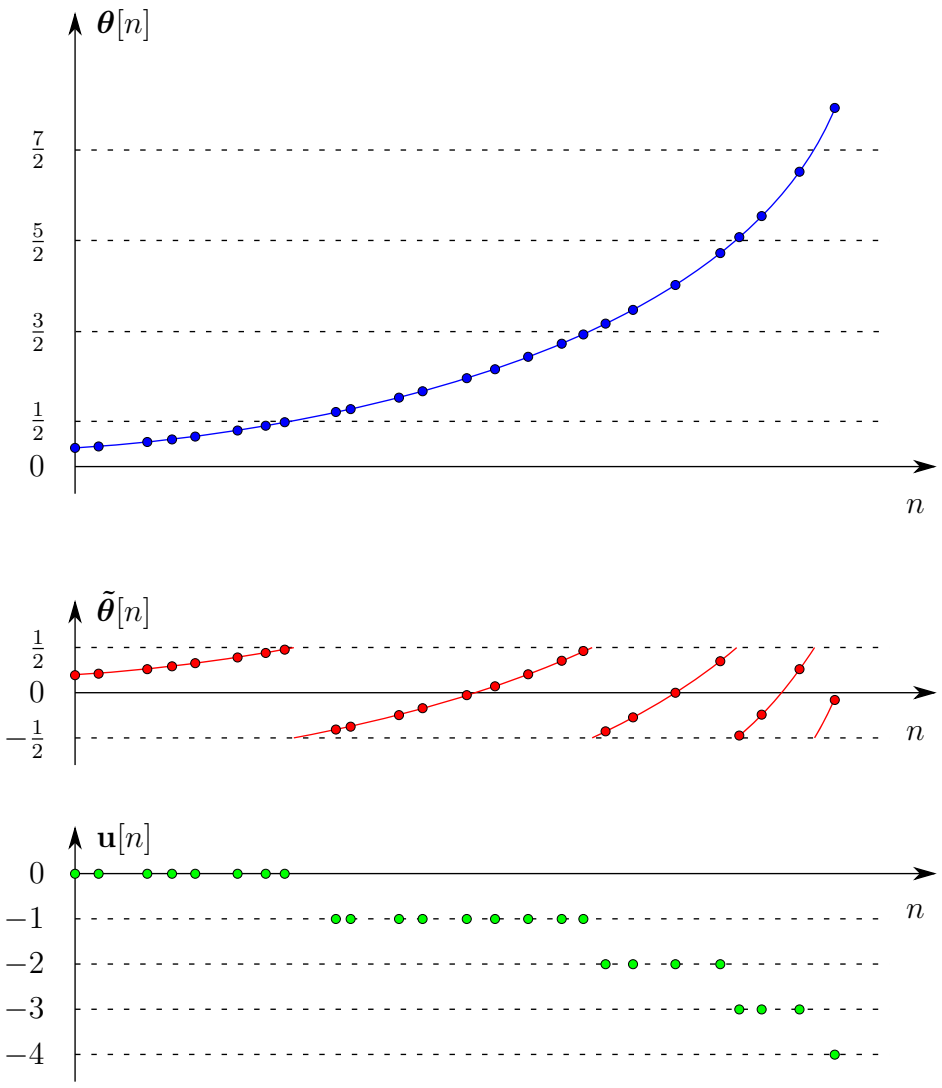

Figure 4.1: *Illustration of the phase wrapping. The unwrapped phase is shown in blue, the wrapped phase in red, and the corresponding unwrapping vector in green. The dots lie on the sampling points.*

For the estimation we use an extended least squares approach where the estimation of the parameter vector $\mathbf{p}$ and the unwrapping vector $\mathbf{u}$ is done jointly, written as

$$(\hat{\mathbf{p}}, \hat{\mathbf{u}}) = \underset{\mathbf{p}\in\mathbb{R}^{m+1},\mathbf{u}\in\mathbb{Z}^N}{\operatorname{argmin}} \|\tilde{\boldsymbol{\theta}} - \mathbf{L}\mathbf{p} - \mathbf{u}\|^2 \tag{4.10}$$

By fixing the unwrapping vector $\mathbf{u}$ and using linear regression for minimizing with respect to $\mathbf{p}$ we get

$$\hat{\mathbf{p}} = \mathbf{L}^{\#}(\tilde{\boldsymbol{\theta}} - \mathbf{u}), \tag{4.11}$$

where $\mathbf{L}^{\#} = (\mathbf{L}^H\mathbf{L})^{-1}\mathbf{L}^H$ is the left pseudoinverse of $\mathbf{L}$. By substituting $\mathbf{p}$ in (4.10) by the estimated vector $\hat{\mathbf{p}}$, we obtain

$$\hat{\mathbf{u}} = \underset{\mathbf{u}\in\mathbb{Z}^N}{\operatorname{argmin}} \|\mathbf{B}(\tilde{\boldsymbol{\theta}} - \mathbf{u})\|^2, \tag{4.12}$$

where $\mathbf{B} = \mathbf{I} - \mathbf{L}\mathbf{L}^{\#}$ is an orthogonal projection matrix into the space orthogonal to the column span of $\mathbf{L}$.

Aforementioned Equation (4.12) describes an integer least squares problem which potentially can be solved by using the closest point search in the lattice generated by $\mathbf{B}$. The approach is the same as in the uniform sampled case. First, the estimate of the unwrapping vector $\hat{\mathbf{u}}$ is determined by finding the closest lattice point $\mathbf{B}\hat{\mathbf{u}}$ to the query point $\mathbf{B}\tilde{\boldsymbol{\theta}}$, i.e., $\mathbf{B}\hat{\mathbf{u}} = \mathrm{CPt}\{\mathbf{B}\tilde{\boldsymbol{\theta}}, \mathcal{L}\}$. Inserting the achieved unwrapping vector $\hat{\mathbf{u}}$ into (4.11), we get an estimated parameter vector according to

$$\hat{\mathbf{p}} = \mathbf{L}^{\#}(\tilde{\boldsymbol{\theta}} - \hat{\mathbf{u}}). \tag{4.13}$$

Since there is no aliasing[1] occurring whenever the sampling points are irrationaly spaced, we don't have to resolve aliasing like we have done in the uniformly sampled case.

[1] In fact aliasing w.r.t.$\mathbf{p}_0$ can occur. This corresponds to a constant phase shift of the signal samples by a multiple of 2π. However, it does not need to be resolved because the wrapping operation always restricts the initial phase to lie in $[-1/2, 1/2)$.

4.2 Identifiability of Polynomial Phase Parameters

In Section 3.2 we faced the problem of aliasing in the uniform sampling scenario. Ängeby [19] suggests that aliasing can be avoided by nonuniform sampling if the time interval between some samples is irrational. McKilliam [20] observes that this is true in the noiseless case but leads to a large estimation error when noise is present.

Let $y(t)$ be a polynomial phase signal in continuous time, i.e.,

$$y(t) = A(t)e^{j2\pi(p_0+p_1t+\cdots+p_mt^m)} + w(t). \tag{4.14}$$

The nonuniformly sampled version of the signal $y(t)$ with given parameter vector $\mathbf{p}$ reads as

$$y_{\mathbf{p}}(t_n) = A(t_n)e^{j2\pi(p_0+p_1t_n+\cdots+p_mt_n^m)} + w(t_n). \tag{4.15}$$

We assume the noiseless case, i.e., $w(t) = 0$ and furthermore the amplitude $A(t) = 1$. The noiseless signal is then given by

$$s_{\mathbf{p}}(t_n) = \exp\left(j2\pi\sum_{k=0}^{m} p_k t_n^k\right). \tag{4.16}$$

Using Kronecker's approximation theorem [23] it can be shown that for $\epsilon > 0$ there exists a $\tilde{\mathbf{p}} \neq \mathbf{p}$ such that $\|\tilde{\mathbf{p}} - \mathbf{p}\| > \delta$ for any $\delta > 0$ and

$$|s_{\mathbf{p}}(t_n) - s_{\tilde{\mathbf{p}}}(t_n)|^2 < \epsilon, \tag{4.17}$$

for all $n = 1, 2, \ldots, N$. There are an infinite number of such $\tilde{\mathbf{p}}$ for arbitrary large δ. In other words, the true signal described by $\mathbf{p}$ is close to an infinite number of signals each described by $\tilde{\mathbf{p}}$. The least squares estimator of $\mathbf{p}$ considering the noisy signal

$s_{\mathbf{p}}(t_n) + w(t_n)$ is given by

$$\underset{\tilde{\mathbf{p}}\in\mathbb{R}^{m+1}}{\operatorname{argmin}} \sum_{n=1}^{N} |s_{\mathbf{p}}(t_n) + w(t_n) - s_{\tilde{\mathbf{p}}}(t_n)|^2. \tag{4.18}$$

As a consequence of (4.17) we can not be sure to obtain the true parameter $\mathbf{p}$ because of the infinite number of close signals.

In the uniform sampling case we have seen that several parameter lead to the same signal (this effect was called aliasing). We have solved this problem by restricting the parameters to lie in an identifiable region and have resolved the aliasing effect. When the signal is nonuniformly sampled with irrational sampling instants we avoid the ambiguity of parameters. The parameters are therefore uniquely identifiable.[2] However, there remains the drawback of having an infinite amount of almost ambiguous parameters. This is crucial when we consider a noisy signal.

4.3 Simulations

In this section we present Monte Carlo simulations of the angular least squares estimator, which we have introduced in Section 4.1. The occurring closest lattice point problem $\mathbf{B}\hat{\mathbf{u}} = \mathrm{CPt}\{\mathbf{B}\tilde{\boldsymbol{\theta}}, \mathcal{L}\}$ can't be exactly solved by the approach from Section 3.4. Therefore we use the following suboptimal ad hoc approach:

- The first $m+1$ columns of the lattice generated by $\mathbf{B} = \mathbf{I} - \mathbf{L}\mathbf{L}^{\#}$ are dropped. The new basis matrix is denoted by $\mathbf{B}_{N-m-1}$.
- The LLL algorithm (Algorithm 1) with parameter $\delta = 3/4$ is applied to the basis $\mathbf{B}_{N-m-1}$; the reduced basis is denoted by $\tilde{\mathbf{B}}_{\mathrm{red}}$.

[2] This excludes the parameter $\mathbf{p}_0$ which describes the constant phase component.

- The closest lattice point problem in the lattice with the generator $\tilde{\mathbf{B}}_{\text{red}}$ reads as

$$\tilde{\mathbf{B}}_{\text{red}}\hat{\mathbf{u}}_{\text{red}} = \text{CPt}\{\mathbf{B}_{N-m-1}\tilde{\boldsymbol{\theta}}_{N-m-1}, \tilde{\mathbf{B}}_{\text{red}}\mathbb{Z}^m\}. \tag{4.19}$$

  We use Babai's nearest plane algorithm (Algorithm 2) to obtain an approximate solution to the problem (4.19). Note that the "observed" point is determined by $\tilde{\boldsymbol{\theta}}_{N-m-1}$, which is obtained by dropping the first $m+1$ entries of $\tilde{\boldsymbol{\theta}}$.

- The result is transformed back to the original domain according to $\hat{\mathbf{u}}_{N-m-1} = \mathbf{T}\hat{\mathbf{u}}_{\text{red}}$, where $\mathbf{T}$ is the unimodular transformation matrix derived by the LLL algorithm.

The parameter estimates are calculated according to

$$\hat{\mathbf{p}} = \mathbf{L}^{\#}_{N-m-1}(\tilde{\boldsymbol{\theta}}_{N-m-1} - \hat{\mathbf{u}}_{N-m-1}), \tag{4.20}$$

where $\mathbf{L}_{N-m-1}$ is obtained by dropping the first $m+1$ rows of $\mathbf{L}$. Since there is no zero padding of the unwrapping vector, we don't get an aliased version as in Chapter 3.4. In the simulations a polynomial phase signals of order $m=3$ is used. The noise term $w(t_n)$ is complex Gaussian with independent real and imaginary parts having variance σ_c^2. In this case the Cramér-Rao bound (see Subsection 3.3.1) is approximated by

$$\frac{\sigma_c^2}{4\pi^2}\mathbf{S}\mathbf{H}^{-1}, \tag{4.21}$$

where $\mathbf{S}$ takes into account the average sampling rate ν (see definition of $\mathbf{S}$ in (3.38)). Also plotted next to the CRB is the asymptotic variance of the angular least squares estimator (ALS), derived in Subsection 3.3.2. The MSE of the estimator is computed for each value of SNR $= 1/2\sigma_c^2$ in the range $[0\text{dB}, 20\text{dB}]$. For the simulations we took 25 sets of randomly generated sampling points, and ran 100 trials for each set. The MSE for each parameter p_k (calculated via $(p_k - \hat{p}_k)^2$) is plotted against the CRB and

the ALS in the following figures. The true parameters are uniformly distributed over a region obtained from the identifiable region (see Section 3.4) by scaling with a factor $1/2$.

In Figure 4.2 the number of sampling points N is varied, while the observation interval of the polynomial phase signal ($T=10$) is constant. It can bee seen that except for $N=20$, the estimator performs well when the SNR is above 15dB. Furthermore we can see gap between the MSE of the estimator and the corresponding CRB in the high SNR scenarios. This gap gets smaller as the number of sampling points N increases. The gap could be due to the fact that the estimation is based on a reduced data vector $\tilde{\boldsymbol{\theta}}_{N-m-1}$. Since we are always dropping $m+1$ columns, this effect is negligible for a high number of sampling points. In Figure 4.2, a curve for $N=20$ and $T=50$ is plotted. In this "undersampled" case the estimator fails. In Figure 4.3 the observation interval of the polynomial phase signal is set to ($T=20$). For $N \leq 100$ the estimator doesn't work properly, this suggests that one has to satisfy a minimum average sampling rate $\nu = N/T$. From the simulation results it seems that a minimum average sampling rate $\nu = 10$ is sufficient. Figure 4.4 displays curves for a fixed number of sampling points $T=500$. For observation time intervals $T \leq 50$ the estimation of the phase parameters works. This supports the assumption of a required average sampling rate $\nu = 10$.

In the simulations the calculation of the MSE is a crucial point. If Babai's algorithm is not delivering the closest lattice point, the unwrapping vector can get large due to the transformation with the unimodular matrix $\mathbf{T}$. This can lead to large differences between the parameter estimates and the true parameters. In the case of uniformly sampled polynomial phase estimation we have faced large differences between true and estimated parameters as well but there it has been caused by the aliasing effect.

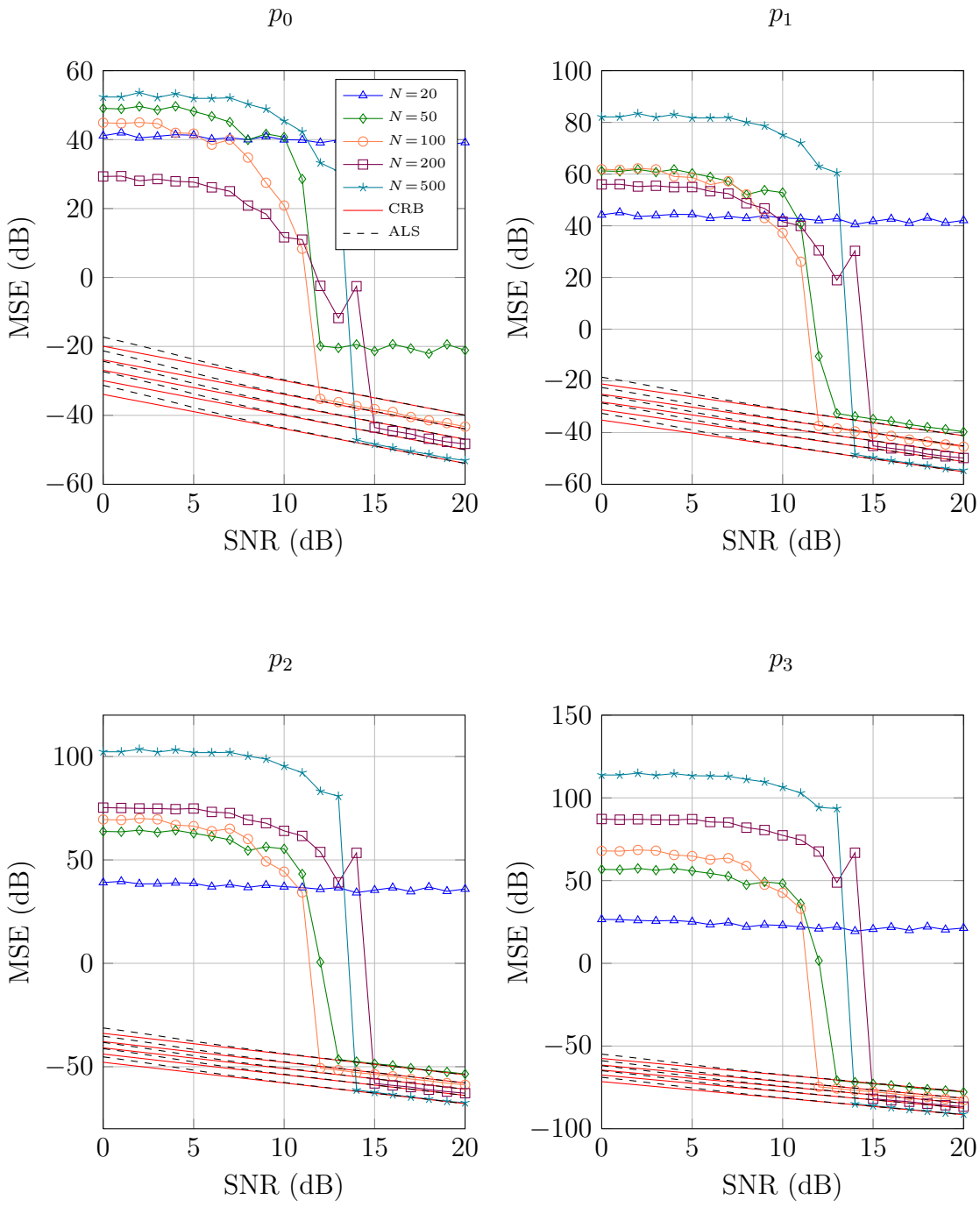

Figure 4.2: *Mean square error for each of the four parameters with* $T=10$ *and* $\mathbf{p}$ *uniformly distributed in a downscaled identifiable region.*

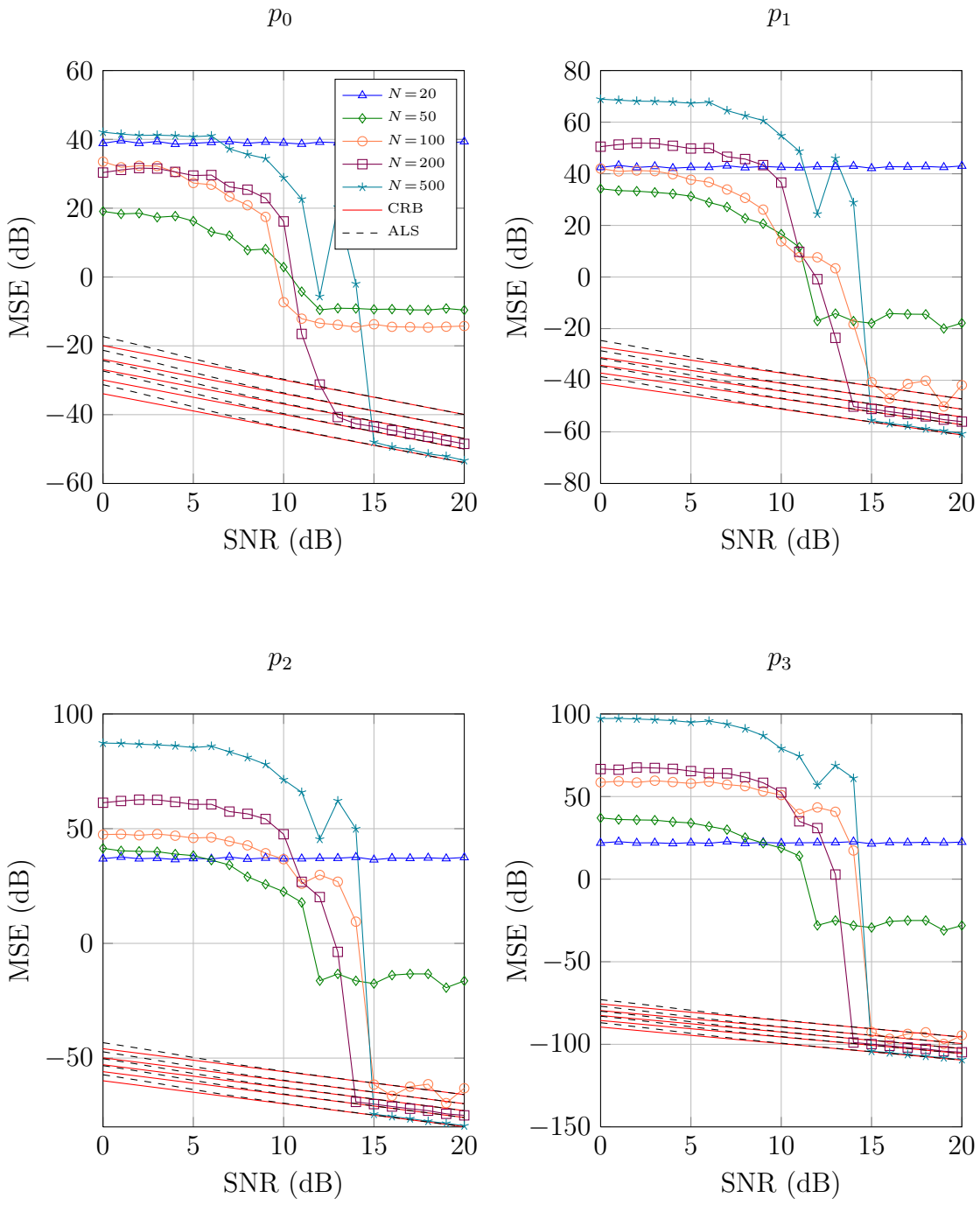

Figure 4.3: *Mean square error for each of the four parameters with $T = 20$ and* $\mathbf{p}$ *uniformly distributed in a downscaled identifiable region.*

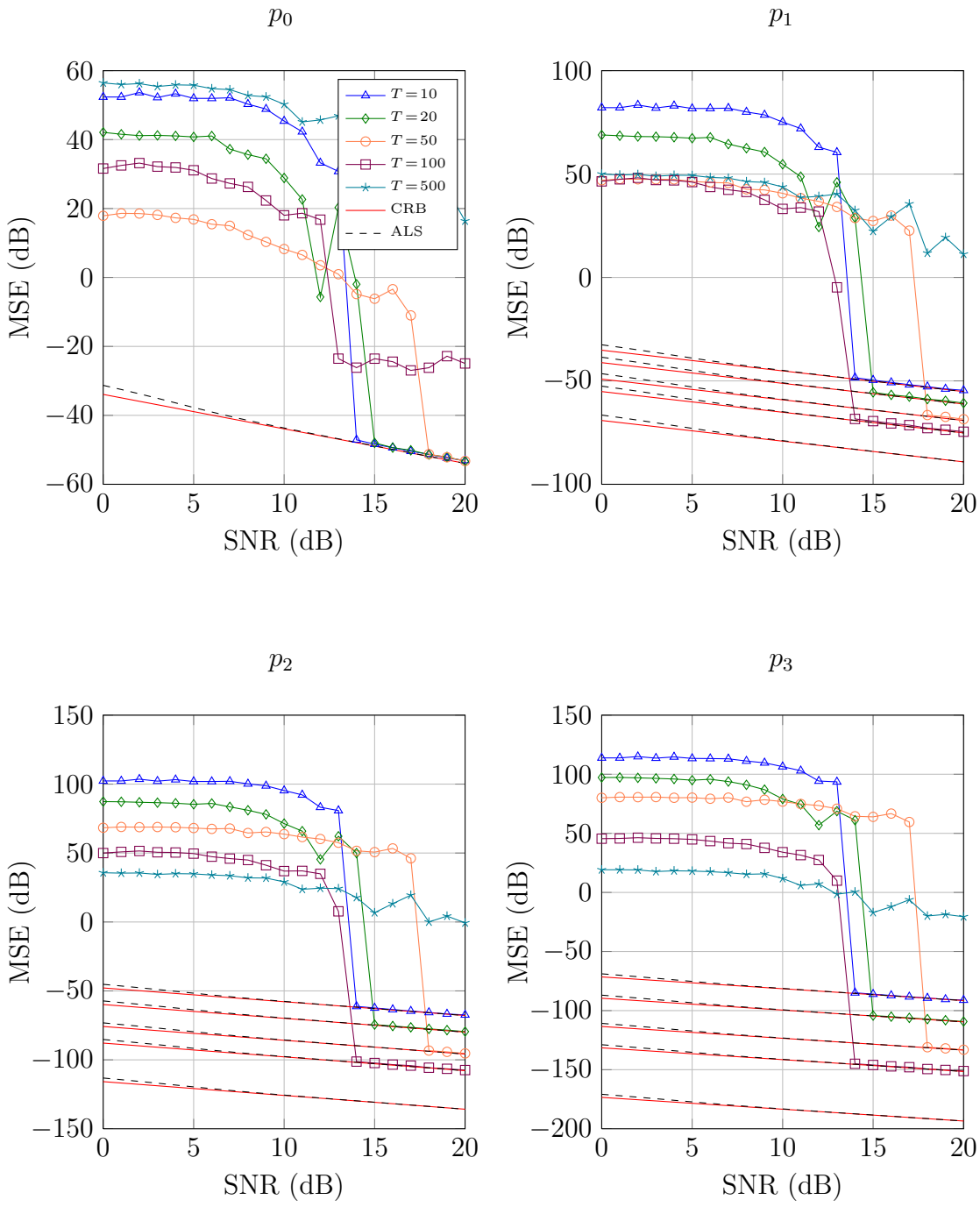

Figure 4.4: *Mean square error for each of the four parameters with* $N=500$ *and* $\mathbf{p}$ *uniformly distributed in a downscaled identifiable region.*

5

Fourier-Based Phase Estimation

In the previous Chapters 3 and 4 we used an angular least squares approach to estimate a polynomial phase signal. The polynomial phase description offers the possibility to model signals with high dynamics. If a bandlimited phase signal needs to be estimated, it might be of advantage to express the phase in terms of a Fourier basis. In this chapter we estimate a Fourier-based signal. Like in Chapter 3 the estimation relies on uniformly taken samples of the signal.

In Section 5.1 the angular least squares approach is formulated. Section 5.2 deals with the identifiability of Fourier-based phase signals. In the concluding section some simulation results for Fourier-based phase estimation are given.

5.1 Angular Least Squares Phase Unwrapping

We assume a continuous-time signal which is modeled as

$$y(t) = A(t)e^{j2\pi\psi(t)} + w(t), \quad \text{with} \quad 0 \leq t < T. \tag{5.1}$$

Here, $A(t)$ being the signal amplitude, and $w(t)$ denoting the additive complex noise. The phase function $\psi(t)$ is modeled using a Fourier basis expansion, i.e.,

$$\psi(t) = \sum_{k=0}^{m} f_k(t)p_k, \tag{5.2}$$

where the linearly independent Fourier basis functions $f_k(t)$ are given by

$$\begin{aligned} f_0(t) &= 1 \\ f_1(t) &= \cos\left(2\pi\frac{t}{T}\right) \\ f_2(t) &= \sin\left(2\pi\frac{t}{T}\right) \\ f_3(t) &= \cos\left(4\pi\frac{t}{T}\right) \\ f_4(t) &= \sin\left(4\pi\frac{t}{T}\right) \\ &\vdots \end{aligned} \tag{5.3}$$

Within this chapter we consider uniform sampling. This means, the sampling points are regularly spaced, i.e., $\{t_n\}_{n=1}^{N} = 1, 2, \ldots, N$. The sampled signal $y[n]$ is written as

$$y[n] = A[n]e^{j2\pi\psi[n]} + w[n], \quad \text{with} \quad \psi[n] = \sum_{k=0}^{m} f_k[n]p_k. \tag{5.4}$$

Here, $\psi[n]$ is the sampled phase function which is expressed by the basis expansion using the sampled Fourier basis

$$\begin{aligned} f_0[n] &= 1 \\ f_1[n] &= \cos\left(2\pi\frac{n}{N}\right) \\ f_2[n] &= \sin\left(2\pi\frac{n}{N}\right) \\ f_3[n] &= \cos\left(4\pi\frac{n}{N}\right) \\ f_4[n] &= \sin\left(4\pi\frac{n}{N}\right) \\ &\vdots \end{aligned} \tag{5.5}$$

The sampled argument of the signal $y(t)$ is given by

$$\theta[n] = \frac{\angle y[n]}{2\pi} = \sum_{k=0}^{m} f_k[n]p_k + v[n], \tag{5.6}$$

where $v[n]$ is the phase noise caused by the additive noise $w[n]$ and the signal amplitude $A[n]$. By assuming the additive noise to be complex Gaussian and the signal amplitude to be constant, the phase noise is distributed according to the projected normal distribution (3.41).

Let $\mathbf{v} = (v[1] \dots v[N])^T$ be the phase noise vector, $\boldsymbol{\theta} = (\theta[1] \dots \theta[N])^T$ the phase vector with normalized phase entries, and $\mathbf{p} = (p_1 \dots p_m)^T$ the parameter vector of length m. We rewrite (5.6) in a vector notation, that is

$$\boldsymbol{\theta} = \mathbf{F}\mathbf{p} + \mathbf{v}, \tag{5.7}$$

where $\mathbf{F}$ is the $N \times m$ Fourier matrix

$$\mathbf{F} = \Big[\mathbf{f}_0 \dots \mathbf{f}_m\Big] = \begin{bmatrix} 1 & \cos\left(2\pi\frac{1}{N}\right) & \cdots & f_m[1] \\ 1 & \cos\left(2\pi\frac{2}{N}\right) & \cdots & f_m[2] \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \cos\left(2\pi\frac{N}{N}\right) & \cdots & f_m[N] \end{bmatrix}. \tag{5.8}$$

Here, $\mathbf{f}_k = (f_k[1] \dots f_k[N])^T$ is the column vector of the Fourier basis function $f_k[n]$ evaluated at the sampling points.

If the phase $\boldsymbol{\theta}$ is given, the parameter vector $\mathbf{p}$ could be directly estimated according to a simple least squares approach, that is

$$\hat{\mathbf{p}} = \underset{\mathbf{p}\in\mathbb{R}^{m+1}}{\operatorname{argmin}} \|\boldsymbol{\theta} - \mathbf{F}\mathbf{p}\|^2. \tag{5.9}$$

Instead of the true phase $\boldsymbol{\theta}$, a wrapped version of the phase is measured, where the phase values are given by

$$\tilde{\theta}[n] = \sum_{k=0}^{m} f_k[n]p_k + v[n] - \left\lfloor \sum_{k=0}^{m} f_k[n]p_k + v[n] \right\rceil. \tag{5.10}$$

The range of the wrapped phase $\tilde{\theta}[n]$ is $[-1/2, 1/2)$. We again model the wrapping by an integer vector $\mathbf{u} = (u_1 \dots u_N)^T$ whose entries are given by $u_n = -\left\lfloor \sum_{k=0}^{m} f_k[n]p_k + v[n] \right\rceil$. The true phase of the signal $\boldsymbol{\theta}$ and the wrapped phase $\tilde{\boldsymbol{\theta}}$ are related via the integer vector $\mathbf{u}$, such that

$$\tilde{\boldsymbol{\theta}} = \boldsymbol{\theta} + \mathbf{u}. \tag{5.11}$$

An illustration of the unwrapped phase $\boldsymbol{\theta}$, the wrapped phase $\tilde{\boldsymbol{\theta}}$, and the corresponding unwrapping vector $\mathbf{u}$ is given in Figure 5.1. Inserting (5.7) into (5.11) yields

$$\tilde{\boldsymbol{\theta}} = \mathbf{F}\mathbf{p} + \mathbf{u} + \mathbf{v}. \tag{5.12}$$

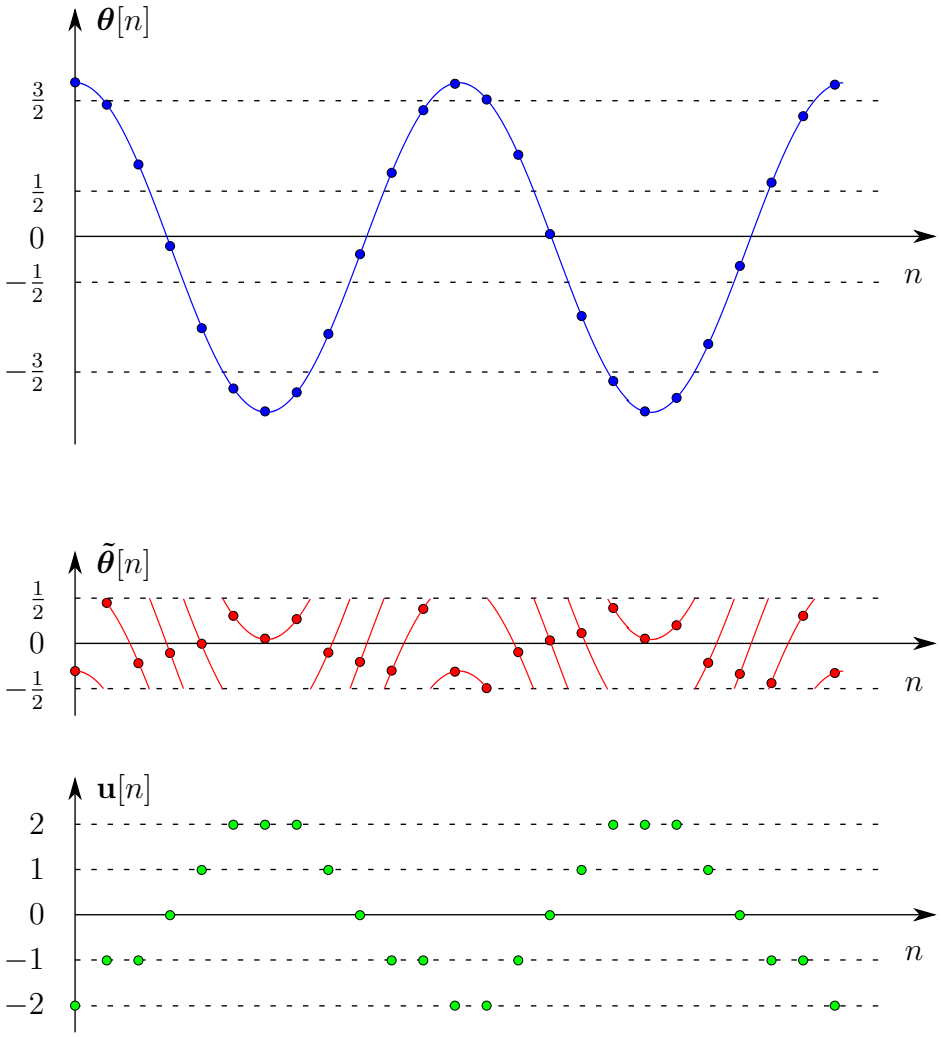

Figure 5.1: *Illustration of the phase wrapping. The unwrapped phase is shown in blue, the wrapped phase in red, and the corresponding unwrapping vector in green. The dots lie on the sampling points.*

We use an extended least squares approach, where the parameter vector $\mathbf{p}$ and the unwrapping vector $\mathbf{u}$ are jointly estimated, that is

$$(\hat{\mathbf{p}}, \hat{\mathbf{u}}) = \underset{\mathbf{p}\in\mathbb{R}^{m+1}, \mathbf{u}\in\mathbb{Z}^N}{\operatorname{argmin}} \|\tilde{\boldsymbol{\theta}} - \mathbf{F}\mathbf{p} - \mathbf{u}\|^2. \tag{5.13}$$

Fixing the unwrapping vector $\mathbf{u}$ and using linear regression for minimizing with respect to $\mathbf{p}$ we obtain

$$\hat{\mathbf{p}} = \mathbf{F}^{\#}(\tilde{\boldsymbol{\theta}} - \mathbf{u}), \tag{5.14}$$

where $\mathbf{F}^{\#} = (\mathbf{F}^H\mathbf{F})^{-1}\mathbf{F}^H$ is the left pseudoinverse of $\mathbf{F}$. Inserting $\hat{\mathbf{p}}$ into (5.13) yields

$$\hat{\mathbf{u}} = \underset{\mathbf{u}\in\mathbb{Z}^N}{\operatorname{argmin}} \|\mathbf{B}(\tilde{\boldsymbol{\theta}} - \mathbf{u})\|^2, \tag{5.15}$$

where $\mathbf{B} = \mathbf{I} - \mathbf{F}\mathbf{F}^{\#}$ is the orthogonal projection matrix into the space orthogonal to the column span of $\mathbf{F}$.

Equation (5.15) describes an integer least squares problem. We use an approach where the integer least squares problem is viewed as a closest point search in the lattice generated by $\mathbf{B}$. First, the estimate of the unwrapping vector $\hat{\mathbf{u}}$ is determined by finding the closest lattice point $\mathbf{B}\hat{\mathbf{u}}$ to the query point $\mathbf{B}\tilde{\boldsymbol{\theta}}$, i.e., $\mathbf{B}\hat{\mathbf{u}} = \mathrm{CPt}\{\mathbf{B}\tilde{\boldsymbol{\theta}}, \mathcal{L}\}$. By inserting the unwrapping vector $\hat{\mathbf{u}}$ back into (5.14), we obtain an estimated parameter vector according to

$$\hat{\mathbf{p}} = \mathbf{F}^{\#}(\tilde{\boldsymbol{\theta}} - \hat{\mathbf{u}}). \tag{5.16}$$

5.2 Identifiability of Fourier Based Phase Parameters

The effect of aliasing, i.e., distinct parameter sets lead to the same signal samples, occurs when uniformly samples of a polynomial phase signal are taken. This has been treated in Section 3.2. In this section we investigate the identifiability of uniformly sampled Fourier-based signals.

Let $s[n]$ denote a noiseless, uniformly sampled Fourier-based phase signal, that is

$$s[n] = e^{j2\pi\psi[n]}, \quad \text{with} \quad \psi[n] = \sum_{k=0}^{m} f_k[n]p_k. \tag{5.17}$$

In vector notation, $\mathbf{s} = (s[1] \dots s[N])^T$ is the vector of signal samples and $\mathbf{p} = (p_0 \dots p_m)^T$ the parameter vector. Aliasing means that several parameter vectors $\mathbf{p}$ are mapped to the same signal sample values $\mathbf{s}$.

We assume the following: $\mathbf{p}$ and $\tilde{\mathbf{p}} = \mathbf{p} + \mathbf{d}$ are distinct parameter vectors which both have the same signal samples $\mathbf{s}$, that is

$$\begin{aligned} s[n] &= \exp\left(j2\pi \sum_{k=0}^{m} f_k[n]p_k\right) \\ &= \exp\left(j2\pi \sum_{k=0}^{m} f_k[n](p_k + d_k)\right) \\ &= \exp\left(j2\pi \sum_{k=0}^{m} f_k[n]p_k\right) \exp\left(j2\pi \sum_{k=0}^{m} f_k[n]d_k\right), \end{aligned} \tag{5.18}$$

and therefore

$$\exp\left(j2\pi \sum_{k=0}^{m} f_k[n]d_k\right) = 1. \tag{5.19}$$

As a consequence, the ambiguity between $\mathbf{p}$ and $\tilde{\mathbf{p}}$ occurs if and only if

$$\sum_{k=0}^{m} f_k[n]d_k \in \mathbb{Z}. \tag{5.20}$$

In (5.8) we see that the first column $\mathbf{f}_0$ is the only one consisting exclusively of integer elements. Therefore, solely the parameter vector

$$\mathbf{d} = \begin{pmatrix} d_0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \text{with} \quad d_0 \in \mathbb{Z}, \tag{5.21}$$

leads to an ambiguity between $\mathbf{p}$ and $\tilde{\mathbf{p}}$. The additive parameter vector $\mathbf{d}$ of (5.21) corresponds to a shift of all signal samples by a multiple of 2π. Therefore, the aliasing only appears in the constant phase component. However, this does not need to be resolved because the wrapping operation always restricts the initial phase to lie in $[-1/2, 1/2)$.

5.3 Simulations

In this section we present Monte Carlo simulations of the angular least squares estimator introduced in Section 5.1. Due to the structure of $\mathbf{B}$ the closest point problem $\mathbf{B}\hat{\mathbf{u}} = \mathrm{CPt}\{\mathbf{B}\tilde{\boldsymbol{\theta}}, \mathcal{L}\}$ can't be exactly solved using the approach from Section 3.4. As in the nonuniform case we use a suboptimal ad hoc approach:

- The first $m+1$ columns of the lattice generated by $\mathbf{B} = \mathbf{I} - \mathbf{F}\mathbf{F}^{\#}$ are dropped. The new basis matrix is denoted by $\mathbf{B}_{N-m-1}$.
- The LLL algorithm (Algorithm 1) with parameter $\delta = 3/4$ is applied to the lattice with basis $\mathbf{B}_{N-m-1}$; the reduced basis is denoted by $\tilde{\mathbf{B}}_{\mathrm{red}}$.
- The closest lattice point problem in the lattice with the generator $\tilde{\mathbf{B}}_{\mathrm{red}}$ reads as

$$\tilde{\mathbf{B}}_{\mathrm{red}}\hat{\mathbf{u}}_{\mathrm{red}} = \mathrm{CPt}\{\mathbf{B}_{N-m-1}\tilde{\boldsymbol{\theta}}_{N-m-1}, \tilde{\mathbf{B}}_{\mathrm{red}}\mathbb{Z}^m\}. \tag{5.22}$$

  We use Babai's nearest plane algorithm (Algorithm 2) to obtain an approximate solution to the closest point problem (5.22). Note that the "observation" is determined by $\tilde{\boldsymbol{\theta}}_{N-m-1}$, which is obtained by dropping the first $m+1$ entries of $\tilde{\boldsymbol{\theta}}$.

- The result is transformed back to the original domain according to $\hat{\mathbf{u}}_{N-m-1} = \mathbf{T}\hat{\mathbf{u}}_{\mathrm{red}}$, where $\mathbf{T}$ is the unimodular transformation matrix derived by the LLL algorithm.

The parameter estimates are calculated according to

$$\hat{\mathbf{p}} = \mathbf{F}^{\#}_{N-m-1}(\tilde{\boldsymbol{\theta}}_{N-m-1} - \hat{\mathbf{u}}_{N-m-1}), \tag{5.23}$$

where $\mathbf{F}_{N-m-1}$ is obtained by dropping the first $m+1$ rows of $\mathbf{F}$. There is no zero padding of the unwrapping vector. In the simulations a Fourier-based phase signal of order $m=3$ is assumed. The noise term w_n is complex Gaussian with independent real and imaginary parts having variance σ_c^2. The MSE of the estimator is computed after 2500 trials for each value of SNR $= 1/2\sigma_c^2$ in the range $[0\text{dB}, 20\text{dB}]$. The MSE for each parameter p_k is calculated by averaging $(p_k - \hat{p}_k)^2$.

In Figure 5.2 the true parameters p_k are randomly chosen from $[0, 0.5)$. We can see that the estimator works quite good above an SNR of 15dB with $N=50$ and $N=60$. Somewhat surprising is that for $N=55$ our estimator doesn't work properly. Figure 5.3 shows the same behavior. Here, the true parameters p_k are randomly chosen from $[0, 0.8)$. In the simulations the calculation of the MSE is a crucial point. If Babai's algorithm is not delivering the closest lattice point, the unwrapping vector can get large due to the transformation with the unimodular matrix $\mathbf{T}$. This can lead to large differences between the parameter estimates and the true parameters. In the case of uniformly sampled polynomial phase estimation we have faced large differences between true and estimated parameters as well but there it has been caused by the aliasing effect.

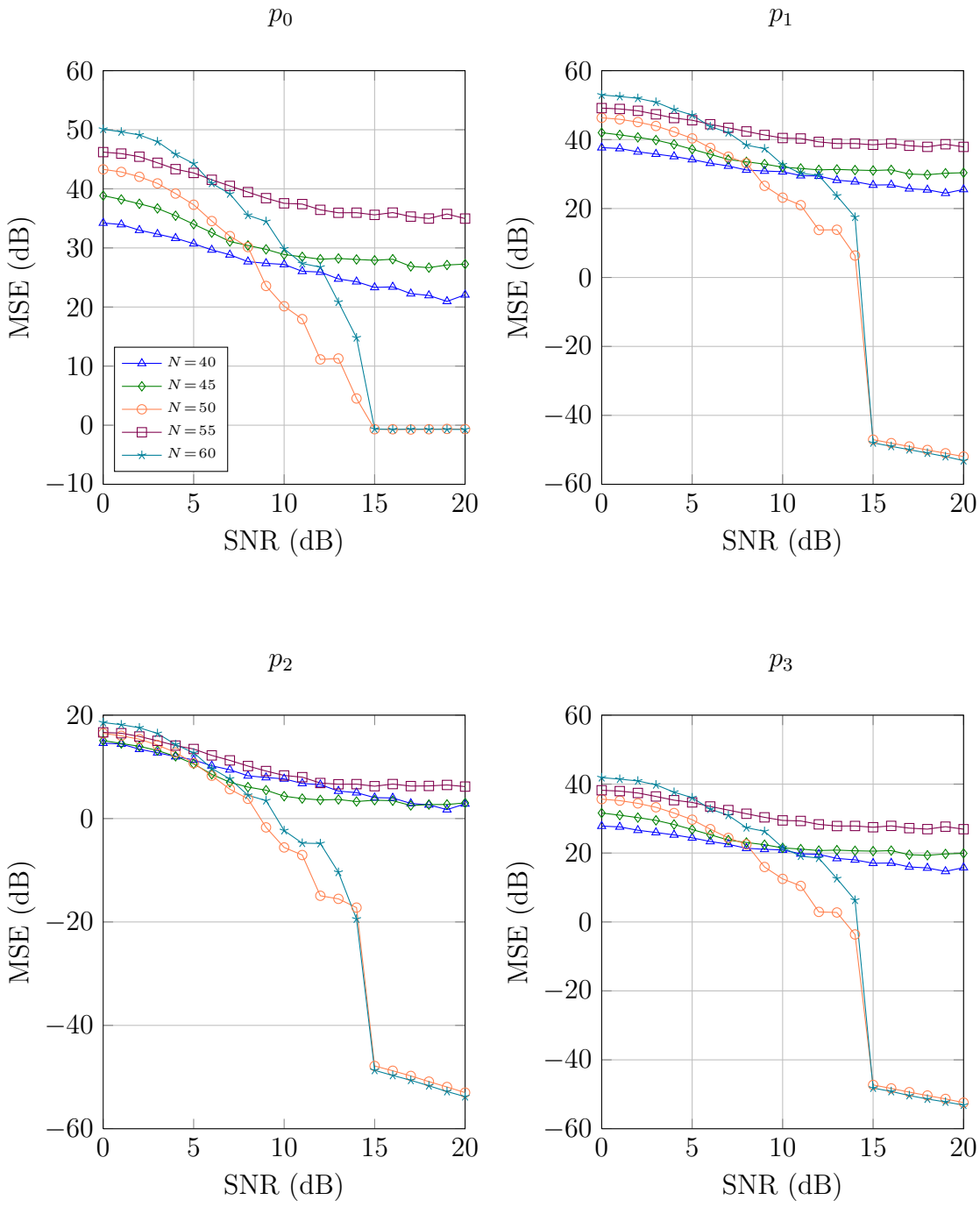

Figure 5.2: *Mean square error for each of the four parameters with p_k randomly taken from $[0, 0.5)$.*

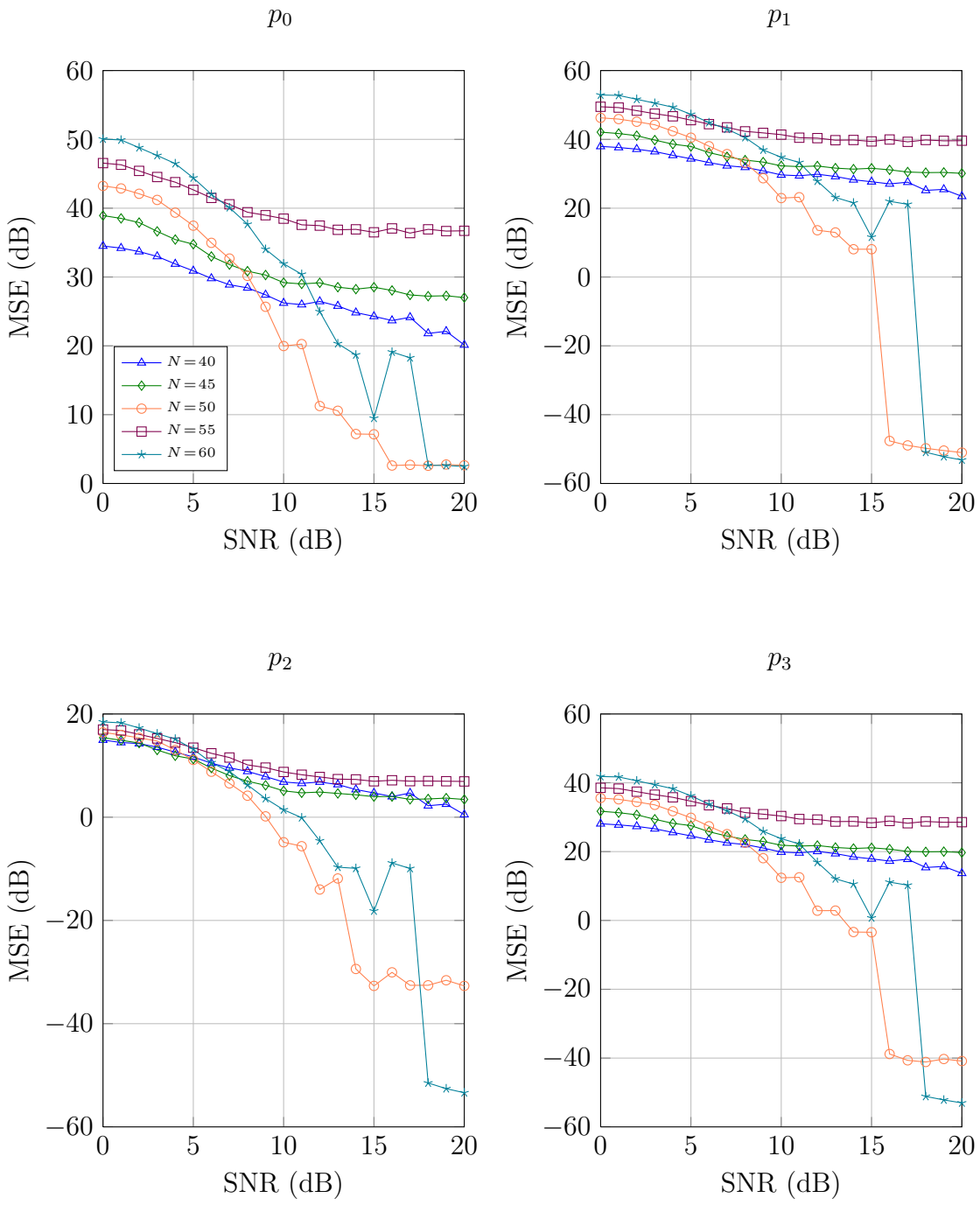

Figure 5.3: *Mean square error for each of the four parameters with p_k randomly taken from $[0, 0.8)$.*

6

Summary and Outlook

In this thesis, we have presented a method to estimate phase signals by using concepts of lattice theory. First we have introduced some basics about lattices including the description in terms of a nonunique basis matrix, the Voronoi region, the fundamental parallelotope, and the orthogonality defect. In lattice theory a fundamental problem is to find the closest lattice point to a given point. We have presented Babai's nearest plane algorithm, which is a fast algorithm that gives an approximate solution to the closest point problem. In order for Babai's nearest plane algorithm to perform well, the lattice needs to be described by a basis matrix with short and fairly orthogonal vectors. Lattice reduction algorithms obtain a reduced basis matrix with aforementioned properties. As an example, we have discussed the LLL algorithm, which is of polynomial average complexity and therefore often used.

Then we have presented an estimator for uniformly sampled polynomial phase signals. This estimator performs phase unwrapping in a least squares manner. The so obtained integer least squares problem has been cast into a closest lattice point problem which has been solved by aforementioned techniques. The effect of aliasing has been described and furthermore resolved by concepts of lattice theory. Some simulation results have been presented wherein it could be seen that the estimator performs well

in high SNR (signal to noise ratio) scenarios. Furthermore it could be seen that the estimator performs uniformly well over the entire aliasing-free region.

We have applied the angular least squares estimator to a nonuniformly sampled polynomial phase signal. This had been motivated by the fact that we avoid aliasing by nonuniformly sampling with irrational spaced sampling instants. Again this has led to an integer least squares problem. For solving this problem, we have used the closest lattice point search as an ad hoc approach. It has yet to be shown theoretically that the closest lattice point search solves the pertinent integer least squares problem. The simulation results suggests that this could be possible.

Finally we have estimated a uniformly sampled Fourier-based phase signal with the above-mentioned approach. As in the previous scenario, we have used the closest point search without proof that this solves the integer least squares problem. We have seen in the simulation results that for some parameter sets the estimator works well at sufficiently high SNR values.

Several problems are left for future research:
The central remaining question is: under what conditions can the integer least squares problem be viewed as a closest lattice point problem? One condition could be that the entries of the basis describing the phase (here we have denoted them $\mathbf{X}, \mathbf{L}$, and $\mathbf{F}$) need to be integer. This also allows for rational entries of the basis vector by an appropriate rescaling of the parameters. For basis with irrational elements such as the Fourier basis $\mathbf{F}$, the closest lattice point search would fail to provide a meaningful solution. It is probably possible to approximate irrational values by rational ones with little loss in practical performance. Furthermore, it could be useful to set a rational grid where the sampling points can lie on and change the sampling pattern time dependent.

The LLL algorithm could be preceded by a sorted QR-decomposition [24]. This should dramatically decrease the computational complexity of the LLL algorithm.

Bibliography

[1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. New York, USA: Springer, 3rd ed., 1998.

[2] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. on Information Theory*, vol. 48, pp. 2201–2214, Aug. 2002.

[3] L. Babai, "On Lovász lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1–13, 1986.

[4] R. G. McKilliam, *Lattice theory, circular statistics and polynomial phase signals*. PhD thesis, University of Queensland, Australia, Dec. 2010.

[5] H. Minkowski, *Geometrie der Zahlen*. Leipzig, Germany: Teubner Verlag, 1896.

[6] C. Hermite, "Extraits de lettres de M. Ch. Hermite á M. Jacobi sur différents objects de la théorie des nombres," *Journal für die reine und angewandte Mathematik*, vol. 40, pp. 279–290, 1850.

[7] A. Korkine and G. Zolotareff, "Sur les formes quadratiques," *Mathematische Annalen*, vol. 6, pp. 366–389, 1873.

[8] C. F. Gauss, *Untersuchungen über höhere Arithmetik, (Disquisitiones Arithmeticae)*. Berlin, Germany: Springer, 1889.

[9] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, pp. 515–534, 1982.

[10] M. Seysen, "Simultaneous reduction of a lattice basis and its reciprocal basis," *Combinatorica*, vol. 13, pp. 363–376, 1993.

[11] D. Wübben, D. Seethaler, J. Jaldén, and G. Matz, "Lattice reduction," *IEEE Signal Processing Magazine*, vol. 28, pp. 70–91, May 2011.

[12] D. Wübben, R. Böhnke, V. Kühn, and K. D. Kammeyer, "Near-maximum-likelihood detection of MIMO systems using MMSE-based lattice reduction," in *Proc. IEEE Int. Conf. on Communications (ICC)*, vol. 2, (Paris, France), pp. 798–802, June 2004.

[13] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, "A vector-perturbation technique for near-capacity multiantenna multiuser communication - Part I: Channel inversion and regularization," *IEEE Trans. on Communications*, vol. 53, pp. 195–202, Jan. 2005.

[14] A. Hassibi and S. Boyd, "Integer parameter estimation in linear models with applications to GPS," *IEEE Trans. on Signal Processing*, vol. 46, pp. 2938–2952, Nov. 1998.

[15] M. Ajtai, "The shortest vector problem in L_2 is NP-hard for randomized reductions," in *Proc. of the 30th annual ACM symposium on theory of computing*, (Dallas, TX, USA), May 1998.

[16] E. Viterbo and J. J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. on Information Theory*, vol. 45, pp. 1639–1642, July 1999.

[17] S. Galbraith, "Mathematics of public key cryptography." http://www.math.auckland.ac.nz/∼sgal018/crypto-book/crypto-book.html, June 2011.

[18] I. V. L. Clarkson, "Frequency estimation, phase unwrapping and the nearest lattice point problem," in *Proc. IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, (Phoenix, AZ, USA), Mar. 1999.

[19] J. Ängeby, "Aliasing of polynomial-phase signal parameters," *IEEE Trans. on Signal Processing*, vol. 48, pp. 1488–1491, May 2000.

[20] R. G. McKilliam and I. V. L. Clarkson, "Identifiability and aliasing in polynomial-phase signals," *IEEE Trans. on Signal Processing*, vol. 57, pp. 4554–4557, Nov. 2009.

[21] S. Peleg and B. Porat, "The Cramer-Rao lower bound for signals with constant amplitude and polynomial phase," *IEEE Trans. on Signal Processing*, vol. 39, pp. 749–752, Mar. 1991.

[22] B. Quinn, "Estimating the mode of a phase distribution," in *Proc. IEEE Asilomar Conference on Signals, Systems and Computers*, (Pacific Grove, CA, USA), pp. 587–591, Nov. 2007.

[23] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*. Springer, 2nd ed., May 1997.

[24] D. Wübben, R. Böhnke, V. Kühn, and K. D. Kammeyer, "MMSE extension of V-BLAST based on sorted QR decomposition," in *Proc. IEEE Vehicular Technology Conference (VTC)*, (Orlando, FL, USA), Oct. 2003.