Lattice Codes and Sphere Decoding

Pasi Pyrrö

School of Science

Bachelor's special assignment
Espoo 10.7.2017

Thesis supervisor:

Prof. Camilla Hollanti

Thesis advisors:

Prof. Marcus Greferath

D.Sc. Oliver Gnilke

Aalto University
School of Science

Author: Pasi Pyrrö

Title: Lattice Codes and Sphere Decoding

Date: 10.7.2017 Language: English Number of pages: 4+9

Degree programme: Mathematics and Systems Analysis

Supervisor: Prof. Camilla Hollanti

Advisors: Prof. Marcus Greferath, D.Sc. Oliver Gnilke

Keywords: sphere decoding, space–time lattice codes, wireless communications

Contents

Symbols and abbreviations

Symbols

$\mathbb{Z}$	Set of integers
$\mathbb{C}$	Field of complex numbers
$\mathbf{x}$	Vector
$\mathbf{X}$	Matrix

Operators

$\|\cdot\|$	Euclidean norm
$\det(\mathbf{X})$	Determinant of matrix $\mathbf{X}$

Abbreviations

SNR	Signal to noise ratio
CVP	Closest vector problem

1 Introduction

Wireless communication has been a crucial part of modern information technology for a couple of decades now. It is facing a lot of practical everyday problems which motivate the ongoing extensive research on the field. One of these problems is the noise and fading that occurs on wireless channels due to obstacles and radiation from the surroundings. To avoid data loss during transmission via wireless link one has to encode the data to be sent in such a robust way that it can still be recovered at the receiving end even in the presence of noise and fading of reasonable scale.

One way to tackle this problem, and the method this thesis focuses on, is the use of space–time lattice codes and sphere decoding. From a mathematical point of view the process of decoding can then be viewed as a problem of finding the closest lattice point to a given input vector, that is, the possibly noisy vector containing the data we receive from the wireless channel. This problem in its general form is known to be NP-hard but for communications applications, where the dimensionality and lattice shape are kept reasonable, there exist algorithms, like the sphere decoder, that offer polynomial expected complexity [1].

2 Lattices in communications technology

Before we go into communications applications of lattices such as lattice codes, let us start off with the definition of a lattice. Let n and m be positive integers such that $n \leq m$ and $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{R}^m$ be linearly independent vectors. A subset Λ of $\mathbb{R}^m$ is called a lattice of dimension n if it is defined as

$$\Lambda = \sum_{i=1}^{n} \mathbb{Z}\mathbf{b}_i = \{a_1\mathbf{b}_1 + ... + a_n\mathbf{b}_n | a_i \in \mathbb{Z}, 1 \leq i \leq n\} \tag{1}$$

where the set of vectors $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{R}^m$ is called the basis of the lattice Λ. All points of the lattice can be obtained as a linear combination of the basis vectors $\mathbf{b}_i$ and integer coefficients $\mathbf{a}_i$ as stated in (1). The number of basis vectors n is also called the rank of the lattice and if $n = m$ the lattice is said to have full rank. The points of the lattice Λ form a group under addition which means that if $\mathbf{x} \in \Lambda$ then $-\mathbf{x} \in \Lambda$ and if $\mathbf{x}, \mathbf{y} \in \Lambda$ then $\mathbf{x} \pm \mathbf{y} \in \Lambda$. [2]

There is also a matrix representation for the same lattice

$$\Lambda = \{\mathbf{x} | \mathbf{x} = \mathbf{B}\mathbf{a}\} \tag{2}$$

where $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n]$ is an $m \times n$ matrix called the generator matrix of the lattice Λ and $\mathbf{a}$ is an n-dimensional integer column vector. Note that $\mathbf{B}$ is not uniquely determined by the lattice as in fact there exists infinitely many bases for the same lattice [2]. If $\mathbf{B}$ is a basis for lattice Λ then $\mathbf{B}'$ is also a basis for the same lattice if the following holds

$$\mathbf{B}' = \mathbf{W}\mathbf{B}, \tag{3}$$
$$\det(\mathbf{W}) = \pm 1 \tag{4}$$

where $\mathbf{W}$ is an $m \times m$ matrix with integer entries [3]. Some bases are however better in some sense than others, especially in communications applications, as one could imagine. Usually reasonable orthogonality and relatively small norm for the basis vectors are desired [3]. A better basis can be obtained via a process called basis reduction, which is illustrated in figure 1. Clearly basis vectors $\mathbf{u}_i$ obtained from the basis reduction are more pleasant to work with than the original vectors $\mathbf{v}_i$ although they both span the same lattice.

What we considered earlier were lattices spanned over real m-dimensional space $\mathbb{R}^m$ but in similar sense we can consider a lattice consisting of complex valued vectors from $\mathbb{C}^m$. The principles of such complex lattice are almost the same, however, now $\mathbf{B}$ and $\mathbf{a}$ take values from $\mathbb{C}$. Note that a complex lattice has an equivalent real representation which has double the rank of the corresponding complex lattice. Consider a lattice $\Lambda \subset \mathbb{C}^m$ with a generator matrix $\mathbf{B} = [\mathbf{z}_1, ..., \mathbf{z}_n]$. Now we can always express it with a real valued lattice $\Lambda_{\text{real}} \subset \mathbb{R}^{2m}$ and the corresponding $2m \times n$ generator matrix is given by

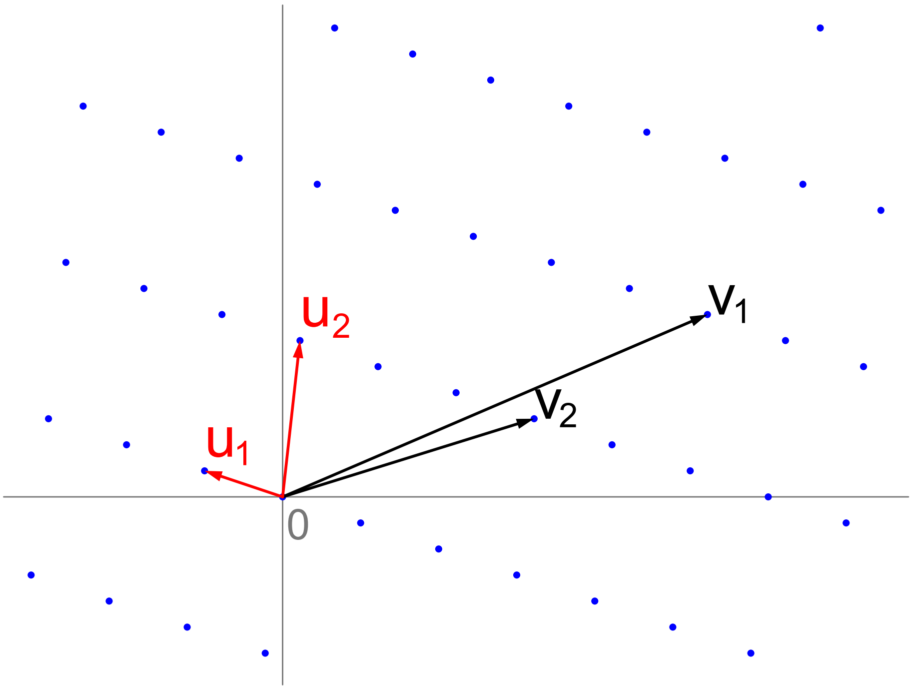

Figure 1: Two different bases for the same two dimensional lattice.

$$\mathbf{B}_{\text{real}} = \begin{bmatrix} \text{Re}(z_{11}) & \dots & \text{Re}(z_{1n}) \\ \text{Im}(z_{11}) & \dots & \text{Im}(z_{1n}) \\ \vdots & \ddots & \vdots \\ \text{Re}(z_{m1}) & \dots & \text{Re}(z_{mn}) \\ \text{Im}(z_{m1}) & \dots & \text{Im}(z_{mn}) \end{bmatrix}. \tag{5}$$

In other words we convert each column of $\mathbf{B}$ to real vector by separating each of their complex elements into two adjacent real elements, that is the real and imaginary parts of the original complex element. This process doubles the amount of rows in $\mathbf{B}_{\text{real}}$ but both representations ultimately describe the same lattice. [4]

2.1 Closest vector problem

One relevant mathematical problem related to sphere decoding, a communications application of interest in this paper, is the closest vector problem (CVP). Given a lattice Λ and an input point $\mathbf{y}$ the problem is to find a lattice point $\hat{\mathbf{x}} \in \Lambda$ that is closest to $\mathbf{y}$. More precisely $\hat{\mathbf{x}} \in \Lambda$ has to meet the following condition

$$\|\mathbf{y} - \hat{\mathbf{x}}\| \leq \|\mathbf{y} - \mathbf{x}\|, \quad \forall \mathbf{x} \in \Lambda. \tag{6}$$

For a fixed point $\hat{\mathbf{x}} \in \Lambda$ the set of vectors $\mathbf{y}_i$ that satisfy the confition (6) is called the Voronoi region of lattice point $\hat{\mathbf{x}}$, $\mathcal{V}_{\hat{\mathbf{x}}}$. This means that if $\mathbf{y} \in \mathcal{V}_{\hat{\mathbf{x}}}$ then the solution to CVP is $\hat{\mathbf{x}}$. The volume of the $\mathcal{V}_{\hat{\mathbf{x}}}$ is given by $\det(\Lambda) = \sqrt{\det(\mathbf{B}^T\mathbf{B})}$, where $\mathbf{B}$ is the generator matrix of Λ.

2.2 Space–time lattice codes

3 Sphere decoder

4 Simulations and results

5 Summary

References

[1] Mäki, M. *Space-time block codes and the complexity of sphere decoding.* Doria, Referenced 10.7.2017. Available: https://www.doria.fi/bitstream/handle/10024/54404/gradu2008maki-miia.pdf

[2] Cassels, J.W.S. *An introduction to the Geometry of Numbers*, New York, Springer–Verlag, 1971.

[3] Agrell, E., Eriksson, T. and Zeger, K. *Closest point search in lattices* IEEE Transactions on Information Theory, Vol. 48, pp.2201-2214, August 2002.

[4] Conway, J.H. and Sloane, N.J.A. *Sphere packings, lattices and groups.* Third edition, New York, Springer–Verlag, 1998.