

# Probability Distribution of Gram-Schmidt Coefficients after LLL-Reduction

Frank Hartmann

Department of Computer Science  
Cryptography and Computeralgebra  
Technische Universität Darmstadt

A thesis submitted for the degree of  
*Bachelor of Science*

23<sup>rd</sup> of September, 2010

Supervised by: Prof. Dr. Johannes Buchmann  
Michael Schneider

## Abstract

The security of lattice-based cryptosystems is based on mathematical problems which are hard to solve, unless one has some additional information. Short and nearly orthogonal basis vectors computed by basis reduction algorithms represent the kind of special information that make some hard mathematical lattice problems easy to compute. The most famous algorithm for reducing lattice bases is the so-called LLL algorithm by Lenstra, Lenstra, and Lovász, which outputs short vectors with size exponential in the lattice dimension [LLL82]. (Un)fortunately this algorithm finds far shorter vectors in practice than the latest theoretical bounds predict for the worst case. The estimation of these bounds is a crucial question for today's security assumptions. In the meantime, some ideas have come up in the challenge of finding average case bounds which significantly meet the practical results. In this paper, we will follow the idea from Schneider et al. [SLB09] where the Gram-Schmidt coefficients are assumed to be randomly distributed in a certain manner. We will give a theoretical analysis of the probabilistic behaviour of the Gram-Schmidt coefficients in a certain model.

## **Acknowledgements**

First, and foremost, I would like to thank Prof. Dr. Johannes Buchmann for giving me the opportunity to write this thesis.

I am deeply grateful to my direct supervisor, Michael Schneider, for his detailed and constructive remarks, and for all his help and support throughout my work.

Last but not least I thank my beloved parents who made this possible.

## **Declaration of authorship**

I herewith declare that I have produced this paper without the prohibited assistance of third parties and without making use of aids other than those specified; notions taken over directly or indirectly from other sources have been identified as such. This paper has not previously been presented in identical or similar form to any other German or foreign examination board.

The thesis work was conducted from July 2010 to September 2010 under the supervision of Prof. Dr. Johannes Buchmann at Technische Universität Darmstadt.

Darmstadt,

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Preliminaries</b>	<b>2</b>
2.1	$\mathbb{R}^n$ and lattices . . . . .	2
2.1.1	Scalar product in $\mathbb{R}^n$ . . . . .	2
2.1.2	Euclidean norm . . . . .	2
2.1.3	Gram-Schmidt orthogonalization (GSO) . . . . .	2
2.2	LLL . . . . .	3
2.2.1	$\delta$ -LLL reduced bases . . . . .	3
2.2.2	The LLL-algorithm . . . . .	3
2.3	Theory of probabilities . . . . .	4
2.3.1	Density functions . . . . .	4
<b>3</b>	<b>Redefined fundamental operations</b>	<b>6</b>
3.1	Distribution of linear transformations . . . . .	6
3.2	Distribution of sums . . . . .	6
3.3	Distribution of quotients . . . . .	7
3.4	Distribution of products . . . . .	8
3.5	Distribution of squares . . . . .	8
3.6	Scalar products revisited . . . . .	9
<b>4</b>	<b>Probability analysis of randomly distributed variables</b>	<b>10</b>
4.1	Selecting the parameters . . . . .	10
4.2	Probability distribution of the initial GSO . . . . .	11
4.3	Probability distribution after SIZE-REDUCE . . . . .	12
4.4	Probability distribution after SWAP . . . . .	12
4.4.1	Probability distribution of $\hat{\mu}_{k,k-1}$ . . . . .	12
4.4.2	Probability distribution of $\hat{\mu}_{j,k-1}$ for all $j \geq k + 1$ . . . . .	17
4.4.3	Probability distribution of $\hat{\mu}_{j,k}$ for all $j \geq k + 1$ . . . . .	21
<b>5</b>	<b>Further Work</b>	<b>22</b>
	<b>References</b>	<b>23</b>

# 1 Introduction

The security of lattice-based cryptosystems is based on mathematical problems which are hard to solve, unless one has some additional information. Short and nearly orthogonal basis vectors computed by basis reduction algorithms represent the kind of special information that make some hard mathematical lattice problems easy to compute. More precisely, the search for short vectors in lattices, especially finding the shortest vector, is assumed to be a hard problem and becomes an easy computational task with the knowledge of short vectors in that particular lattice.

A successful and efficient algorithm that works for higher dimensions was introduced by Arjen Lenstra, Hendrik Lenstra, and László Lovász in 1982 [LLL82]. This famous algorithm was named after its authors and is called the LLL-algorithm.

Where the output of the LLL-algorithm is an approximation of the shortest lattice vectors, the estimation of the bounds of these shortest lattice vectors is a crucial question for today's security assumptions. Concerning the shortest vector's length, there are worst-case bounds which are tight and cannot be improved [NS05], as well as theoretical average-case bounds which predict a realistic assertion in practice [SLB09],[NS05].

Some ideas have come up in the challenge of finding average case bounds which significantly satisfy the practical results.

In this paper, we will follow the idea from Schneider et al. [SLB09] where the Gram-Schmidt coefficients are assumed to be randomly distributed in a certain manner. Essentially, the main characteristic calculations of the LLL-algorithm are performed on the Gram-Schmidt coefficients, which represent the orthogonal projection and degree of reducedness during the LLL-reduction. In [SLB09], a probabilistic analysis of the Gram-Schmidt coefficients yield an expectation of the length of the shortest vector. Instead of performing and analyzing experiments on lattice reduction scenarios, we will give a theoretical analysis of the probabilistic behaviour of the Gram-Schmidt coefficients in a certain model.

This paper begins with an introduction to the mathematical basics which will be used throughout this paper. This section intends to give the definitions of the operations and algorithms, which are then analyzed from a probabilistic point of view.

The next section states all the probabilistic density functions of random variables being a mathematical combination of two or more randomly distributed variables. These generic density functions will be adopted in our probabilistic analysis of the operations taking place in the LLL-algorithm.

The actual probabilistic analysis is then performed in Section 4.

At first, we select the vectorial basis on which these calculations are performed, then the initial distribution of the Gram-Schmidt coefficients and the projected vectors are computed. Finally, we give the probabilistic distribution of the Gram-Schmidt coefficients after they were touched by the SIZE-REDUCE-algorithm and the SWAP-algorithm.

## 2 Preliminaries

This section gives an introduction to basic mathematical definitions of lattices and probability theory which will be used in the following sections.

Generally, all indices  $i$  of a variable  $x$  or a vector  $\mathbf{x}$  are defined, such that  $i > 0$  with  $i \in \mathbb{N}$ .

### 2.1 $\mathbb{R}^n$ and lattices

A lattice  $\mathcal{L}$  in  $\mathbb{R}^n$  is a discrete additive subgroup of  $\mathbb{R}^n$  which spans the real euclidean vector space  $\mathbb{R}$  of dimension  $n \in \mathbb{N}$  in case its basis has full rank. Typically a full-rank lattice is described as

$$\mathcal{L}(\mathbf{B}) := \left\{ \sum_{i=1}^n a_i \mathbf{v}_i \mid a_i \in \mathbb{Z} \wedge \mathbf{v}_i \in \mathbf{B} \right\}.$$

$\mathbf{B}$  represents the basis of the lattice  $\mathcal{L}$  and is defined as the matrix  $\mathbf{B} := [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{n-1}, \mathbf{b}_n]^T$  with  $\mathbf{b}_i \in \mathbb{R}^n$  being linear independent row vectors.

A more detailed definition of lattices can be found in [Sch06]

#### 2.1.1 Scalar product in $\mathbb{R}^n$

The scalar product or inner product of the  $n$ -dimensional real vector space  $\mathbb{R}^n$  of two vectors  $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$  with  $\mathbf{a} = (a_1, a_2, \dots, a_{n-1}, a_n)$  and  $\mathbf{b} = (b_1, b_2, \dots, b_{n-1}, b_n)$  is a symmetric and positive definite, bilinear form and defined as  $\langle \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \mapsto \mathbb{R}$  with

$$\langle \mathbf{a} \cdot \mathbf{b} \rangle := \sum_{i=1}^n a_i b_i.$$

#### 2.1.2 Euclidean norm

A norm on  $\mathbb{R}^n$  is a function  $\|\cdot\| : \mathbb{R}^n \mapsto \mathbb{R}$  that assigns a strictly positive length to all vectors in a vector space.

The most commonly used norm on  $\mathbb{R}^n$  is the so called euclidean norm which describes an intuitive notion of the length of a vector  $\mathbf{a}$ , such that

$$\|\mathbf{a}\| := \sqrt{a_1^2 + \dots + a_n^2} = \sqrt{\langle \mathbf{a} \cdot \mathbf{a} \rangle}.$$

#### 2.1.3 Gram-Schmidt orthogonalization (GSO)

A Gram-Schmidt-orthogonalized basis  $\mathbf{B}^*$  of  $\mathbf{B}$  is defined as the matrix  $\mathbf{B}^* = [\mathbf{b}_1^*, \mathbf{b}_2^*, \dots, \mathbf{b}_{n-1}^*, \mathbf{b}_n^*]^T$  with the components  $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{k=1}^{i-1} \mu_{i,k} \mathbf{b}_k^*$  and the Gram-Schmidt coefficients  $\mu_{i,j} = \frac{r_{i,j}}{r_{j,j}}$ ,  $r_{i,j} = \langle \mathbf{b}_i \cdot \mathbf{b}_j^* \rangle$ ,  $r_{j,j} = \langle \mathbf{b}_j^* \cdot \mathbf{b}_j^* \rangle$  with  $\mathbf{b}_i \in \mathbf{B}$  and all  $j \leq i$ . The pairwise orthogonal vectors  $\mathbf{b}_i^* \in \mathbf{B}^*$  span the same  $n$ -dimensional subspace of  $\mathbb{R}^n$  as the vectors  $\mathbf{b}_i \in \mathbf{B}$ .

The Gram-Schmidt coefficients  $\mu_{i,j}$  can be calculated from the lower triangular matrix  $\mathbf{R}$  which can be viewed as:

$$\mathbf{R} := \begin{pmatrix} r_{1,1} & 0 & 0 & \cdots & 0 \\ r_{2,1} & r_{2,2} & 0 & \cdots & 0 \\ r_{3,1} & r_{3,2} & r_{3,3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ r_{n,1} & r_{n,2} & r_{n,3} & \cdots & r_{n,n} \end{pmatrix}$$

## 2.2 LLL

The LLL-Algorithm computes a reduced lattice basis in a time polynomial in the lattice dimension and is named after its creators Arjen Lenstra, Hendrik Lenstra, and László Lovász. The final version of the algorithm is presented in [LLL82].

Given an input basis  $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_n]^T$  for a lattice  $\mathcal{L}$  in  $\mathbb{R}^n$ , the LLL algorithm outputs a LLL-reduced lattice basis whose vectors are short and nearly orthogonal. First we give a short description of the mathematical meaning of LLL-reduced bases, then parts of the LLL-algorithm are presented, which are examined in following sections.

### 2.2.1 $\delta$ -LLL reduced bases

A basis  $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]^T$  is called  $\delta$ -LLL reduced with  $\delta \in (\frac{1}{4}; 1]$  if

$$\begin{aligned} |\mu_{i,j}| &\leq 0.5 && \text{for } 1 \leq j < i \leq n \\ \|\mathbf{b}_i^*\|^2 &\leq \frac{\|\mathbf{b}_{i+1}^*\|^2}{(\delta - \mu_{i+1,i})} && \text{for } i = 1, \dots, n. \end{aligned}$$

Bases which satisfy the first property are called size-reduced.  $\delta$  represents the quality of the reduction. The bigger  $\delta$ , the more the bases are reduced.

The latter condition is called the Lovász-condition. Note that this condition only relies on the Gram-Schmidt coefficient on the subdiagonal of the Gram-Schmidt matrix.

### 2.2.2 The LLL-algorithm

A complete definition of the algorithm can be found in [Sch06] or [LLL82]. For this work, the main interesting parts of the algorithm are the size reduction operation and the swap operation performed on the vectors of the input basis.

Unless otherwise stated, the parameter  $k$  stands for the current step of the LLL-algorithm in this paper.

**Swap algorithm: SWAP** In case the orthogonal projected vectors  $\mathbf{b}_k^*$  and  $\mathbf{b}_{k-1}^*$  of the basis vectors  $\mathbf{b}_k, \mathbf{b}_{k-1} \in \mathbf{B}$  violate the Lovász-condition, the vectors  $\mathbf{b}_k$  and  $\mathbf{b}_{k-1}$  are swapped.

The exchange of the two basis vectors leads to several new computations performed on the Gram-Schmidt-matrix  $\boldsymbol{\mu}$ .

The values of  $\mu_{k,i}$  and  $\mu_{k-1,i}$  are swapped with  $1 \leq i \leq k-2$  according to Algorithm 2.  $\mu_{k,k-1}$  on the subdiagonal, as well as all  $\mu_{j,k-1}$  and all  $\mu_{j,k}$  with  $k+1 \leq j \leq n$  have to be recomputed according to Algorithm 3, 4 and 5.

All variables  $x$  denoted like  $\hat{x}$  are the output of the following algorithms, emphasizing its recomputation.

**Size reduction algorithm: SIZE-REDUCE** The reduction of the basis vectors is performed by the following Algorithm 1 as a part of the LLL-algorithm.

---

**Algorithm 1:** SIZE-REDUCE. Size-reduction of  $\mathbf{b}_k$  and update of the Gram-Schmidt coefficients

---

**Input:** Lattice basis  $\mathbf{B}_k = [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_k]$  with  $\mathbf{B}_k \subset \mathbf{B}$ , the vector  $\boldsymbol{\mu}_k = [\mu_{k,1}, \mu_{k,2}, \dots, \mu_{k,k-1}]$ ,  $k \leq n$

**Output:** size-reduced  $\mathbf{b}_k$  such that  $\|\mathbf{b}_k\|^2 \leq \max(\|\mathbf{b}_1\|^2, \dots, \|\mathbf{b}_n\|^2)$  and the updated Gram-Schmidt coefficients  $\boldsymbol{\mu}_k$

```

for  $j = k - 1, \dots, 1$  do
     $\mathbf{b}_k := \mathbf{b}_k - \lfloor \mu_{k,j} \rfloor \mathbf{b}_j$ 
    for  $i = 1, \dots, j$  do
         $\mu_{k,i} := \mu_{k,i} - \lfloor \mu_{k,j} \rfloor \mu_{j,i}$ 

```

---

For more details on the bounds of  $\|\mathbf{b}_k\|^2$ ,  $\boldsymbol{\mu}_k$  or the runtime of the algorithm, we refer to [Sch06].

In Section 4, we will step deeper into the impacts of these calculations and analyze their probabilistic behaviour.

## 2.3 Theory of probabilities

In this paper we will only face functions of continuous probability distributions. For a measure-theoretic formalization of probability theory we refer to [Koh09]. We will keep the definitions simple as the need arises.

### 2.3.1 Density functions

**Definition 2.1** (Density function). *A function  $f_X : \mathbb{R} \mapsto \mathbb{R}$  is called density function of a random variable  $X$  if*

$$F_X(x) = Pr[X \leq x] = \int_{-\infty}^x f(u) du, \quad (1)$$

with  $F_X$  being the cumulative distribution function of  $X$ . The image of  $f_X$  is non-negative:

$$f_X(x) \in [0 : \infty) \quad (2)$$

and the density function  $f_X(x)$  is normed such that

$$\int_{-\infty}^{\infty} f_X(x) dx = 1. \quad (3)$$

All density functions developed in the following lemmata and theorems fulfill these absolute necessary properties and are denoted with the letter  $f$  and an identifying index.

---

**Algorithm 2:** Swapping  $\mu_{k,i}$  and  $\mu_{k-1,i}$  for  $i = 1, \dots, k-2$ 

---

**Input:** the vectors  $\boldsymbol{\mu}_k = [\mu_{k,1}, \mu_{k,2}, \dots, \mu_{k,k-2}]$  and  $\boldsymbol{\mu}_{k-1} = [\mu_{k-1,1}, \mu_{k-1,2}, \dots, \mu_{k-1,k-2}]$ ,  $k \leq n$

**Output:**  $\hat{\mu}_{k,i}$  and  $\hat{\mu}_{k-1,i}$

for  $i = 1, \dots, k-2$  do

$$\left[ \begin{array}{l} \hat{\mu}_{k,i} = \mu_{k-1,i} \\ \hat{\mu}_{k-1,i} = \mu_{k,i} \end{array} \right.$$

---

---

**Algorithm 3:** Recomputation of  $\mu_{k,k-1}$ 

---

**Input:** The Gram-Schmidt coefficient  $\mu_{k,k-1}$ ,  $r_{k,k}$  and  $r_{k-1,k-1}$

**Output:**  $\hat{\mu}_{k,k-1}$

$$\hat{\mu}_{k,k-1} := \mu_{k,k-1} \frac{r_{k-1,k-1}}{\hat{r}_{k-1,k-1}} \text{ with } \hat{r}_{k-1,k-1} := \mu_{k,k-1}^2 r_{k-1,k-1} + r_{k,k}$$

---

---

**Algorithm 4:** Recomputation of  $\mu_{j,k-1}$  with  $k+1 \leq j \leq n$ 

---

**Input:**  $\hat{r}_{k-1,k-1}$ , the new projected basis vector  $\hat{\mathbf{b}}_{k-1}^*$ , and the basis vectors  $[\mathbf{b}_j, \dots, \mathbf{b}_n]^T$

**Output:**  $[\hat{\mu}_{k+1,k-1}, \hat{\mu}_{k+2,k-1}, \dots, \hat{\mu}_{n,k-1}]^T$

for  $j = k+1, \dots, n$  do

$$\left[ \hat{\mu}_{j,k-1} := \frac{\langle \mathbf{b}_j, \hat{\mathbf{b}}_{k-1}^* \rangle}{\hat{r}_{k-1,k-1}} \right.$$

---

---

**Algorithm 5:** Recomputation of  $\mu_{j,k}$  with  $k+1 \leq j \leq n$ 

---

**Input:** The new Gram-Schmidt coefficient  $\hat{\mu}_{k,k-1}$ ,  $\mathbf{b}_{k-1}^*$ ,  $\hat{\mathbf{b}}_{k-1}^*$ , and the basis vectors  $[\mathbf{b}_k, \dots, \mathbf{b}_n]^T$

**Output:**  $[\hat{\mu}_{k+1,k}, \hat{\mu}_{k+2,k}, \dots, \hat{\mu}_{n,k}]^T$

for  $j = k+1, \dots, n$  do

$$\left[ \begin{array}{l} \hat{\mathbf{b}}_k^* = \mathbf{b}_{k-1}^* - \hat{\mu}_{k,k-1} \hat{\mathbf{b}}_{k-1}^* \\ \hat{r}_{k,k} := \langle \hat{\mathbf{b}}_k^*, \hat{\mathbf{b}}_k^* \rangle \\ \hat{\mu}_{j,k} := \frac{\langle \mathbf{b}_j, \hat{\mathbf{b}}_k^* \rangle}{\hat{r}_{k,k}} \end{array} \right.$$

---

### 3 Redefined fundamental operations

Having some basic density functions of random variables  $X, Y$ , it is possible to calculate density functions of new random variables  $Z$  resulting from fundamental operations like summation or squaring of these variables  $X, Y$ .

In this section we will present probabilistic redefinitions of all the fundamental mathematical operations that take place throughout the LLL-algorithm. In the next section, these tools are used to model the behaviour of certain distributed variables touched by the LLL algorithm.

All random variables are linear independent unless otherwise stated.

#### 3.1 Distribution of linear transformations

**Lemma 3.1** (Distribution of  $Y = \alpha X + \beta$ ). *Let  $X$  be a random variable, whose values are distributed with a certain density function  $f_X$ . The random variable  $Y = \alpha X + \beta$  with  $\alpha > 0$  has the density*

$$f_Y(y) = \frac{1}{\alpha} \cdot f_X\left(\frac{y - \beta}{\alpha}\right). \quad (4)$$

*Proof.* With  $F_Y(y)$  being the distribution function of the random variable  $Y = \alpha X + \beta$  and  $f_X(x)$  being the density function of  $X$ ,  $F_Y(y)$  is defined as

$$\begin{aligned} F_Y(y) &= Pr[Y \leq y] = Pr[\alpha X + \beta \leq y] = Pr\left[X \leq \frac{y - \beta}{\alpha}\right] \\ &= F_X\left(\frac{y - \beta}{\alpha}\right) = \int_{-\infty}^{\frac{y - \beta}{\alpha}} f_X(u) du \\ f_Y(y) &= \frac{dF_Y(y)}{dy} = \frac{dF_X\left(\frac{y - \beta}{\alpha}\right)}{dy} \\ &= \frac{1}{\alpha} \cdot f_X\left(\frac{y - \beta}{\alpha}\right). \end{aligned}$$

□

#### 3.2 Distribution of sums

**Lemma 3.2** (Distribution of  $Y = \sum_i X_i$ ). *Let  $X_i$  with  $i, n \in \mathbb{N}$  and  $1 \leq i \leq n$  be a random variable, whose values are distributed with a certain combined density function  $f_X^n : \mathbb{R}^n \mapsto \mathbb{R}$  and the summation  $Y = \sum_i X_i$  with the random variable  $Y$ . Then*

$$f_Y(y) = \int_{-\infty}^{\infty} \dots \int_{-\infty}^{\infty} f_X^n\left(y - \sum_{i=2}^n x_i, x_2, x_3, \dots, x_n\right) d(x_2, x_3, \dots, x_n). \quad (5)$$

*Proof.* With  $F_Y(y)$  being the distribution function of the random variable  $Y = \sum_{i=1}^n X_i$  and  $f_X^n(x_1, x_2, \dots, x_n) : \mathbb{R}^n \mapsto \mathbb{R}$  being the combined density function of the  $n$ -dimensional random variable  $\mathbf{X}$ ,  $F_Y(y)$  is defined as

$$F_Y(y) = Pr[Y \leq y] = Pr\left[\sum_{i=1}^n X_i \leq y\right].$$

With  $\mathbf{X} = (X_1, X_2, \dots, X_n)$  and the set  $\mathfrak{B}_n \subseteq \mathbb{R}^n$ ,  $\mathfrak{B}_n := \{(X_1, X_2, \dots, X_n) \mid \sum_{i=1}^n X_i \leq y\}$  the above statement is equivalent to

$$\begin{aligned} F_Y(y) &= Pr[(X_1, X_2, \dots, X_n) \in \mathfrak{B}_n] \\ &= \int_{\mathfrak{B}_n} f_X^n(x_1, x_2, \dots, x_n) d(x_1, x_2, \dots, x_n), \end{aligned}$$

with  $X_1 \leq y - \sum_{i=2}^n X_i$

$$\begin{aligned} F_Y(y) &= \int_{-\infty}^{\infty} \dots \int_{-\infty}^{y - \sum_{i=2}^n x_i} f_X^n(x_1, x_2, \dots, x_n) d(x_1, x_2, \dots, x_n) \\ &= \int_{-\infty}^{\infty} \dots \int_{-\infty}^y f_X^n(x_1 - \sum_{i=2}^n x_i, x_2, \dots, x_n) d(x_1, x_2, \dots, x_n). \end{aligned}$$

So the density function  $f_Y(y)$  is

$$f_Y(y) = \frac{dF_Y(y)}{dy} = \int_{-\infty}^{\infty} \dots \int_{-\infty}^y f_X^n(y - \sum_{i=2}^n x_i, x_2, \dots, x_n) d(x_2, \dots, x_n).$$

□

While Lemma 3.2 comes in a bit unhandy, it is also possible to state an inductive formula representing the probability density function of a random variable  $Y = \sum_i X_i$  as in Lemma 3.3.

**Definition 3.3** (Inductive variant of Lemma 3.2). *Let  $X_i, Y_i$  be random variables with  $1 \leq i \leq n$  and  $i, n \in \mathbb{N}$ . With  $Y_n = \sum_{i=1}^n X_i$ , the density function of  $Y_i$  is defined as*

$$\begin{aligned} f_{Y_1}(y) &= f_{X_1}(x) \\ f_{Y_2}(y) &= \int_{-\infty}^{\infty} f_{X_1}(y-t) f_{X_2}(t) dt \\ f_{Y_n}(y) &= \int_{-\infty}^{\infty} f_{Y_{n-1}}(y-t) f_{X_n}(t) dt. \end{aligned}$$

### 3.3 Distribution of quotients

**Lemma 3.4** (Distribution of  $\frac{X_1}{X_2}$ ). *Let  $X_1, X_2$  be random variables, whose values are distributed with a certain combined density function  $f_X : \mathbb{R}^2 \mapsto \mathbb{R}$  and the random variable  $Y$  defined as  $Y = \frac{X_1}{X_2}$ . The density function  $f_Y(y)$  is given by*

$$f_{\frac{X_1}{X_2}}(y) = \int_{-\infty}^{\infty} |t| \cdot f_X(ty, t) dt \quad (6)$$

*Proof.* With the cumulative distribution function  $F_Y(y)$  and  $\mathfrak{B}_2 \subseteq \mathbb{R}^2$ ,  $\mathfrak{B}_2 := \{(x_1, x_2) \mid \frac{x_1}{x_2} \leq y\}$

$$\begin{aligned} F_Y(y) &= \iint_{\mathfrak{B}_2} f_X(x_1, x_2) dx_1 dx_2 \\ &= \int_{-\infty}^0 \left\{ \int_{x_2 y}^{\infty} f_X(x_1, x_2) dx_1 \right\} dx_2 + \int_0^{\infty} \left\{ \int_{-\infty}^{x_2 y} f_X(x_1, x_2) dx_1 \right\} dx_2. \end{aligned}$$

The density function  $f_Y(y)$  is given by derivating  $F_Y(y)$ :

$$\begin{aligned} f_Y(y) &= \frac{dF_Y(y)}{dy} = \int_{-\infty}^0 (-x_2) \cdot f_X(x_2y, x_2) dx_2 + \int_0^{\infty} x_2 \cdot f_X(x_2y, x_2) dx_2 \\ &= \int_{-\infty}^{\infty} |x| \cdot f_X(xy, x) dx. \end{aligned}$$

As shown in [HT00]. □

### 3.4 Distribution of products

**Lemma 3.5** (Distribution of  $X_1X_2$ ). *Let  $X_1, X_2$  be random variables, whose values are distributed with a certain combined density function  $f_X : \mathbb{R}^2 \mapsto \mathbb{R}$  and the random variable  $Y$  defined as  $Y = X_1X_2$ . The density function  $f_{X_1X_2}(y)$  is given by*

$$f_{X_1X_2}(y) = \int_{-\infty}^{\infty} \frac{1}{|t|} \cdot f_X(t, \frac{y}{t}) dt. \quad (7)$$

*Proof.* The proof is analog to the proof of Lemma 3.4. □

### 3.5 Distribution of squares

Let  $X_1, X_2, Y$  be random variables. Consider the distribution of the product  $Y = X_1X_2$  in the special case that  $X_1 = X_2$ . The vector  $\mathbf{X} = (X_1, X_2)$  is concentrated on the line  $\mathfrak{G} := \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 = x_2\}$  and  $F_X(\mathfrak{G}) = 1$  exists. Otherwise, this line  $\mathfrak{G}$  is a Borel null set of  $\mathbb{R}^2$ , meaning the 2-dimensional Lebesgue measure  $\lambda^{(2)}(\mathfrak{G}) = 0$ . Therefore the cumulative distribution function  $F_X$  of  $\mathbf{X}$  is not absolutely continuous, so the density function  $f_X$  of  $\mathbf{X}$  cannot exist.

**Lemma 3.6** (Distribution of  $X^2$ ). *Let  $X$  be a random variable, whose values are distributed with a certain density function  $f_X$  and the random variable  $Y$  representing the square  $Y = X^2$ . Then*

$$f_{X^2}(y) = \frac{1}{2\sqrt{y}} \cdot (f_X(\sqrt{y}) + f_X(-\sqrt{y})). \quad (8)$$

*Proof.* With  $F_Y(y)$  being the distribution function of the random variable  $Y$  and  $f_X(x)$  being the density function of  $X$ ,  $F_Y(y)$  is defined as

$$\begin{aligned} F_Y(y) &= Pr[Y \leq y] = Pr[X^2 \leq y] = Pr[-\sqrt{y} \leq X \leq \sqrt{y}] \\ &= \int_{-\sqrt{y}}^{\sqrt{y}} f_X(x) dx = \int_{-\sqrt{y}}^0 f_X(x) dx + \int_0^{\sqrt{y}} f_X(x) dx. \end{aligned}$$

With the substitution  $x = \sqrt{v} \Rightarrow dx = \frac{dv}{2\sqrt{v}}$  is

$$\int_0^{\sqrt{y}} f_X(x) dx = \int_0^y \frac{1}{2\sqrt{v}} f_X(\sqrt{v}) dv$$

and  $x = -\sqrt{v} \Rightarrow dx = \frac{dv}{2\sqrt{v}}$  is

$$\int_{-\sqrt{y}}^0 f_X(x) dx = \int_0^y \frac{1}{2\sqrt{v}} f_X(-\sqrt{v}) dv$$

so

$$F_Y(y) = \int_{-\sqrt{y}}^{\sqrt{y}} f_X(x) dx = \int_0^y \frac{1}{2\sqrt{v}} (f_X(\sqrt{v}) + f_X(-\sqrt{v})) dv.$$

The density function  $f_{X^2}(y)$  is defined as

$$f_{X^2}(y) = \frac{dF_Y(y)}{dy} = \frac{1}{2\sqrt{y}} (f_X(\sqrt{y}) + f_X(-\sqrt{y})).$$

□

### 3.6 Scalar products revisited

The scalar product is defined as the sum of products as in Section 2.1.1. Already having defined how summation and multiplication influence the distribution of some initial random variables, it is possible to model even more complex operations like the scalar product.

**Theorem 3.7** (Distribution of the scalar product). *Let  $X_i, Y_i, Z_i$  be random variables with  $1 \leq i \leq n$  and  $i, n \in \mathbb{N}$  and their density functions  $f_{X_i}, f_{Y_i}, f_{Z_i}$ . With  $Z_n = \sum_{i=1}^n X_i Y_i$  the density function  $f_{Z_i}$  of  $Z_i$  is defined as*

$$\begin{aligned} f_{Z_1}(z) &= f_{X_1 Y_1}(z) = \int_{-\infty}^{\infty} \frac{1}{|t|} \cdot f_{X_1}(t) \cdot f_{Y_1}\left(\frac{z}{t}\right) dt \\ f_{Z_2}(z) &= \int_{-\infty}^{\infty} f_{Z_1}(t) f_{X_2 Y_2}(z-t) dt \\ &\vdots \\ f_{Z_n}(z) &= \int_{-\infty}^{\infty} f_{Z_{n-1}}(t) f_{X_n Y_n}(z-t) dt \end{aligned} .$$

*Proof.* Theorem 3.7 follows directly from combining Definition 3.3 with Lemma 3.5.

□

## 4 Probability analysis of randomly distributed variables

Having specified all the necessary tools in the sections before, now we will analyze the probabilistic distribution of certain variables operated by the LLL-algorithm on a meaningful model of a lattice.

As mentioned before, we assume that major variables like the Gram-Schmidt coefficients  $\mu_{i,j}$  or the projected basis vectors  $\mathbf{b}_i^*$  behave like random variables. Because these variables are deterministically computed by several operations on the basis vectors  $\mathbf{b}_i \in \mathbf{B}$  of the lattice  $\mathcal{L}(\mathbf{B})$ , the components  $b_{i,j} \in \mathbf{b}_i$  also have to be distributed in a certain manner.

We initially give a model of a lattice with fixed parameters, then we analyze the initial distribution of the Gram-Schmidt coefficients  $\mu_{i,j}$  and the influence that the LLL-operations SWAP and SIZE-REDUCE have on these variables  $\mu_{i,j}$ .

Note that the second indice of a Gram-Schmidt coefficient  $\mu$  is always smaller than the first indice. Gram-Schmidt coefficients  $\mu_{i,j}$  with  $i \leq j$  are not subject to this analysis, because either  $\mu_{i,j} = 1$  for  $i = j$  or  $\mu_{i,j} = 0$  for  $i < j$ .

### 4.1 Selecting the parameters

To start with our analysis, we have to fix the distribution of the components of the basis vectors  $b_{i,j} \in \mathbf{b}_i$  and so the base of the lattice. The indice  $j \in \mathbb{N}$  denotes the component of the vector  $\mathbf{b}_i$ .

Consider following algorithm for generating our base:

---

**Algorithm 6:** Generating a basis matrix with certain distributed components

---

**Input:** A model parameter  $q \in \mathbb{N}$ , dimension  $n$

**Output:** Lower triangular matrix with row vectors  $\mathbf{b}_i$ , whose components are uniformly and independently distributed, except of the parameter  $q$  on the diagonal

---

```

for  $i = 1, \dots, n$  do
  for  $j = 1, \dots, i$  do
    if  $i == j$  then
       $b_{j,j} := q$ 
    else
       $b_{i,j} \in_{\mathcal{S}} [-\frac{q}{2}, \frac{q}{2}]$   $\triangleright$  uniformly, independently pick a number at random

```

---

The resulting lattice basis  $\mathbf{B}$  will look like:

$$\mathbf{B} := \begin{pmatrix} q & 0 & 0 & \cdots & 0 \\ b_{21} & q & 0 & \cdots & 0 \\ b_{31} & b_{32} & q & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ b_{n1} & b_{n2} & b_{n3} & \cdots & q \end{pmatrix} = \begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_n \end{bmatrix}. \quad (9)$$

With  $j < i$ ,  $b_{i,j}$  are uniformly and independently distributed in the interval  $[-\frac{q}{2}; \frac{q}{2}]$  and  $\mathbf{b}_i$  for  $i = 1, \dots, n$  are row vectors.

## 4.2 Probability distribution of the initial GSO

The examination of the initial GSO (Gram-Schmidt-Orthogonalization) consists of studying the probabilistic distribution of the variables  $\mu_{i,j}$  and  $\mathbf{b}_i^*$  before the LLL-algorithm applies its SWAP and SIZE-REDUCE operations.

First we examine the computation rule for  $\mu_{i,j} = \frac{r_{i,j}}{r_{jj}}$ , with  $j < i$  and give the probabilistic distributions of these random variables. Then we look at the projected vectors  $\mathbf{b}_i^*$  and its computation rule for  $1 \leq i \leq n$ .

**Theorem 4.1** (Distribution of the Gram-Schmidt coefficients  $\mu_{i,j}$ ). *The coefficients  $\mu_{i,j}$  are uniformly distributed within the interval  $[-\frac{1}{2}; \frac{1}{2}]$ , the density of  $\mu_{i,j}$  for  $j < i$  is given by*

$$f_{\mu_{i,j}}(x) = \begin{cases} 1 & \text{if } x \in [-\frac{1}{2}; \frac{1}{2}] \\ 0 & \text{otherwise.} \end{cases} \quad (10)$$

*Proof.* The Theorem 4.1 can be either shown by direct application of the computation rule for  $\mu_{i,j}$ , or by using the distribution functions from Section 3. To simplify matters, we will use the computation rule here:

$$\mu_{i,j} = \frac{r_{i,j}}{r_{jj}} = \frac{\langle \mathbf{b}_i \cdot \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^* \cdot \mathbf{b}_j^* \rangle} = \frac{q \cdot b_{i,j}}{q^2} = \frac{b_{i,j}}{q}.$$

With  $b_{i,j} \in_{\mathcal{S}} [-\frac{q}{2}, \frac{q}{2}]$ , this implies that  $\frac{b_{i,j}}{q} \in [-\frac{1}{2}, \frac{1}{2}]$ , so  $\mu_{i,j}$  has the density function  $f_{\mu_{i,j}}(x)$  of a uniformly distributed variable for  $j < i$ .  $\square$

**Theorem 4.2** (Distribution of the projected vectors  $\mathbf{b}_i^*$ ). *The vectors  $\mathbf{b}_i^*$  are distributed as follows*

$$\mathbf{b}_i^* = q \cdot \vec{\mathbf{e}}_i = (0, \dots, 0, q, 0, \dots, 0). \quad (11)$$

Where  $\vec{\mathbf{e}}_i \in \mathbb{R}^n$  represents the  $i$ -th unit vector of  $\mathbb{R}^n$ .

*Proof.* The Theorem 4.2 is inductively shown over  $i$ .

By Definition 2.1.3, it holds that,  $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*$ .

The inductive basis with  $i = 1$  holds:  $\mathbf{b}_1^* = \mathbf{b}_1 = q \cdot \vec{\mathbf{e}}_1$ .

For the inductive step, we assume that Theorem 4.2 holds for  $j \leq i - 1$ .  $(\dagger)$

So Theorem 4.2 follows for all  $1 \leq i \leq n$ :

$$\begin{aligned} \mathbf{b}_i^* &= \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^* \quad \text{with Theorem 4.1 follows} \\ &= \mathbf{b}_i - \sum_{j=1}^{i-1} \frac{b_{i,j}}{q} \mathbf{b}_j^* \quad \text{with the assumption } (\dagger) \\ &= \mathbf{b}_i - \sum_{j=1}^{i-1} b_{i,j} \cdot \vec{\mathbf{e}}_i \\ &= q \cdot \vec{\mathbf{e}}_i. \end{aligned}$$

$\square$

### 4.3 Probability distribution after SIZE-REDUCE

The Algorithm SIZE-REDUCE is called on every iteration of the while-loop within the LLL-algorithm 2.2.2. In this paper, we limit ourselves to analyzing the SIZE-REDUCE-algorithm executed in the first iteration of the while-loop, right after the initial GSO has been computed.

Because the Lovász-condition only refers to the Gram-Schmidt coefficients lying on the subdiagonal, we will further limit the following analysis to these coefficients.

As we view all operations on the Gram-Schmidt coefficients from a probabilistic point of view, the essential instruction  $\mu_{k,k-1} := \mu_{k,k-1} - \lfloor \mu_{k,k-1} \rfloor \mu_{k-1,k-1}$  can be represented by the function  $h : \mathbb{R}^2 \mapsto \mathbb{R}$ . With the random variables  $X$  taking values of  $\mu_{k,k-1}$  and  $Y$  is modelling  $\mu_{k-1,k-1}$ ,

$$h(X, Y) = X - \lfloor X \rfloor Y.$$

By taking a closer look at the random variables  $X$  and  $Y$ , one realizes that  $Y$  is defined as being constanly 1. The random variable  $X$  is ranging in the interval  $[-\frac{1}{2}; \frac{1}{2}]$ , which means that  $\lfloor X \rfloor = 0$ . So, in fact SIZE-REDUCE is applied on already reduced Gram-Schmidt coefficients and the algorithm does not change their values on the subdiagonal.

### 4.4 Probability distribution after SWAP

As already stated in Section 2.2.2, the SWAP-algorithm is responsible for several updates of the Gram-Schmidt coefficients. These are divided into several parts by means of Algorithm 3, 4 and 5. The first part, defined by Algorithm 2, simply swaps the values of  $\mu_{k,i}$  and  $\mu_{k-1,i}$  for all  $i \leq k-2$ . Their distributions are not altered during these computations.

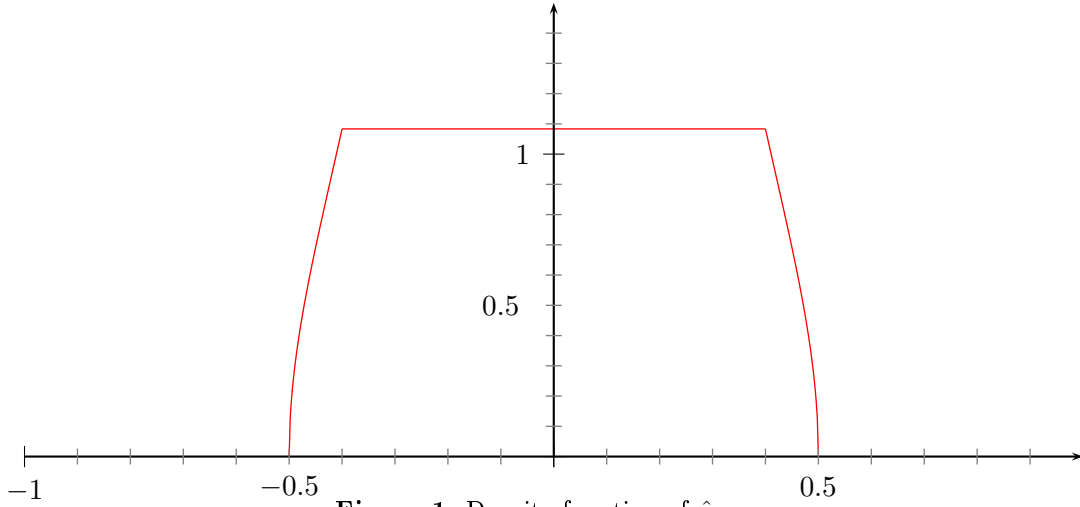
The interesting parts of SWAP are given by the algorithms 3 to 5. There, the values of some specific Gram-Schmidt coefficient are recomputed. In fact, this leads to different distributions for  $\hat{\mu}_{k,k-1}$  and  $\hat{\mu}_{j,k-1}, \hat{\mu}_{j,k}$  for  $j \geq k+1 \wedge j \leq n$ .

#### 4.4.1 Probability distribution of $\hat{\mu}_{k,k-1}$

**Theorem 4.3** (Distribution of  $\hat{\mu}_{k,k-1}$ ). *Given a random variable  $Z$  which takes values of the randomly distributed  $\hat{\mu}_{k,k-1} = \mu_{k,k-1} \frac{r_{k-1,k-1}}{\hat{r}_{k-1,k-1}}$ , with  $\mu_{k,k-1}$  being uniformly distributed as shown in Theorem 4.1.*

*With the lattice basis generated by Algorithm 6, the density function of the randomly distributed  $\hat{\mu}_{k,k-1}$  is given by*

$$f_{\hat{\mu}_{k,k-1}}(z) = \begin{cases} \frac{2}{3} \sqrt{-\frac{1}{2z} - 1} (2 - \frac{1}{2z}) & \text{if } z \in [-\frac{1}{2}; -\frac{2}{5}) \\ \frac{13}{12} & \text{if } z \in [-\frac{2}{5}; \frac{2}{5}] \\ \frac{2}{3} \sqrt{\frac{1}{2z} - 1} (2 + \frac{1}{2z}) & \text{if } z \in (\frac{2}{5}; \frac{1}{2}] \\ 0 & \text{otherwise.} \end{cases} \quad (12)$$



**Figure 1:** Density function of  $\hat{\mu}_{k,k-1}$

**Proof of Theorem 4.3.** Having all the operations defined in Section 3, we can apply them to the uniformly distributed random variable  $\mu_{k,k-1}$  in the way  $\hat{\mu}_{k,k-1}$  is being computed.

There are several parts to take care of. First we identify all the needed operations, that are applied to our uniformly distributed  $\mu_{k,k-1}$ , then we calculate the density functions for each step of the computation and in the end, we combine all steps resulting in the above stated Theorem 4.3.

With definition of Algorithm 3, it holds that,

$$\hat{\mu}_{k,k-1} := \mu_{k,k-1} \cdot \frac{r_{k-1,k-1}}{\hat{r}_{k-1,k-1}} = \frac{\mu_{k,k-1} \cdot r_{k-1,k-1}}{\hat{r}_{k-1,k-1}}, \quad (13)$$

with  $\hat{r}_{k-1,k-1} := \mu_{k,k-1}^2 \cdot r_{k-1,k-1} + r_{k,k}$  and  $r_{k-1,k-1} = \|\mathbf{b}_{k-1}^*\|^2$ .

The distribution of  $\mu_{k,k-1}$  is already known and given by Theorem 4.1, also the value of  $r_{k-1,k-1}$  is known and follows from Theorem 4.2:

$$r_{k-1,k-1} = \|\mathbf{b}_{k-1}^*\|^2 = \langle \mathbf{b}_{k-1}^* \cdot \mathbf{b}_{k-1}^* \rangle = q^2. \quad (14)$$

Next, we need to calculate the distribution, respectively the density function of the random variable  $\hat{r}_{k-1,k-1}$ .

After that, all required density functions for (13) are known and can be applied to the calculation rule of the density function of the multiplication operation in Lemma 3.5.

In (13) we have two multiplications of two random variables and one squared model parameter  $q^2$ .

**Distribution of  $\hat{r}_{k-1,k-1}$ .** In the following, we will calculate the distribution of  $\hat{\mathbf{b}}_{k-1}^*$  and then the square of its euclidean norm  $\|\hat{\mathbf{b}}_{k-1}^*\|^2 = \hat{r}_{k-1,k-1}$ . According to Section 2.1.3(GSO) and the explanation of SWAP in Section 2.2.2, it

holds that

$$\begin{aligned}
\hat{\mathbf{b}}_{k-1}^* &= \hat{\mathbf{b}}_{k-1} - \sum_{j=1}^{k-2} \hat{\mu}_{k-1,j} \cdot \hat{\mathbf{b}}_j^* \\
&= \mathbf{b}_k - \sum_{j=1}^{k-2} \mu_{k,j} \cdot \mathbf{b}_j^* \\
&= \mathbf{b}_k^* + \mu_{k,k-1} \cdot \mathbf{b}_{k-1}^*.
\end{aligned}$$

In order to get the distribution of  $\hat{\mathbf{b}}_{k-1}^*$ , we have to sum up two vectors. As stated in Theorem 4.2, the components of  $\mathbf{b}_{k-1}^*$  are 0 except in the index  $k-1$ , where  $b_{k-1,k-1}^* = q$ . The same holds for the vector  $\mathbf{b}_k^*$  for the index  $k$ .

First, we model the random variable  $X$  as the multiplication of the uniformly distributed random variable  $Y$  and the model parameter  $q$ , representing the calculation instruction  $\mu_{k,k-1} \cdot \mathbf{b}_k^*$ . This leads directly to the density function  $f_{\mu_{k,k-1} \cdot q}(x)$  for the random variable  $X$ , which is uniformly distributed.

$$f_{\mu_{k,k-1} \cdot q}(x) = \begin{cases} \frac{1}{q} & \text{if } x \in [-\frac{q}{2}; \frac{q}{2}] \\ 0 & \text{otherwise.} \end{cases} \quad (15)$$

Because of Theorem 4.2, summing  $\mu_{k,k-1} \cdot \mathbf{b}_{k-1}^*$  with the vector  $\mathbf{b}_k^*$  has no effect on the distribution of its components:

$$\hat{\mathbf{b}}_{k-1}^* = q \cdot \vec{\mathbf{e}}_k + \mu_{k,k-1} \cdot q \cdot \vec{\mathbf{e}}_{k-1} \quad (16)$$

**Lemma 4.4** (Distribution of  $\left\| \hat{\mathbf{b}}_{k-1}^* \right\|^2 = \hat{r}_{k-1,k-1}$ ). *The distribution of  $\left\| \hat{\mathbf{b}}_{k-1}^* \right\|^2$ , represented by the random variable  $Z$ , is given by the density function  $f_{\left\| \hat{\mathbf{b}}_{k-1}^* \right\|^2}(z)$*

$$f_{\left\| \hat{\mathbf{b}}_{k-1}^* \right\|^2}(z) = \begin{cases} \frac{1}{q \cdot \sqrt{z-q^2}} & \text{if } z \in (q^2; \frac{5q^2}{4}] \\ 0 & \text{otherwise.} \end{cases} \quad (17)$$

*Proof.* With (16), it holds that  $\left\| \hat{\mathbf{b}}_{k-1}^* \right\|^2 = (\mu_{k,k-1} \cdot q)^2 + q^2$ .

Note, that  $q$  is not a random variable and instead represents the model parameter picked in Section 4.1 (Selecting the parameters).

This calculation will be represented on random variables  $X, Y$  and  $Z$ , defined as  $Z = Y + q^2$ , with  $Y = X^2$ . The random variable  $Z$  represents  $\left\| \hat{\mathbf{b}}_{k-1}^* \right\|^2$  and  $X$  is taking values of  $\mu_{k,k-1} \cdot q$ .

First, we give the density function of  $Y = X^2$  and then sum  $Y$  with  $q^2$  to achieve the density function  $f_{\left\| \hat{\mathbf{b}}_{k-1}^* \right\|^2}(z)$ .

With  $X$  and its density function  $f_{\mu_{k,k-1} \cdot q}$  as stated in (15) and  $X^2$  following the

instructions of Lemma 3.6 (Distribution of squares), we get

$$\begin{aligned}
f_{(\mu_{k,k-1}\cdot q)^2}(y) &= \frac{1}{2\sqrt{y}} \cdot (f_{\mu_{k,k-1}\cdot q}(\sqrt{y}) + f_{\mu_{k,k-1}\cdot q}(-\sqrt{y})) \\
&= \frac{1}{2\sqrt{y}} \cdot \left(\frac{1}{q} + \frac{1}{q}\right) \\
&= \frac{1}{q\sqrt{y}},
\end{aligned}$$

meaning

$$f_{(\mu_{k,k-1}\cdot q)^2}(y) = \begin{cases} \frac{1}{q\sqrt{y}} & \text{if } y \in (0; \frac{q^2}{4}] \\ 0 & \text{otherwise.} \end{cases} \quad (18)$$

Now, having the density function of  $Y = X^2$ , we can state the density function of the random variable  $Z$ , being the representation of  $Z = Y + q^2$ .

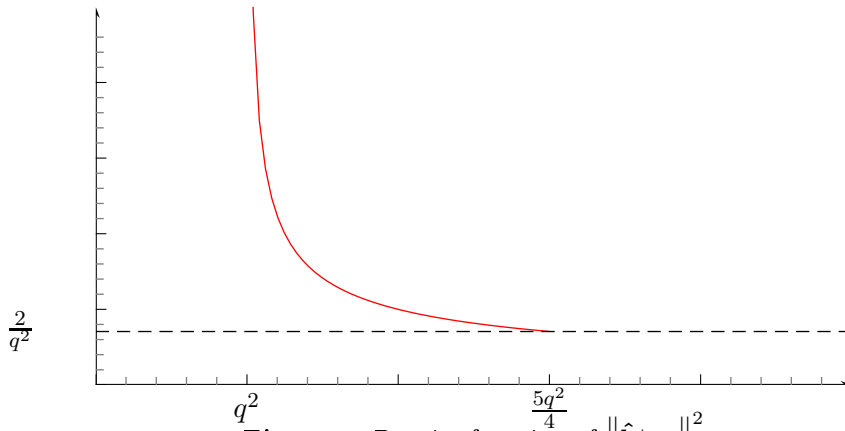
Let  $F_Z(z)$  be the distribution function of the linear transformation  $Z = Y + q^2$ , the following equations are similar to the proof of Lemma 3.1 (Distribution of linear transformation)

$$\begin{aligned}
F_Z(z) &= P(Z \leq z) = Pr[Y + q^2 \leq z] = Pr[Y \leq (z - q^2)] \\
&= F_Y(z - q^2) \\
&= \int_{-\infty}^{z-q^2} f_Y(u) du = \int_{-\infty}^{z-q^2} f_{(\mu_{k,k-1}\cdot q)^2}(u) du = \int_{-\infty}^{z-q^2} \frac{1}{q\sqrt{u}} du \\
&= \frac{2\sqrt{z - q^2}}{q},
\end{aligned}$$

so

$$f_{\|\hat{\mathbf{b}}_{k-1}^*\|^2}(z) = f_Z(z) = \frac{dF_Z(z)}{dz} = \frac{1}{q \cdot \sqrt{z - q^2}}.$$

With  $z = y + q^2$  is  $z \in (q^2; \frac{5q^2}{4}]$  □



**Figure 2:** Density function of  $\|\hat{\mathbf{b}}_{k-1}^*\|^2$

**Distribution of  $\hat{\mu}_{k,k-1}$ .** Now, we have all the necessary density functions to calculate the density of  $\hat{\mu}_{k,k-1}$ .

In remembrance of Equation (13) the calculation instruction is

$$\hat{\mu}_{k,k-1} = \frac{\mu_{k,k-1} \cdot r_{k-1,k-1}}{\hat{r}_{k-1,k-1}} \quad (19)$$

- $\mu_{k,k-1}$  represented by  $X$  is distributed with the density function  $f_{\mu_{i,j}}(x)$  as in Theorem 4.1
- $r_{k-1,k-1} = q^2$  is the squared model paramter as (14)
- $\hat{r}_{k-1,k-1}$  represented by  $Y$  is distributed with the density function  $f_{\|\hat{\mathbf{b}}_{k-1}^*\|^2}(y) = \frac{1}{q \cdot \sqrt{y-q^2}}$  as stated in Lemma 4.4

**Combining our lemmata.** Now, we use our lemmata and complete our proof of Theorem 4.3. Similiar to the proof of Lemma 4.4, we split our equation into two parts and then combine the results.

*Proof.* In the first part, we formulate the density function  $f_{\mu_{k,k-1} \cdot q^2}(x)$  of the random variable  $X = \mu_{k,k-1} \cdot r_{k-1,k-1} = \mu_{k,k-1} \cdot q^2$ . In the second part, we achieve the density function  $f_{\hat{\mu}_{k,k-1}}(z)$  of the random variable  $Z = \frac{X}{Y}$  with the random variable  $Y$  representing  $\hat{r}_{k-1,k-1}$  as stated above.  $Z$  will then model the probabilistic behaviour of  $\hat{\mu}_{k,k-1}$ .

In the same manner as in (15) we can directly state the density function of the random variable  $X$ .

$$f_{\mu_{k,k-1} \cdot q^2}(x) = \begin{cases} \frac{1}{q^2} & \text{if } x \in [-\frac{q^2}{2}; \frac{q^2}{2}] \\ 0 & \text{otherwise} \end{cases} \quad (20)$$

As formulated in Lemma 3.4 the density function of the division of two random variables  $X$  and  $Y$  is proven to be

$$f_{\frac{X}{Y}}(z) = \int_{-\infty}^{\infty} |t| \cdot f_X(tz) \cdot f_Y(t) dt \quad (21)$$

With  $f_X(x) = f_{\mu_{k,k-1} \cdot q^2}(x)$  and  $f_Y = f_{\|\hat{\mathbf{b}}_{k-1}^*\|^2}(y)$ , we get

$$f_{\frac{X}{Y}}(z) = \int_{-\infty}^{\infty} \frac{|t|}{q^3 \cdot \sqrt{t-q^2}} dt \quad (22)$$

In order to explicitly formulate the integral (22) we give a case analysis on instances  $z$  of the random variable  $Z$ . With  $x \in [-\frac{q^2}{2}; \frac{q^2}{2}]$  and  $y \in [q^2; \frac{5q^2}{4}]$ ,  $z$  is ranging in the

interval  $[-\frac{q^2}{2q^2}; \frac{q^2}{2q^2}] = [-\frac{1}{2}; \frac{1}{2}]$ .

$$f_{\frac{X}{Y}}(z) = \begin{cases} \int_{q^2}^{-\frac{q^2}{2z}} \frac{t}{q^3 \sqrt{t-q^2}} dt & \text{if } z \in [-\frac{1}{2}; -\frac{2}{5}) \\ \int_{q^2}^{\frac{5q^2}{4}} \frac{t}{q^3 \sqrt{t-q^2}} dt & \text{if } z \in [-\frac{2}{5}; \frac{2}{5}] \\ \int_{q^2}^{\frac{q^2}{2z}} \frac{t}{q^3 \sqrt{t-q^2}} dt & \text{if } z \in (\frac{2}{5}; \frac{1}{2}] \\ 0 & \text{otherwise} \end{cases}$$

By solving the integrals, we achieve the density function of the random variable  $Z$  representing  $\hat{\mu}_{k,k-1}$ :

$$f_{\hat{\mu}_{k,k-1}}(z) = \begin{cases} \frac{2}{3} \sqrt{-\frac{1}{2z} - 1} (2 - \frac{1}{2z}) & \text{if } z \in [-\frac{1}{2}; -\frac{2}{5}) \\ \frac{13}{12} & \text{if } z \in [-\frac{2}{5}; \frac{2}{5}] \\ \frac{2}{3} \sqrt{\frac{1}{2z} - 1} (2 + \frac{1}{2z}) & \text{if } z \in (\frac{2}{5}; \frac{1}{2}] \\ 0 & \text{otherwise} \end{cases}$$

A plot of this function  $f_{\hat{\mu}_{k,k-1}}(z)$  is given with Figure 1. □

#### 4.4.2 Probability distribution of $\hat{\mu}_{j,k-1}$ for all $j \geq k+1$

**Theorem 4.5** (Distribution of  $\hat{\mu}_{j,k-1}$ ). *Given a random variable  $Z$  which takes values of the randomly distributed  $\hat{\mu}_{j,k-1} = \frac{\langle \mathbf{b}_j, \hat{\mathbf{b}}_{k-1}^* \rangle}{\hat{r}_{k-1,k-1}}$ . The density function of the randomly distributed  $\hat{\mu}_{j,k-1}$  for  $j \geq k+1 \wedge j \leq n$  is given by*

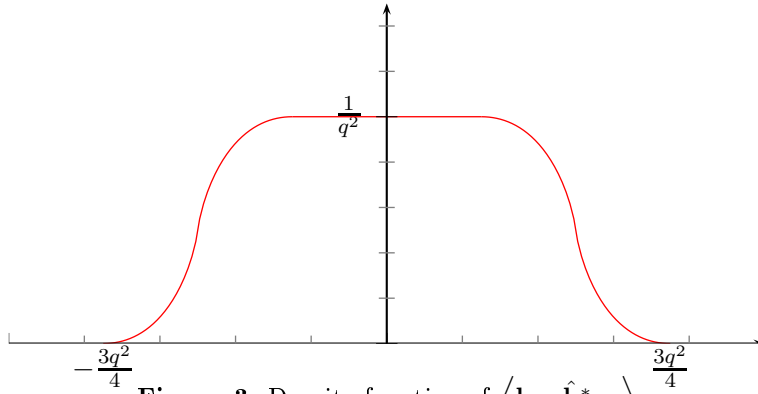
$$f_{\hat{\mu}_{j,k-1}}(z) = \begin{cases} \int_{q^2}^{-\frac{3q^2}{4z}} t \cdot f_{\langle \mathbf{b}_j, \hat{\mathbf{b}}_{k-1}^* \rangle}(z \cdot t) \cdot \frac{1}{q \sqrt{t-q^2}} dt & \text{if } z \in [-\frac{3q^2}{4}; -\frac{q^2}{4}) \\ \int_{q^2}^{\frac{5q^2}{4}} t \cdot f_{\langle \mathbf{b}_j, \hat{\mathbf{b}}_{k-1}^* \rangle}(z \cdot t) \cdot \frac{1}{q \sqrt{t-q^2}} dt & \text{if } |z| \in [0; \frac{q^2}{4}] \\ \int_{q^2}^{\frac{3q^2}{4z}} t \cdot f_{\langle \mathbf{b}_j, \hat{\mathbf{b}}_{k-1}^* \rangle}(z \cdot t) \cdot \frac{1}{q \sqrt{t-q^2}} dt & \text{if } z \in (\frac{q^2}{4}; \frac{3q^2}{4}] \\ 0 & \text{otherwise} \end{cases} \quad (23)$$

The function  $f_{\langle \mathbf{b}_j, \hat{\mathbf{b}}_{k-1}^* \rangle}$  is given with Equation (24) of the following Lemma 4.6.

**Proof of Theorem 4.5.** The density functions for the components  $\mathbf{b}_j$ ,  $\hat{\mathbf{b}}_{k-1}^*$ , and  $\hat{r}_{k-1,k-1}$  of  $\hat{\mu}_{j,k-1} = \frac{\langle \mathbf{b}_j, \hat{\mathbf{b}}_{k-1}^* \rangle}{\hat{r}_{k-1,k-1}}$  are already known as they were developed before. According to the computation rule of  $\hat{\mu}_{j,k-1}$  as stated in Theorem 4.5, we will apply our redefined fundamental operations from Section 3. In fact, we need to calculate the density function of the scalar product  $\langle \mathbf{b}_j, \hat{\mathbf{b}}_{k-1}^* \rangle$  and the density of the division with  $\hat{r}_{k-1,k-1}$ .

**Lemma 4.6** (Distribution of  $\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle$ ). *With  $\ln(\cdot)$  denoting the natural logarithm, the density function of  $\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle$  is*

$$f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}(z) = \begin{cases} \frac{1}{2q^2} + \frac{(q^2+2z) \cdot (\ln(|\frac{q^2}{2q^2+4z}|)+1)}{q^4} & \text{if } z \in [-\frac{3q^2}{4}, -\frac{q^2}{4}) \\ \frac{1}{q^2} & \text{if } z \in [-\frac{1}{4}q^2, \frac{q^2}{4}] \\ \frac{(q^2-2z) \cdot (\ln(|\frac{q^2}{-2q^2+4z}|)+1)}{q^4} & \text{if } z \in (\frac{q^2}{4}, \frac{3q^2}{4}] \\ 0 & \text{otherwise} \end{cases} \quad (24)$$



**Figure 3:** Density function of  $\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle$

*Proof.* The scalar product  $\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle$  with  $j \geq k+1$  and (16) is defined as

$$\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle = b_{k+1_k} \cdot q + b_{k+1_{k-1}} \mu_{k,k-1} \cdot q, \quad (25)$$

with

- $b_{k+1_k}$  and  $b_{k+1_{k+1}}$  uniformly distributed as stated in Section 4.1 after (9)
- $q$  as the parameter of the model and
- $\mu_{k,k-1}$  uniformly distributed with the density function stated in Theorem 4.1.

In order to calculate the probability distribution of this scalar product, we calculate the density functions  $f_{b_{k+1_k} \cdot q}$ ,  $f_{b_{k+1_{k-1}} \mu_{k,k-1} \cdot q}$  of the products and then the density function  $f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}$  of the sum of their products. According to Section 4.1, the density function  $f_{b_{k+1_k} \cdot q}$  of the uniformly distributed  $b_{k+1_k}$  multiplied with the model parameter  $q$  is modelled by the random variable  $Z$  and given by

$$f_{b_{k+1_k} \cdot q}(z) = \begin{cases} \frac{1}{q^2} & \text{if } |z| \in [0, \frac{q^2}{2}) \\ 0 & \text{otherwise} \end{cases} \quad (26)$$

**The density function  $f_{b_{k+1}k_{-1}\mu_{k,k-1}q}$ .** The density function of  $f_{b_{k+1}k_{-1}\mu_{k,k-1}q}$  is a combination of  $f_{b_{k+1}k_{-1}}$  and  $f_{\mu_{k,k-1}q}$  and developed in the following equations. The density function of  $f_{\mu_{k,k-1}q}$  of the random variable  $Z$ , representing the density of multiplying the uniformly distributed variable  $\mu_{k,k-1}$  with the model parameter  $q$ , is:

$$f_{\mu_{k,k-1}q}(z) = \begin{cases} \frac{1}{q} & \text{if } |z| \in [0, \frac{q}{2}) \\ 0 & \text{otherwise} \end{cases} \quad (27)$$

The density function  $f_{XY}$  of the product of two random variables  $X, Y$  is already given in Lemma 3.5

$$f_{XY}(z) = \int_{-\infty}^{\infty} \frac{1}{|t|} \cdot f_X(t) \cdot f_Y\left(\frac{z}{t}\right) dt. \quad (28)$$

With the random variable  $Z = X \cdot Y$  being the representation of the product of the random variables  $X, Y$  modelling  $b_{k+1}k_{-1}$  and  $\mu_{k,k-1} \cdot q$ , such that  $f_X(x) = f_{b_{k+1}k_{-1}}(x) = f_Y(y) = f_{\mu_{k,k-1}q}(y) = \frac{1}{q}$ , we get

$$f_{XY}(z) = \int_{-\infty}^{\infty} \frac{1}{|t| \cdot q^2} dt. \quad (29)$$

In order to explicitly formulate this integral, we give a case analysis on instances  $z$  of the random variable  $Z$ . With  $x, y \in [-\frac{q}{2}; \frac{q}{2}]$ ,  $z$  is ranging in the interval  $[-\frac{q^2}{4}; \frac{q^2}{4}]$ .

$$f_{XY}(z) = \begin{cases} \int_{-\frac{q}{2}}^{\frac{q}{2}} \frac{1}{|t| \cdot q^2} dt & \text{if } z = 0 \\ \int_{-\frac{2z}{q}}^{\frac{q}{2}} \frac{1}{|t| \cdot q^2} dt & \text{if } |z| \in (0; \frac{q^2}{4}] \\ 0 & \text{otherwise} \end{cases}. \quad (30)$$

By solving the integrals, we achieve the density function of the random variable  $Z$  representing  $b_{k+1}k_{-1} \cdot \mu_{k,k-1} \cdot q$

$$f_{b_{k+1}k_{-1}\mu_{k,k-1}q}(z) = \begin{cases} \frac{2 \cdot \ln(\frac{q}{2})}{q^2} & \text{if } z = 0 \\ \frac{2 \cdot \ln(|\frac{q^2}{4z}|)}{q^2} & \text{if } |z| \in (0; \frac{q^2}{4}] \\ 0 & \text{otherwise} \end{cases}. \quad (31)$$

**The density function  $f_{\langle \mathbf{b}_j \cdot \mathbf{b}_{k-1}^* \rangle}$ .** With a random variable  $Z$  and the help of the density function for a summation of two random variables  $X, Y$  from Definition 3.3, we now calculate the sum  $Z = X + Y$  of the products  $b_{k+1}k_{-1} \cdot \mu_{k,k-1} \cdot q$  represented by the random variable  $X$  with its density function  $f_X = f_{b_{k+1}k_{-1}\mu_{k,k-1}q}$  and  $b_{k+1}k_{-1}q$  represented by the random variable  $Y$  with its density function  $f_Y = f_{b_{k+1}k_{-1}q}$ .

$$\begin{aligned} f_{X+Y}(z) &= \int_{-\infty}^{\infty} f_X(t) \cdot f_Y(z-t) dt \\ &= \int_{-\infty}^{\infty} \frac{2 \cdot \ln(|\frac{q^2}{4t}|)}{q^4} dt. \end{aligned}$$

With  $x \in [-\frac{q^2}{4}; \frac{q^2}{4}]$  and  $y \in [-\frac{q^2}{2}; \frac{q^2}{2}]$ , follows  $z \in [-\frac{3q^2}{4}; \frac{3q^2}{4}]$ , we will do a case analysis on instances  $z$  of the random variable  $Z$ :

$$f_{X+Y}(z) = \begin{cases} \int_{\frac{q^2}{4}}^{\frac{q^2}{2}+z} \frac{2 \cdot \ln(|\frac{q^2}{4t}|)}{q^4} dt & \text{if } z \in [-\frac{3q^2}{4}; -\frac{q^2}{4}) \\ \int_0^{\frac{q^2}{4}} \frac{4 \cdot \ln(\frac{q^2}{4t})}{q^4} dt & \text{if } |z| \in [0; \frac{q^2}{4}] \\ \int_{-\frac{q^2}{2}+z}^{\frac{q^2}{4}} \frac{2 \cdot \ln(|\frac{q^2}{4t}|)}{q^4} dt & \text{if } z \in (\frac{q^2}{4}; \frac{3q^2}{4}] \\ 0 & \text{otherwise} \end{cases} \quad (32)$$

$$= \begin{cases} \frac{1}{2q^2} + \frac{(q^2+2z) \cdot (\ln(|\frac{q^2}{2q^2+4z}|)+1)}{q^4} & \text{if } z \in [-\frac{3q^2}{4}; -\frac{q^2}{4}) \\ \frac{1}{q^2} & \text{if } z \in [-\frac{1}{4}q^2; \frac{q^2}{4}] \\ \frac{(q^2-2z) \cdot (\ln(|\frac{q^2}{-2q^2+4z}|)+1)}{q^4} & \text{if } z \in (\frac{q^2}{4}; \frac{3q^2}{4}] \\ 0 & \text{otherwise} \end{cases} \quad (33)$$

$$= f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}. \quad (34)$$

□

**Applying Lemma 4.6** Now, we will use the density function  $f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}$  of the scalar product from Lemma 4.6 and the density function  $f_{\|\hat{\mathbf{b}}_{k-1}^*\|^2}$  of  $\hat{r}_{k-1, k-1}$  from Lemma 4.4 in order to calculate the density function of the division  $Z = \frac{X}{Y}$ . The random variable  $X$  will represent values of  $\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle$  and the random variable  $Y$  will represent values of  $\hat{r}_{k-1, k-1}$ .

Again, as stated in Section 3.4, the density function of a random variable  $Z = \frac{X}{Y}$  is proven to be

$$f_{\frac{X}{Y}}(z) = \int_{-\infty}^{\infty} |t| \cdot f_X(t \cdot z) \cdot f_Y(t) dt. \quad (35)$$

With  $f_X = f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}$  and  $f_Y = f_{\|\hat{\mathbf{b}}_{k-1}^*\|^2}$ , the density function of the division results to

$$f_{\frac{X}{Y}}(z) = \int_{-\infty}^{\infty} |t| \cdot f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}(t \cdot z) \cdot \frac{1}{q \cdot \sqrt{t - q^2}} dt. \quad (36)$$

Because  $x \in [-\frac{3q^2}{4}, \frac{3q^2}{4}]$  and  $y \in (q^2; \frac{5q^2}{4}]$ , it follows that  $z \in [-\frac{3}{4}, \frac{3}{4}]$  and with a case analysis on  $z$  we achieve our desired density function  $f_{\hat{\mu}_{j, k-1}}$  with  $j > k + 1$ :

$$f_{\frac{X}{Y}}(z) = \begin{cases} \int_{q^2}^{\frac{-3q^2}{4z}} t \cdot f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}(z \cdot t) \cdot \frac{1}{q \cdot \sqrt{t - q^2}} dt & \text{if } z \in [-\frac{3}{4}; -\frac{1}{4}) \\ \int_{q^2}^{\frac{5q^2}{4}} t \cdot f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}(z \cdot t) \cdot \frac{1}{q \cdot \sqrt{t - q^2}} dt & \text{if } |z| \in [0; \frac{1}{4}] \\ \int_{q^2}^{\frac{3q^2}{4z}} t \cdot f_{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_{k-1}^* \rangle}(z \cdot t) \cdot \frac{1}{q \cdot \sqrt{t - q^2}} dt & \text{if } z \in (\frac{1}{4}; \frac{3}{4}] \\ 0 & \text{otherwise} \end{cases} \quad (37)$$

$$= f_{\hat{\mu}_{j, k-1}}(z) \quad (38)$$

#### 4.4.3 Probability distribution of $\hat{\mu}_{j,k}$ for all $j \geq k+1$

The Gram-Schmidt coefficients  $\hat{\mu}_{j,k}$  can be calculated as follows:

$$\hat{\mu}_{j,k} = \frac{\hat{r}_{j,k}}{\hat{r}_{k,k}} = \frac{\langle \hat{\mathbf{b}}_j \cdot \hat{\mathbf{b}}_k^* \rangle}{\langle \hat{\mathbf{b}}_k^* \cdot \hat{\mathbf{b}}_k^* \rangle} = \frac{\langle \mathbf{b}_j \cdot \hat{\mathbf{b}}_k^* \rangle}{\langle \hat{\mathbf{b}}_k^* \cdot \hat{\mathbf{b}}_k^* \rangle}.$$

As already shown in Algorithm 5,  $\hat{\mathbf{b}}_k^*$  simplifies as follows

$$\begin{aligned} \hat{\mathbf{b}}_k^* &= \hat{\mathbf{b}}_k - \sum_{i=1}^{k-1} \hat{\mu}_{k,i} \cdot \hat{\mathbf{b}}_i^* \\ &= \mathbf{b}_{k-1} - \sum_{i=1}^{k-2} \mu_{k-1,i} \cdot \mathbf{b}_i^* - \hat{\mu}_{k,k-1} \cdot \hat{\mathbf{b}}_{k-1}^* \\ &= \mathbf{b}_{k-1}^* - \hat{\mu}_{k,k-1} \cdot \hat{\mathbf{b}}_{k-1}^*. \end{aligned}$$

With  $\mathbf{b}_{k-1}^* = q \cdot \vec{\mathbf{e}}_{k-1}$  and  $\hat{\mathbf{b}}_{k-1}^* = q \cdot \vec{\mathbf{e}}_k + \mu_{k,k-1} \cdot q \cdot \vec{\mathbf{e}}_{k-1}$  as in (16), this means that

$$\hat{\mathbf{b}}_k^* = q \cdot \vec{\mathbf{e}}_{k-1} \cdot (1 + \hat{\mu}_{k,k-1} \cdot \mu_{k,k-1}) - q \cdot \vec{\mathbf{e}}_k \cdot \hat{\mu}_{k,k-1}. \quad (39)$$

Applying the calculation instruction for  $\hat{\mu}_{j,k}$  results in

$$\hat{\mu}_{j,k} = \frac{b_{j_{k-1}} \cdot q \cdot (1 + \hat{\mu}_{k,k-1} \cdot \mu_{k,k-1}) - b_{j_k} \cdot q \cdot \hat{\mu}_{k,k-1}}{(q \cdot (1 + \hat{\mu}_{k,k-1} \cdot \mu_{k,k-1}))^2 + (q \cdot \hat{\mu}_{k,k-1})^2}, \quad (40)$$

with  $q$  being the model parameter and  $b_{j_{k-1}}$ , such as  $b_{j_k}$  being uniformly distributed as defined in Section 4.1,  $\mu_{k,k-1}$  is distributed as stated in Theorem 4.1 and  $\hat{\mu}_{k,k-1}$  is distributed according to the density function from Theorem 4.3.

## 5 Further Work

In order to show a more precise analysis of the Gram-Schmidt coefficients after LLL reduction than was done before, we make several restrictions to our purely theoretical probabilistic analysis.

Whether giving a theoretical or practical analysis, there are countless alternatives that could be considered.

One approach would be to vary or to relieve the restrictions that are made during this analysis, coming up with more or less meaningful results.

The first restriction comes with the design of the lattice basis. Several alternatives can be made leading to immense influences on the possibility of the success which an analysis of the Gram-Schmidt coefficients during the LLL-algorithm would have. Therefore, a lattice basis consisting of components which follow a certain Gaussian distribution, would be interesting, for example.

There are also several possible alternatives of analyzing Gram-Schmidt coefficients during the LLL-algorithm. A central question with an interesting answer would yield an analysis on Gram-Schmidt coefficients being swapped several times, or being size-reduced after they were swapped an iteration before. Even more interesting would be a deep analysis on Gram-Schmidt coefficients being processed by both operations several times, resulting in some statements of their convergence behaviour throughout their lifetime.

Unfortunately the technique of analyzing the probabilistic distribution of several random variables conjuncted in complex ways has its computational limits. While sticking to a purely theoretical analysis, we were able to use this technique in rather less complex environments.

Considering the use of automated numerical integration, there would be much more possible regarding this strict technique. Having lattices in high dimensions would make it necessary to solve high dimensional integrals like the scalar product for example. From this point of view, there would be interesting opportunities for a Monte-Carlo Simulation or numerical integrations.

## References

- [HT00] Hans-Dieter Heike and Constantin Tarcolea. *Grundlagen der Statistik und Wahrscheinlichkeitsrechnung*. Statistik 1. Oldenbourg, 2000. 8
- [Koh09] Michael Kohler. Wahrscheinlichkeitstheorie. *Vorlesungsskript*, 2009. 4
- [LLL82] Arjen Lenstra, Hendrik Lenstra, and László Lovász. *Factoring polynomials with rational coefficients*, volume Mathematische Annalen. 1982. 2, 1, 3
- [NS05] Phong Q. Nguyen and Damien Stehlé. Floating-point lll revisited. 2005. 1
- [Sch06] C.P. Schnorr. Gitter und Kryptographie. *Vorlesungsskript*, 2006. 2, 3, 4
- [SLB09] Michael Schneider, Richard Lindner, and Johannes Buchmann. Probabilistic analysis of LLL reduced bases. *WeWork 2009, Springer*, 2009. 2, 1