Institute of Information Security

University of Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

Bachelorarbeit

A Tool for the Estimation of Lattice Parameters

Nicolai Krebs

Course of Study:	Informatik, B.Sc.
Examiner:	Prof. Dr. Ralf Küsters
Supervisor:	Marc Rivinius, M.Sc.
Commenced:	April 22, 2021
Completed:	October 22, 2021

Abstract

<Short summary of the thesis>

Contents

List of Figures

List of Tables

List of Listings

List of Algorithms

Acronyms

ER error rate. 56

FR Fehlerrate. 56

RDBMS Relational Database Management System. 56

1 Introduction

- rise of quantum computing (short history)

* conceptual

* reality

- problem: some hard classical problems no longer hard

* Shor's Algorithm (Peter Shor, 1994) => quantum computers can solve the factoring and the discrete logarithm problem in polynomial time

* application to encryption

* overview of current encryption methods that will become insecure

- one solution (among hash-based, code-based, isogeny-based, and multivariate): lattice crypto

* overview over history and capability of lattice crypto

* advantages: good (quasilinear) asymptotic key sized, good concrete runtimes and key sizes, worst-case secure instantiations, advanced cryptographic primitives previously infeasible

* including intro to LWE/SIS and applications to build crypto systems

. SIS: signature schemes, hash functions

. LWE: "cryptomania" applications (PKE, ...), signature schemes, lines:

- cryptographic applications

- establishing theoretical and asymptotic hardness [Reg05] [BLP+13; MP13] - concrete hardness of LWE: attacks, runtime estimates,

* briefly outline concept and benefits of hard-case to average-case reductions

- purpose of this thesis

* building schemes: need realistic hardness estimates of schemes for given parameter settings

* lack in the past: no unified/easy to use tool => thesis aims to solve this problem tool we call *Lattice Parameter Estimation*

- overview of chapters/how to read

2 Preliminaries

2.1 Notation

In the following, we denote vectors by bold lower-case letters like $\mathbf{v}$ and matrices by bold upper-case letters $\mathbf{M}$. Unless specified otherwise, $\|\cdot\|$ is the Euclidean norm.

2.2 Math

2.2.1 Norms and Bounds

Let $\mathcal{R}_q$ be a ring as defined in [BDL+18] and $f \in \mathcal{R}_q$ with $f = \sum_i f_i X^i$. We define the following norms [BDL+18]:

(2.1) $\updownarrow_1 : \|f\|\|_1 = \sum_i |f_i|$

(2.2) $\updownarrow_2 : \|f\|\|_2 = \left(\sum_i |f_i|^2\right)^{\frac{1}{2}}$

(2.3) $\updownarrow_\infty : \|f\|\|_\infty = \max_i |f_i|$

Then the following inequations hold [BDL+18]:

(2.4) $\|f\|_1 \leq \sqrt{n}\|f\|_2$

(2.5) $\|f\|_1 \leq n\|f\|_\infty$

(2.6) $\|f\|_2 \leq \sqrt{n}\|f\|_\infty$ (since $\sqrt{n}\|f\|_2 \leq n\|f\|_\infty$)

(2.7) $\|f\|_\infty \leq \|f\|_1$

Let O_K be the ring of integers of a number field $K = \mathbb{Q}(\theta)$, where θ is an algebraic number and σ denote the canonical embedding as defined in [DPSZ12]. Then, for $x, y \in O_K$ it holds the following inequations hold (we assume that C_m in [DPSZ12] is 1) [DPSZ12].

(2.8) $\|f\|_\infty \leq \|\sigma(f)\|_\infty$

(2.9) $\|\sigma(f)\|_\infty \leq \|f\|_1$

From the above inequations, we obtain the following norm transformations to $\updownarrow_p$-norms:

- From 2.4, it follows that $\|f\|_1 \leq \sqrt{n}\|f\|_2$ and from 2.5, $\|f\|_1 \leq n\|f\|_\infty$.

- From 2.6 and 2.7, it follows that $\|f\|_2 \leq \sqrt{n}\|f\|_1$ and from 2.6, $\|f\|_2 \leq \sqrt{n}\|f\|_\infty$.
- From 2.7, it follows that $\|f\|_\infty \leq \|f\|_1$ and from 2.4 and 2.7, $\|f\|_\infty \leq \sqrt{n}\|f\|_2$.
- From 2.9, it follows that $\|\sigma(f)\|_\infty \leq \|f\|_1$, from 2.4 and 2.9, $\|\sigma(f)\|_\infty \leq \sqrt{n}\|f\|_2$, and from 2.5 and 2.9, $\|\sigma(f)\|_\infty \leq n\|f\|_\infty$.

Likewise, we get the following transformations to the C_∞-norm:

- From 2.5 and 2.8, it follows that $\|f\|_1 \leq n\|\sigma(f)\|_\infty$.
- From 2.6 and 2.8, it follows that $\|f\|_2 \leq \sqrt{n}\|\sigma(f)\|_\infty$.
- From 2.8, it follows that $\|f\|_\infty \leq \|\sigma(f)\|_\infty$.

Let f be defined as above and let $g \in \mathcal{R}_q$ where $g = \sum_i \overline{g}_i X^i$ where $g_i \in [-(q-1)/2, (q-1)/2]$ and $\overline{g}_i = g_i \mod q$ as in [BDL+18]. Then, we can define the following inequations for multiplication according to [BDL+18]:

- If $\|f\|_\infty \leq \beta, \|g\|_1 \leq \gamma$ then $\|f \cdot g\|_\infty \leq \beta \cdot \gamma$.
- If $\|f\|_2 \leq \beta, \|g\|_2 \leq \gamma$ then $\|f \cdot g\|_\infty \leq \beta \cdot \gamma$.

Let $x, y \in \mathcal{O}_K$. Again, we assume that $C_m = 1$. Then, the following inequation holds according to [DPSZ12]:

(2.10)
$$\|x \cdot y\|_\infty \leq C_m \cdot n^2 \cdot \|x\|_\infty \cdot \|y\|_\infty$$
(2.11)
$$\|\sigma(x \cdot y)\|_\infty \leq \|\sigma(x)\|_\infty \cdot \|\sigma(y)\|_\infty.$$

2.2.2 lattice

- background and history: example from lecture -> change

* Birhoff [Bir40]

* cryptoanalysis [LLL82]

* cryptosystems [Atj96, HPS98]

* [MR04]

* LWE, assumption: worst-case lattice problems are hard [Reg05]

* fully homomorphic [Gen09]

* BGV scheme [BV11, BGV12]

* tools [LPR10, LPR13] ideal latties, RLWE

- math

* lattice Λ

- discrete additive subgroup of $\mathbb{R}^m$

- Let $\mathbf{b}_1, ..., \mathbf{b}_n \in \mathbb{R}^m$ be a set of linearly independent basis vectors and $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ be the corresponding basis with column vectors $\mathbf{b}_i$

- n is the dimension of the Lattice

- $\Lambda(\mathbf{B})$ defined by all integer combinations of elements of $\mathbf{B}$:

$$\Lambda(\mathbf{B}) = \left\{ x \in \mathbb{R}^m \mid \exists \alpha_1, ..., \alpha_n \in \mathbb{Z} : \mathbf{x} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i \right\} \tag{2.12}$$

- show example plot

- full-ranked lattice: dimension is maximal, m

- basis $\mathbf{B}$ is not unique -> let $\mathbf{U} \in \mathbb{Z}^{n \times n}$ be a modular matrix (determinant is ± 1), then $\mathbf{B} \cdot \mathbf{U}$ is also a basis of the Λ ($\mathbf{U} \cdot \mathbb{Z}^n = \mathbb{Z}^n$) -> different basis for the same lattice Λ

- lattice coset: quotient group $\mathbb{R}^n / \Lambda$ of cosets

$$\mathbf{c} + \Lambda = \mathbf{c} + \mathbf{v} \mid v \in \Lambda$$

with $\mathbf{c} \in \mathbb{R}^n$

- fundamental domain: subset of $\mathbb{R}^m$ containing exactly one representative of every coset

- fundamental parallelipiped: $\mathbf{B} \cdot [-1/2, 1/2)^n$ every coset has representative

- determinant of a full-ranked lattice $\Lambda(\mathbf{B})$

$$\det(\Lambda(\mathbf{B})) = \mid \det(\mathbf{B}) \mid \tag{2.13}$$

is well-defined (independent from basis) => volume of fundamental domain can be generalized to not full-ranked => $\det(\Lambda(\mathbf{A})) = \sqrt{\det(\mathbf{A}^\perp \mathbf{A})}$

* minimum distance of $\lambda_1(\Lambda)$ of a lattice is the length of its shortest nonzero vector, i.e. $\lambda_1(\Lambda) \min_{v \in \Lambda \setminus \{0\}}$ * ith successive minimum $\lambda_i(\Lambda)$

- smallest radius r such that Λ has i linearly independent lattice vectors of norm at most r

- in general hard to calculate $\lambda_i(\Lambda(\mathbf{B}))$ for a given basis

* modular integer (or q-ary) lattices

- full-ranked lattice Λ such that $q\mathbb{Z}^m \subseteq \Lambda \subseteq \mathbb{Z}^m$ given $q \in \mathbb{N}$

- can be specified in two ways by matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$:

$$\Lambda_q(\mathbf{A}) = \{x \in \mathbb{Z}^m \mid \exists y \mathbb{Z}^n : \mathbf{x} = \mathbf{A}\mathbf{y} \mod q\} \tag{2.14}$$

or

$$\Lambda_q^\perp(\mathbf{A}) = \{x \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{x} = 0 \mod q\} \tag{2.15}$$

- finding a short vector in $\Lambda_q(\mathbf{A})$ corresponds to LWE

- finding short vectors in $\Lambda_q^\perp(\mathbf{A})$ corresponds to SIS

- easy to find basis of $\Lambda_q(\mathbf{A})$ [AFG13]

- with high probability determinant of q-ary lattice is $\det(\Lambda_q(\mathbf{A})) = q^{m-n}$ if $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$

* Gram-Schmidt basis

- set of column vectors $\mathbf{B} \in \mathbb{Z}_q^{m \times n}$, $\pi_{\text{span}(\mathbf{B})}(\mathbf{t})$ for projection of vector $\mathbf{t}$ unto span of vectors of $\mathbf{B}$

- $\pi_{\text{span}(\mathbf{B})}(\mathbf{t}) = \mathbf{B}(\mathbf{B}^{\perp}\mathbf{B})^{-1}\mathbf{B}^T \cdot \mathbf{t}$

- Gram-Schmidt orthogonalization $\tilde{\mathbf{B}} = \left\{\tilde{\mathbf{b}}_1, ..., \tilde{\mathbf{b}}_n\right\}$ of basis $\mathbf{B}$: $\tilde{\mathbf{b}}_i = \mathbf{b}_i - \pi_{\text{span}(\mathbf{b}_1,...,\mathbf{b}_{i-1})}(\mathbf{b}_i)$ for $i \in \{1, ..., n\}$

Alternative: Let $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n], \mathbf{b}_i \in \mathbb{Z}_q^m$ be a basis. Define $\tilde{\mathbf{b}}_i$ as follows: $\tilde{\mathbf{b}}_1 = \mathbf{b}_1$. For $i \in \{2, ..., n\}$ let $\tilde{\mathbf{b}}_i$ be the projection of $\mathbf{b}_i$ to the vector that is orthogonal to the span of $\{\mathbf{b}_1, ..., \mathbf{b}_{i-1}\}$. Then, $\tilde{\mathbf{B}} = \left[\tilde{\mathbf{b}}_1, ..., \tilde{\mathbf{b}}_n\right]$ is called the Gram-Schmidt orthogonalization of basis $\mathbf{B}$ where $\|\tilde{\mathbf{b}}_i\| \leq \|\mathbf{b}_i\|$.

* dual of a lattice is "the set of points whose inner products with the vectors in the lattice are integers"Λ: $\Lambda^{\perp} := \{\mathbf{w} \mid \langle \mathbf{w}, \Lambda \rangle \subset \mathbb{Z}\}$

* smoothing lemma

- Lattice problems

* Minkowski theorem: Let Λ be a lattice of dimension n, then $\lambda_1 \leq \sqrt{n} \cdot (\det \Lambda)^{\frac{1}{n}}$

* Lattice reduction: find short basis compared to $\lambda_1(\Lambda)$...

* SVP: given a basis $\mathbf{B}$ of lattice Λ find shortest nonzero lattice vector => $v \in \Lambda$ s.t. $\|v\| = \lambda_1(\Lambda)$

* SVP$_\gamma$: given a basis $\mathbf{B}$ of lattice Λ find $v \in \Lambda$ s.t. $0 < \|v\| \leq \gamma\lambda_1(\Lambda)$

* α-Approximate SVP: vector of length $\alpha\lambda_1$

* GapSVP$_\gamma$ (decision version of SVP): "given basis $\mathbf{B}$ of n-dimensional lattice Λ with either $\lambda_1\Lambda \leq 1$ or $\lambda_1\Lambda \geq \gamma(n)$, decide which is the case"

* CVP$_\gamma$: given basis $\mathbf{B}$ of n-dimensional lattice Λ and target $\mathbf{t} \in \mathbb{R}^n$ find point in lattice that is close to $\mathbf{t}$ => find $\mathbf{v} \in \mathbb{R}^n$ with $\|\mathbf{t} - \mathbf{v}\| < \gamma \min_{\mathbf{v}' \in \Lambda} \|\mathbf{v}' - \mathbf{v}\|$

* SIVP (shortest independent vector problem): given basis $\mathbf{B}$ of n-dimensional lattice Λ, find n linearly independent lattice vectors $\mathbf{v}_1, ..., \mathbf{v}_n \in \Lambda(\mathbf{B})$ such that $\max_i \|\mathbf{v}_i\|$ for $i \in \{1, ..., n\}$ is minimal

* BDD$_\gamma$: given basis $\mathbf{B}$ of n-dimensional lattice Λ and target $\mathbf{t} \in \mathbb{R}^n$ with $\text{dist}(\mathbf{t}, \Lambda) < d)\lambda_1(\Lambda)/(2\gamma(n))$, find unique lattice vector $\mathbf{v} \in \Lambda$ such that $\|\mathbf{t} - \mathbf{v}\| < d$

* ideal lattice (do I need that?)

* ...?

* eher die Sachen für LWE/SIS als die Sachen für Algorithmen (analog Vorlesung), evtl.

Intuition für die anderen Sachen... Solving SVP with approximation factors: - 1 => NP-hard [Ajt98] - $\tilde{O}(n)$ => OWF [Ajt96; MR04] - $2^{n \log\log n/\log n}$ and $2^{n/2}$ in Poly-time [LLL82] => best known 2^k-approx in $2^{\tilde{O}(n/k)}$ time (even quantum!)

2.2.3 distributions

- Gaussian, def, component-wise, trafo to bound

* definition: discrete Gaussian distribution over q-ary lattice Λ with Gaussian width parameter $s > 0$ and center $\mathbf{c}$, denoted by $D_{\Lambda,s,\mathbf{c}}$: probability of sampling a vector $\mathbf{x} \in \Lambda$ is proportional to $e^{-\pi \|\mathbf{x}-\mathbf{c}\|^2/s^2}$ In order to avoid confusion, throughout this work and in the *Lattice Parameter Estimation* we use σ to denote the standard deviation, where $\sigma = \frac{s}{\sqrt{2\pi}}$, and define $\alpha := \frac{s}{q} = \frac{\sqrt{2\pi}\sigma}{q}$.

* better definition in GPV08 => different definition needed for LWE??? * how to do this? => variant of Babai's "nearest-plane" algorithm, see [GPV08]

* component-wise

For some applications, we receive a Gaussian distribution as input, but require a bound in some norm in order to estimate the hardness of SIS. Hence, we need to transform the Gaussian width parameter into a bound β given some security parameter sec. Note that a n-dimensional Gaussian can be sampled by sampling n independent 1-dimensional Gaussians.

For a Gaussian distribution, the following holds:

$$\Pr\left[|X| \geq \beta\right] \leq 2e^{-\pi\beta^2/s^2} \tag{2.16}$$

We demand $2e^{-\pi\beta^2/s^2} \approx 2^{-sec}$, hence

$$\begin{aligned}
2e^{-\pi\beta^2/s^2} &\approx 2^{-sec} \\
-\pi\frac{\beta^2}{s^2} &\approx (-sec-1)\ln(2) \\
\beta &\approx s\sqrt{\frac{(sec+1)\ln(2)}{\pi}}
\end{aligned}$$

* smoothing factor here?

* Uniform (stuff I use in tool)

2.3 LWE and SIS

Applications: SIS can be used for one-way functions and collision-resistant hasing. LWE can be used to build pseudo-random number generators, public-key encryption schemes and oblivious transfer and secure MPC. Lattice Trapdoors (trapdoor functions, digital signatures)? Punctured Trapdoors (identity-based encryption, attribute-based encryption, predicate encryption)?

2.3.1 LWE

Following based on [Reg10]:

Introduced by Regev in [Reg09] Origin: work of Ajtai and Dwork [AD97], first public-key cryptosystem based on worst-case lattice problems, simlifications/improvements [GGH97; Reg03] imply hardness result for LWE. Early work: hardness based on unique-SVP, Peikert [Pei09] and Lyubashevsky and Micciancio [LM09] show that unique-SVP is essentially equivalent to GapSVP.

- ´cryptomania´ applications: public-key encryption schemes under chosen-plaintext attacks [KTX07; PVW08; Reg05], and chosen-ciphertext attacks [Pei09; PW08], oblivious transfer protocoles [PVW08], identity-based encryption (IBE) schemes [ABB10; CHKP10; GPV08], leakage-resilient encryption [ACPS09; AGV09; DGK+10; GKPV10], and more

- most important: fully homomorphic encryption schemes [Bra12; BV11; Gen09; GSW13]

Intuition: "recover $\mathbf{s} \in \mathbb{Z}_q^n$ given sequence of ´approximate´ random linear equations on $\mathbf{s}$"

Formal Definition:

Definition 2.3.1 (LWE Distribution [Reg10])
For $n \geq 1$, modulus $q \geq 2$, error distribution χ on $\mathbb{Z}_q$, and a fixed secret vector $\boldsymbol{s}$, let $\mathcal{A}_{\boldsymbol{s},\chi}$ be the probability distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ by choosing a vector $\boldsymbol{a} \in \mathbb{Z}_q^n$ uniformly at random, $e \in \mathbb{Z}_q$ according to χ and returning pairs of $(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e)$.

For m samples, we obtain the output $(\mathbf{A}, \mathbf{s}^{\perp}\mathbf{A} + e^{\perp})$. Additions are performed in $\mathbb{Z}_q$. We say that an algorithm solves LWE with modulus q and error distribution χ if, for any $\mathbf{s} \in \mathbb{Z}_q^n$, given an arbitrary number of independent samples from $\mathcal{A}_{\mathbf{s},\chi}$ it outputs $\mathbf{s}$ (with high probability). For $q = 2$ corresponds to *learning parity with noise* (LPN) problem.

Definition 2.3.2 (Search-LWE$_{n,q,m,\chi}$)
Search-LWE$_{n,q,m,\chi}$ asks for the recovery of the secret vector $\mathbf{s}$ given m samples

Definition 2.3.3 (Decision-LWE$_{n,q,m,\chi}$)
Given m samples, Search-LWE$_{n,q,m,\chi}$ asks to distinguish whether the samples were drawn from $\mathcal{A}_{\boldsymbol{s},\chi}$ or from a uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

Solving LWE corresponds to solving the *Bounded Distance Decoding problem* (BDD) in the lattice $\Lambda(\mathbf{A}) = \{\mathbf{s}^T \cdot A \mid \mathbf{s} \in \mathbb{Z}_q^n\} + q\mathbb{Z}^m$, where the m columns of $\mathbf{A}$ are randomly uniform vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$.

Best algorithm to solve LWE: Blum, Kalai, and Wasserman [BKW03] with $2^{O(n)}$ samples and time.

Hardness: best algorithm exponential, extension of LPN (LPN believed to be hard), hard assuming worst-case hardness of GapSVP and SIVP [Pei09; Reg05]. More details? Different cases for q exponential/polynomial, approximation factors... Hardness based on worst-case lattice problems => strong security guarantees, such as conjectured security against quantum computers...

Search to decision reduction => distiguishing is LWE samples from uniform samples sufficient, worst-case to average-case reduction => sufficient to solve distinguishing for uniform secret

2.3.2 Short Integer Solution (SIS)

The dual problem to LWE is the *Short Integer Solution problem* (SIS).

- principle: given a set of set of uniformly random vectors $\mathbf{a}_1, ..., \mathbf{a}_m \in \mathbb{Z}_q^n$ find a subset of them or combination with small coefficients that sums to zero (modulo q).

- introduced in [MR04], origins in [**Atj96**], used for ´minicrypt´ primitives: one-way functions [**Atj96**], collision resistant hash functions [GGH96], digital signature schemes [CHKP10; GPV08], and identification schemes [KTX07; Lyu08; MV03]

Definition 2.3.4 (SIS Problem (Adapted from [[LS15], Definition 3.1)
)] The problem $SIS_{n,q,m,\beta}$ is defined as follows: Given a uniformly random matrix $\mathbf{A}^{n\times m}$, find a vector $\mathbf{s} \in \mathbb{Z}_q^m$ such that $\mathbf{A} \cdot \mathbf{s} = 0$ mod q and $0 < \|\mathbf{s}\| \leq \beta$.

Finding such a vector corresponds to finding a short lattice vector in costets of the lattice $\Lambda^{\perp}(\mathbf{A}) = \{y \mid \mathbf{A} \cdot y \mod q\}$

Hardness: for any poly-bounded m, β and for "large enough" prime q: $\mathrm{SIS}_{n,q,m,\beta}$ is as hard as worst-case approx-SIVP (and GapSVP) to within $\beta \cdot \tilde{O}(\sqrt{n})$ factor

2.3.3 Ring and Module Variants

- problem key sizes in LWE/SIS in $O(n^2)$ (matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$), where $m \in \Omega(n)$)

- idea: introduce some sort of a structure in samples: n power of two, $\mathbf{a}$ vectors in groups of size n, for each group $\mathbf{a}_1 = (a_1, ..., a_n)$, a_i are uniformly random in $\mathbb{Z}_q$, and $\mathbf{a}_i = (a_i, ..., a_n, -a_1, ..., -a_{i-1})$. Hence, n vectors only need $O(n)$ memory, also speedups in operations by using FFT

- formally: vectors are elements of the ring $\mathbb{Z}_q\,[x]\,/\langle x^n + 1\rangle$ which we call $\mathcal{R}_q$ instead of the group $\mathbb{Z}_q^n$, n power of two ensures that $x^n + 1$ is irreducible over the rationals

- add more?

Definition 2.3.5 (Ring-SIS Problem [[LS15], Definition 3.3)
)] The problem $RSIS_{n,q,m,\beta}$ is defined as follows: Given $a_1, ..., a_n \in \mathcal{R}_q$ chosen independently from the uniform distribution, find $s_1, ..., s_n \in \mathcal{R}$ such that $\sum_{i=1}^m a_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = (s_1, ..., s_m)^T \in \mathcal{R}^m$.

Definition 2.3.6 (Module-SIS Problem [[LS15], Definition 3.3)
)] The problem $MSIS_{n,d,q,m,\beta}$ is defined as follows: Given $a_1, ..., a_n \in \mathcal{R}_q^d$ chosen independently from the uniform distribution, find $s_1, ..., s_n \in \mathcal{R}$ such that $\sum_{i=1}^m a_i \cdot s_i = 0 \mod q$ and $0 < \|\mathbf{s}\| \leq \beta$, where $\mathbf{s} = (s_1, ..., s_m)^T \in \mathcal{R}^m$.

While there exist special cases where the Ring structure of problem instances can be exploited in an attack on LWE or SIS, in general, the hardness of Ring and Module variants is estimated by interpreting the coefficients of elements of $\mathcal{R}_q$ as vectors in $\mathbb{Z}_q^n$ [ACD+18]. We thus reduce Ring and Module instances as follows:

- $\mathrm{RLWE}_{n,q,m,\chi} \longrightarrow \mathrm{LWE}_{n,q,m\cdot n,\chi}$

- $\mathrm{MLWE}_{n,d,q,m,\chi} \longrightarrow \mathrm{LWE}_{n\cdot d,q,m\cdot n,\chi}$
- $\mathrm{RSIS}_{n,q,m,\beta} \longrightarrow \mathrm{SIS}_{n,q,m\cdot n,\beta}$
- $\mathrm{MSIS}_{n,d,q,m,\beta} \longrightarrow \mathrm{SIS}_{n\cdot d,q,m\cdot n,\beta}$

Note that in the Ring and Module variants n denotes the degree of the polnomial of the underlying Ring, while in the standard variant, n denots the dimension of the secret.

3 Algorithms and Estimates

3.1 Lattice Basis Reduction

- measure quality of basis: Hermite factor

* basis $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_m\}$, m-dimensional lattice $\Lambda(\mathbf{B})$ has Hermite factor δ if

(3.1) $||\mathbf{b}_1|| \approx \delta^m \det(\Lambda)^{1/m}$

* use Geometric Series Assumption (GSA) to obtain estimates for $\mathbf{b}_i$:

(3.2) $||\tilde{\mathbf{b}}_i|| \approx \alpha^{i-1} ||\mathbf{b}_1||$

for $0 < \alpha < 1$ 3.1 into 3.2 -> $||\tilde{\mathbf{b}}_i|| \approx \alpha^{i-1}\delta^m \det(\Lambda)^{1/m}$ with $\prod_{i-1}^m ||\tilde{\mathbf{b}}_i|| = \det(\Lambda)$ we get

$$
\begin{aligned}
& & \prod_{i-1}^{m} ||\tilde{\mathbf{b}}_i|| &\approx \prod_{i-1}^{m} \alpha^{i-1}\delta^m \det(\Lambda)^{1/m} \\
\Leftrightarrow & & \det(\Lambda) &\approx \delta^{2m} \det(\Lambda) \prod_{i-1}^{m} \alpha^{i-1} \\
\Leftrightarrow & & \delta^{-m^2} &\approx \alpha^{\frac{m(m-1)}{2}} \\
\Leftrightarrow & & \delta^{-2} &\approx \alpha^{(m-1)/m}
\end{aligned}
$$

Hence, $alpha \approx \delta^{-2}$ and

(3.3) $||\tilde{\mathbf{b}}_i|| \approx \delta^{-2(i-1)+m} \det(\Lambda)^{1/m}$

* good basis -> first Gram-Schmidt vectors become shorter (latter longer)

* $\delta = 1.01$ feasible, $\delta = 1.007$ seems infeasible for now

* gap between provable and experimental cost estimate to reach some hermite δ => provable results only give upper bounds, for practical security we need lower bound => combine theoretical results with experimental results

* well-established estimate [LP11]

3.1.1 Cost Models for Lattice Reduction

Just insert a table and reference somewhere else? Warum notwendig, wie kommt man darauf? ... alg laufen lassen, extrapolieren...

3.2 LWE

3.2.1 Approaches

SIS

rewrite LWE as the problem of finding short vector in dual lattice => SIS

BDD

lattice reduction algorithms solve SIS and BDD

Direct

- algebraic approach Arora and Ge with subexponential complexity when $\sigma \leq \sqrt{n}$, else fully exponential, mainly of asymptotic interest (higher complexity than others)

- combinatorial algorithms: BKW as basis [BKW03], resembles generalized birthday approach by Wagner, originally for solving LPN, can be analyzed => explicit complexity for different LWE instances, theoretical analysis and actual performance close, very memory expensive (often same order as time complexity)

3.2.2 Algorithms in Estimator

Coded-BKW [GuoJohSta15]

modified BKW step -> coded-BKWE step to cancel out more positions in the **a** vectors than traditional BKW step

map part of **a** vector into nearest codeword in lattice code (linear code over $\mathcal{Z}_q$, Euclidean distance)

introduces some noise, can be kept small by appropriate parameters

pair of **a** vectors map to same codeword => add together to create new sample with part of **a** vector cancelled

samples are input to next step in BKW procedure

additional steps using discrete FFT

slightly modified for BINARY-LWE (secret vector uniformly chosen from $\{0, 1\}^n$) greatly increases performance

Dual Attack [MicReg09]

Decoding Attack [LinPei11]

Primal-uSVP [ADPS16, BaiGal14]

Meet-in-the-Middle [AlbPlaSco15]

Arora-Ge [AroGe11,ACFP14]

3.3 SIS

3.3.1 Dual Attack

MR variant [MR09]

RS variant [RS10]

3.3.2 Combinatorial Attack [MR09]

3.4 Tool

class for distributions... from section this modelling, problems, generic search... Überblick, wie verwendbar, automatische norm umwandlung, sonstige features

3.4.1 Runtime and Cost Comparison

defaults... schnellste, beste => effizient, etc. parallel... problem reductions...

4 Usage Examples

4.1 Two Problem Search

basiert auf [BDLOP18]

4.2 TODO: find other schemes to apply

5 Conclusion

Bibliography

[ABB10] S. Agrawal, D. Boneh, X. Boyen. "Efficient Lattice (H)IBE in the Standard Model". In: *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*. Ed. by H. Gilbert. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 553–572. DOI: 10.1007/978-3-642-13190-5_28. URL: https://doi.org/10.1007/978-3-642-13190-5%5C_28 (cit. on p. 24).

[ACD+18] M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, T. Wunderer. "Estimate All the {LWE, NTRU} Schemes!" In: *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*. Ed. by D. Catalano, R. D. Prisco. Vol. 11035. Lecture Notes in Computer Science. Springer, 2018, pp. 351–367. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-319-98113-0_19%7D (cit. on p. 25).

[ACPS09] B. Applebaum, D. Cash, C. Peikert, A. Sahai. "Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems". In: *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. Ed. by S. Halevi. Vol. 5677. Lecture Notes in Computer Science. Springer, 2009, pp. 595–618. DOI: 10.1007/978-3-642-03356-8_35. URL: https://doi.org/10.1007/978-3-642-03356-8%5C_35 (cit. on p. 24).

[AD97] M. Ajtai, C. Dwork. "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence". In: *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*. STOC '97. El Paso, Texas, USA: Association for Computing Machinery, 1997, pp. 284–293. ISBN: 0897918886. URL: https://doi.org/10.1145/258533.258604 (cit. on p. 24).

[AFG13] M. R. Albrecht, R. Fitzpatrick, F. Göpfert. "On the Efficacy of Solving LWE by Reduction to Unique-SVP". In: *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*. Ed. by H.-S. Lee, D.-G. Han. Vol. 8565. Lecture Notes in Computer Science. Springer, 2013, pp. 293–310. DOI: 10.1007/978-3-319-12160-4_18. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-319-12160-4_18%7D (cit. on p. 22).

[AGV09] A. Akavia, S. Goldwasser, V. Vaikuntanathan. "Simultaneous Hardcore Bits and Cryptography against Memory Attacks". In: *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings*. Ed. by O. Reingold. Vol. 5444. Lecture Notes in Computer Science. Springer, 2009, pp. 474–495. DOI: 10.1007/978-3-642-00457-5_28. URL: https://doi.org/10.1007/978-3-642-00457-5%5C_28 (cit. on p. 24).

[Ajt96] M. Ajtai. “Generating Hard Instances of Lattice Problems (Extended Abstract)”. In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*. Ed. by G. L. Miller. ACM, 1996, pp. 99–108. URL: https://doi.org/10.1145/237814.237838 (cit. on p. 22).

[Ajt98] M. Ajtai. “The Shortest Vector Problem in L_2 is *NP*-hard for Randomized Reductions (Extended Abstract)”. In: *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*. Ed. by J. S. Vitter. ACM, 1998, pp. 10–19. DOI: 10.1145/276698.276705. URL: https://doi.org/10.1145/276698.276705 (cit. on p. 22).

[BDL+18] C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner, C. Peikert. “More Efficient Commitments from Structured Lattice Assumptions”. In: *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*. Ed. by D. Catalano, R. D. Prisco. Vol. 11035. Lecture Notes in Computer Science. Springer, 2018, pp. 368–385. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-319-98113-0_20%7D (cit. on pp. 19, 20).

[BKW03] A. Blum, A. Kalai, H. Wasserman. “Noise-tolerant learning, the parity problem, and the statistical query model”. In: *J. ACM* 50.4 (2003), pp. 506–519. URL: https://doi.org/10.1145/792538.792543 (cit. on pp. 24, 28).

[BLP+13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé. “Classical hardness of learning with errors”. In: *Symposium on Theory of Computing Conference, STOC’13, Palo Alto, CA, USA, June 1-4, 2013*. Ed. by D. Boneh, T. Roughgarden, J. Feigenbaum. ACM, 2013, pp. 575–584. URL: https://doi.org/10.1145/2488608.2488680 (cit. on p. 17).

[Bra12] Z. Brakerski. “Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP”. In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*. Ed. by R. Safavi-Naini, R. Canetti. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 868–886. DOI: 10.1007/978-3-642-32009-5_50. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-32009-5_50%7D (cit. on p. 24).

[BV11] Z. Brakerski, V. Vaikuntanathan. “Efficient Fully Homomorphic Encryption from (Standard) LWE”. In: *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*. Ed. by R. Ostrovsky. IEEE Computer Society, 2011, pp. 97–106. URL: https://doi.org/10.1109/FOCS.2011.12 (cit. on p. 24).

[CHKP10] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert. “Bonsai Trees, or How to Delegate a Lattice Basis”. In: *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*. Ed. by H. Gilbert. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 523–552. DOI: 10.1007/978-3-642-13190-5_27. URL: https://doi.org/10.1007/978-3-642-13190-5%5C_27 (cit. on pp. 24, 25).

[DGK+10] Y. Dodis, S. Goldwasser, Y. T. Kalai, C. Peikert, V. Vaikuntanathan. "Public-Key Encryption Schemes with Auxiliary Inputs". In: *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*. Ed. by D. Micciancio. Vol. 5978. Lecture Notes in Computer Science. Springer, 2010, pp. 361–381. DOI: 10.1007/978-3-642-11799-2_22. URL: https://doi.org/10.1007/978-3-642-11799-2%5C_22 (cit. on p. 24).

[DPSZ12] I. Damgård, V. Pastro, N. P. Smart, S. Zakarias. "Multiparty Computation from Somewhat Homomorphic Encryption". In: *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*. Ed. by R. Safavi-Naini, R. Canetti. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 643–662. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-32009-5_38%7D (cit. on pp. 19, 20).

[Gen09] C. Gentry. "A Fully Homomorphic Encryption Scheme". AAI3382729. PhD thesis. Stanford, CA, USA, 2009. ISBN: 9781109444506 (cit. on p. 24).

[GGH96] O. Goldreich, S. Goldwasser, S. Halevi. "Collision-Free Hashing from Lattice Problems". In: *Electron. Colloquium Comput. Complex.* 3.42 (1996). URL: https://eccc.weizmann.ac.il/eccc-reports/1996/TR96-042/index.html (cit. on p. 25).

[GGH97] O. Goldreich, S. Goldwasser, S. Halevi. "Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem". In: *Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings*. Ed. by B. S. K. Jr. Vol. 1294. Lecture Notes in Computer Science. Springer, 1997, pp. 105–111. DOI: 10.1007/BFb0052230. URL: https://doi.org/10.1007/BFb0052230 (cit. on p. 24).

[GKPV10] S. Goldwasser, Y. T. Kalai, C. Peikert, V. Vaikuntanathan. "Robustness of the Learning with Errors Assumption". In: *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*. Ed. by A. C.-C. Yao. Tsinghua University Press, 2010, pp. 230–240. URL: http://conference.iiis.tsinghua.edu.cn/ICS2010/content/papers/19.html (cit. on p. 24).

[GPV08] C. Gentry, C. Peikert, V. Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. Ed. by C. Dwork. ACM, 2008, pp. 197–206. URL: https://doi.org/10.1145/1374376.1374407 (cit. on pp. 23–25).

[GSW13] C. Gentry, A. Sahai, B. Waters. "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based". In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*. Ed. by R. Canetti, J. A. Garay. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 75–92. DOI: 10.1007/978-3-642-40041-4_5. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-40041-4_5%7D (cit. on p. 24).

[KTX07] A. Kawachi, K. Tanaka, K. Xagawa. "Multi-bit Cryptosystems Based on Lattice Problems". In: *Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 16-20, 2007,* *Proceedings*. Ed. by T. Okamoto, X. Wang. Vol. 4450. Lecture Notes in Computer Science. Springer, 2007, pp. 315–329. DOI: 10.1007/978-3-540-71677-8_21. URL: https://doi.org/10.1007/978-3-540-71677-8%5C_21 (cit. on pp. 24, 25).

[LLL82] A. Lenstra, H. Lenstra, L. Lovász. "Factoring Polynomials with Rational Coefficients". In: *Mathematische Annalen* 261 (Dec. 1982). URL: %5Curl%7Bhttps://doi.org/10.1007/BF01457454%7D (cit. on p. 22).

[LM09] V. Lyubashevsky, D. Micciancio. "On Bounded Distance Decoding, Unique Shortest Vectors, and the Minimum Distance Problem". In: *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. Ed. by S. Halevi. Vol. 5677. Lecture Notes in Computer Science. Springer, 2009, pp. 577–594. DOI: 10.1007/978-3-642-03356-8_34. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-03356-8%5C_34%7D (cit. on p. 24).

[LP11] R. Lindner, C. Peikert. "Better Key Sizes (and Attacks) for LWE-Based Encryption". In: *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*. Ed. by A. Kiayias. Vol. 6558. Lecture Notes in Computer Science. Springer, 2011, pp. 319–339. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-19074-2_21%7D (cit. on p. 27).

[LS15] A. Langlois, D. Stehlé. "Worst-case to average-case reductions for module lattices". In: *Des. Codes Cryptogr.* 75.3 (2015), pp. 565–599. URL: https://doi.org/10.1007/s10623-014-9938-4 (cit. on p. 25).

[Lyu08] V. Lyubashevsky. "Lattice-Based Identification Schemes Secure Under Active Attacks". In: *Public Key Cryptography - PKC 2008, 11th International Workshop on Practice and Theory in Public-Key Cryptography, Barcelona, Spain, March 9-12, 2008. Proceedings*. Ed. by R. Cramer. Vol. 4939. Lecture Notes in Computer Science. Springer, 2008, pp. 162–179. DOI: 10.1007/978-3-540-78440-1_10. URL: https://doi.org/10.1007/978-3-540-78440-1%5C_10 (cit. on p. 25).

[MP13] D. Micciancio, C. Peikert. "Hardness of SIS and LWE with Small Parameters". In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*. Ed. by R. Canetti, J. A. Garay. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 21–39. URL: %5Curl%7Bhttps://doi.org/10.1007/978-3-642-40041-4_2%7D (cit. on p. 17).

[MR04] D. Micciancio, O. Regev. "Worst-Case to Average-Case Reductions Based on Gaussian Measures". In: *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*. IEEE Computer Society, 2004, pp. 372–381. URL: https://doi.org/10.1109/FOCS.2004.72 (cit. on pp. 22, 25).

[MV03] D. Micciancio, S. P. Vadhan. "Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More". In: *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*. Ed. by D. Boneh. Vol. 2729. Lecture Notes in Computer Science. Springer, 2003, pp. 282–298. DOI: 10.1007/978-3-540-45146-4_17. URL: https://doi.org/10.1007/978-3-540-45146-4%5C_17 (cit. on p. 25).

[Pei09] C. Peikert. “Public-key cryptosystems from the worst-case shortest vector problem: extended abstract”. In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*. Ed. by M. Mitzenmacher. ACM, 2009, pp. 333–342. URL: https://doi.org/10.1145/1536414.1536461 (cit. on p. 24).

[PVW08] C. Peikert, V. Vaikuntanathan, B. Waters. “A Framework for Efficient and Composable Oblivious Transfer”. In: *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*. Ed. by D. A. Wagner. Vol. 5157. Lecture Notes in Computer Science. Springer, 2008, pp. 554–571. DOI: 10.1007/978-3-540-85174-5_31. URL: https://doi.org/10.1007/978-3-540-85174-5%5C_31 (cit. on p. 24).

[PW08] C. Peikert, B. Waters. “Lossy trapdoor functions and their applications”. In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. Ed. by C. Dwork. ACM, 2008, pp. 187–196. DOI: 10.1145/1374376.1374406. URL: https://doi.org/10.1145/1374376.1374406 (cit. on p. 24).

[Reg03] O. Regev. “New lattice based cryptographic constructions”. In: *Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA*. Ed. by L. L. Larmore, M. X. Goemans. ACM, 2003, pp. 407–416. DOI: 10.1145/780542.780603. URL: https://doi.org/10.1145/780542.780603 (cit. on p. 24).

[Reg05] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*. Ed. by H. N. Gabow, R. Fagin. ACM, 2005, pp. 84–93. URL: https://doi.org/10.1145/1060590.1060603 (cit. on pp. 17, 24).

[Reg09] O. Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *J. ACM* 56.6 (2009), 34:1–34:40. URL: http://doi.acm.org/10.1145/1568318.1568324 (cit. on p. 24).

[Reg10] O. Regev. “The Learning with Errors Problem (Invited Survey)”. In: *Proceedings of the 25th Annual IEEE Conference on Computational Complexity, CCC 2010, Cambridge, Massachusetts, USA, June 9-12, 2010*. IEEE Computer Society, 2010, pp. 191–204. URL: https://doi.org/10.1109/CCC.2010.26 (cit. on p. 24).

All links were last followed on October 1, 2021.

A LaTeX Hints

> We cannot solve our problems with the same level of thinking that created them
>
> *(Albert Einstein)*

One sentence per line. This rule is important for the usage of version control systems. A new line is generated with a blank line. As you would do in Word: New paragraphs are generated by pressing enter. In LaTeX, this does not lead to a new paragraph as LaTeX joins subsequent lines. In case you want a new paragraph, just press enter twice (!). This leads to an empty line. In word, there is the functionality to press shift and enter. This leads to a hard line break. The text starts at the beginning of a new line. In LaTeX, you can do that by using two backslashes (\\). This is rarely used.

Please do *not* use two backslahes for new paragraphs. For instance, this sentence belongs to the same paragraph, whereas the last one started a new one. A long motivation for that is provided at `http://loopspace.mathforge.org/HowDidIDoThat/TeX/VCS/#section.3`.

One can write *emphasizied text (rendered in italics)* and **bold text**.

A.1 File Encoding and Support of Umlauts

The template offers foll UTF-8 support. All recent editors should not have issues with that.

A.2 Citations

References are set by means of `\cite[key]`.

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen am Satzanfang,
  \item die richtige Zitation unter Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der Namenspräfix \qq{van der} von \qq{Wil M.\,P.\ van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

The following sentence demonstrates 1. the capitalization of author names at the beginning of the sentence, 2. the correct citation using author names and the reference, 3. that the author names are a hyperlink to the bibliography and that 4. the bibliography contains the name prefix “van der” of “Wil M. P. van der Aalst”.

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

The following sentence demonstrates that you can overwrite the text part of the generated label using `label` in a bibliopgrahie-entry, but the year and the uniqueness is still generated by biber.

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

When creating the Bibtex file it is recommended to make sure that the DOI is listed.

A.3 Formulas and Equations

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

A list with all available mathematical symbols is provided at http://texdoc.net/pkg/symbols-a4.

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

For the documentation of editing mathematical formulas read the package documentation of `amsmath`[1].

[1] http://texdoc.net/pkg/amsmath

Equation ?? is numbered and can be referenced in the text:

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

Following equation is not numbered because of using `\align*` as environment.

Code:


```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```


Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

The template offers `\abs` to enable the bars scaling well at the absolute value:

Code:


```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```


Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

Listing A.1 The code is separated by two horizontal lines in the listings environment.

```
<listing name="second sample">
  <content>not interesting</content>
</listing>
```

More details about mathematical environments provides the documentation available at http://www.ctan.org/tex-archive/help/Catalogue/entries/voss-mathmode.html.

A.4 Sourcecode

Listing A.1 shows how to emmbed source code. With `\lstinputlisting` the source code can be loaded directly from files.

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

A.5 Pseudocode

Algorithm A.1 shows a sample algorithm.

Algorithm A.1 Sample algorithm

procedure $\textsc{Sample}(a,v_e)$
  $\mathsf{parentHandled} \leftarrow (a = \mathsf{process}) \lor \mathsf{visited}(a'), (a', c, a) \in \mathsf{HR}$
    // $(a', c'a) \in \mathsf{HR}$ denotes that a' is the parent of a
  if $\mathsf{parentHandled} \land (\mathcal{L}_{in}(a) = \emptyset \lor \forall l \in \mathcal{L}_{in}(a) : \mathsf{visited}(l))$ **then**
    $\mathsf{visited}(a) \leftarrow \text{true}$
    $$\mathsf{writes}_\circ(a, v_e) \leftarrow \begin{cases} \mathsf{joinLinks}(a, v_e) & |\mathcal{L}_{in}(a)| > 0 \\ \mathsf{writes}_\circ(p, v_e) & \exists p : (p, c, a) \in \mathsf{HR} \\ (\emptyset, \emptyset, \emptyset, false) & \text{otherwise} \end{cases}$$
    if $a \in \mathcal{A}_{basic}$ **then**
      $\textsc{HandleBasicActivity}(a,v_e)$
    else if $a \in \mathcal{A}_{flow}$ **then**
      $\textsc{HandleFlow}(a,v_e)$
    else if $a = \mathsf{process}$ **then** // Directly handle the contained activity
      $\textsc{HandleActivity}(a',v_e), (a, \perp, a') \in \mathsf{HR}$
      $\mathsf{writes}_\bullet(a) \leftarrow \mathsf{writes}_\bullet(a')$
    end if
    for all $l \in \mathcal{L}_{out}(a)$ **do**
      $\textsc{HandleLink}(l,v_e)$
    end for
  end if
end procedure

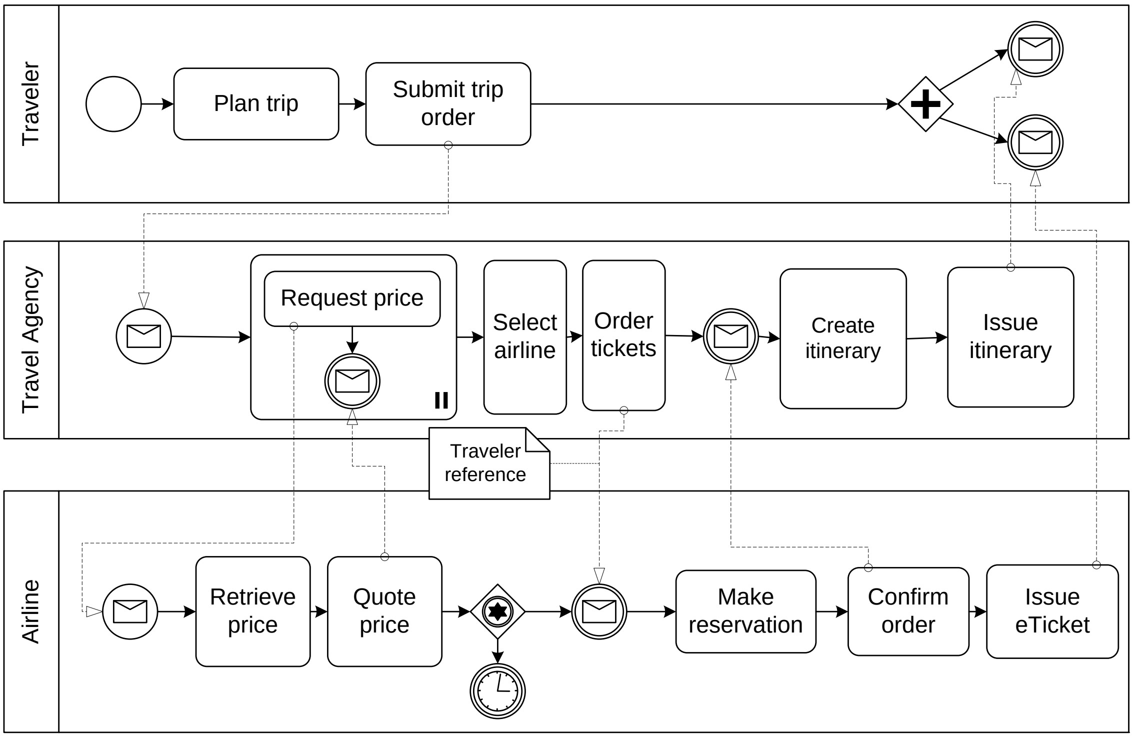


Figure A.1: Example Choreography

And if you want to write an algorithm that goes over several pages, you can only do this with the following **dirty** hack:

Algorithmus A.2 Description

code goes here
test2

A.6 Figures

The Figure A.1 and A.2 are important to understand this document. In the appendix Figure A.4 on page 49 shows again the complete choreography.

Figure A.3 shows the usage of the package subcaption. It is indeed possible to reference to sub figures: Figure A.3a.

It is possible to convert SVGs to PDF directly during compilation. This is described in the source code of latex-tipps.tex, but commented out.

A.7 More Illustrations

Figures A.4 and A.5 show two choreographies, which should further explain the facts. The second figure is rotated 90 degrees to demonstrate the `pdflscape` package.

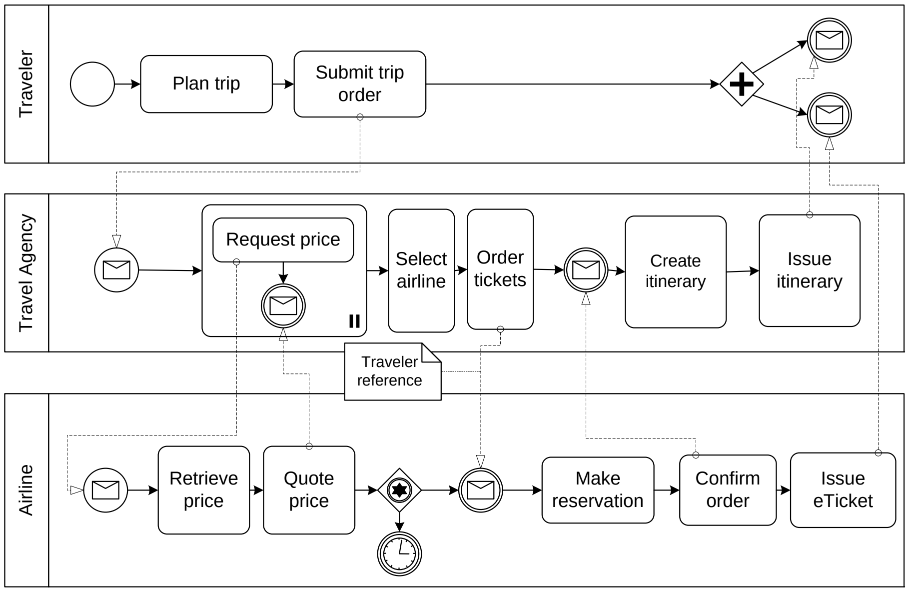
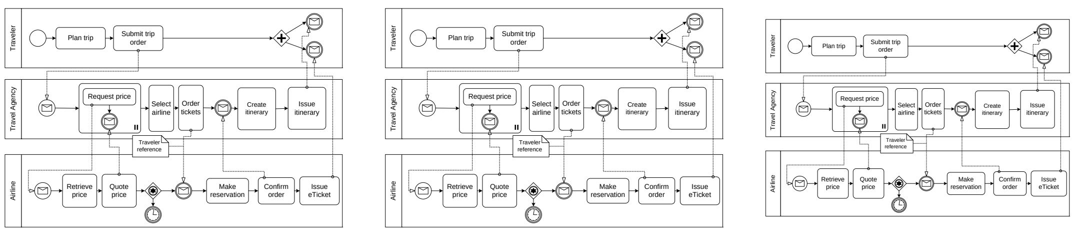


Figure A.2: The example choreography. Now slightly smaller to demonstrate `\textwidth`. And also the use of alternative captions for the list of images. However, the latter is only conditionally recommended, because who reads so much text under a picture? Or is it just a matter of style?



(a) Choreography 1 **(b)** Choreography 2 **(c)** Choreography 3

Figure A.3: Example to place 3 illustrations next to each other. Further, it is possible to reference each separately.

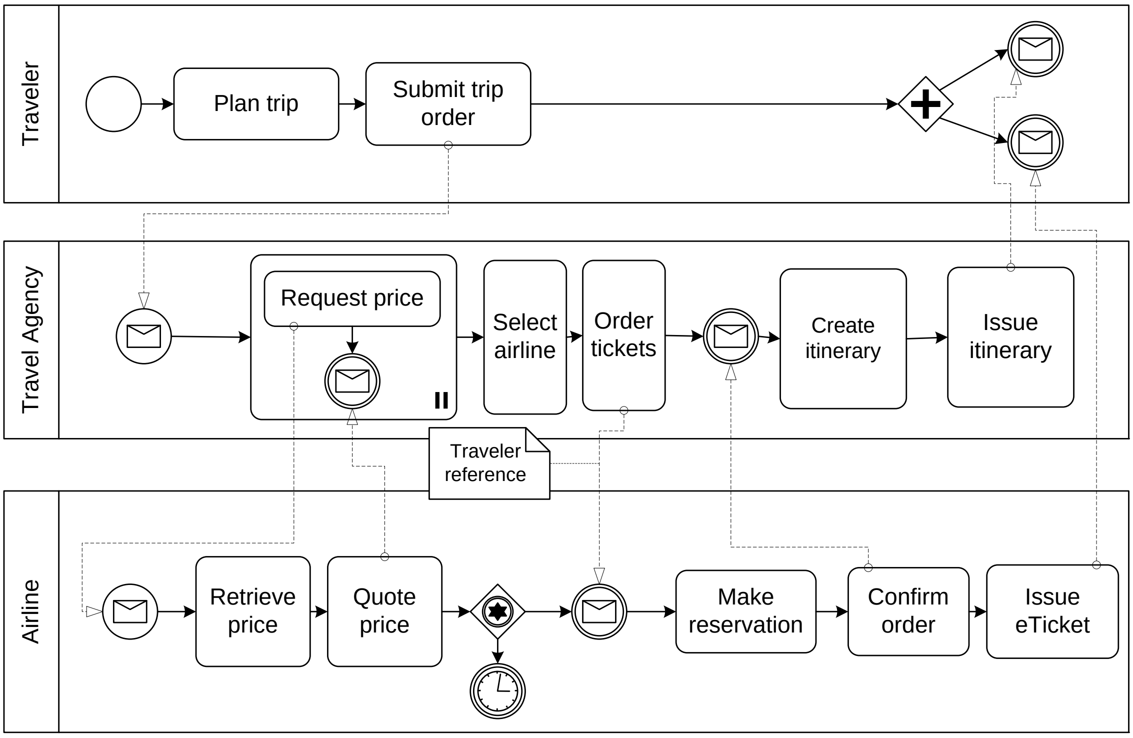


Figure A.4: Example Choreography I

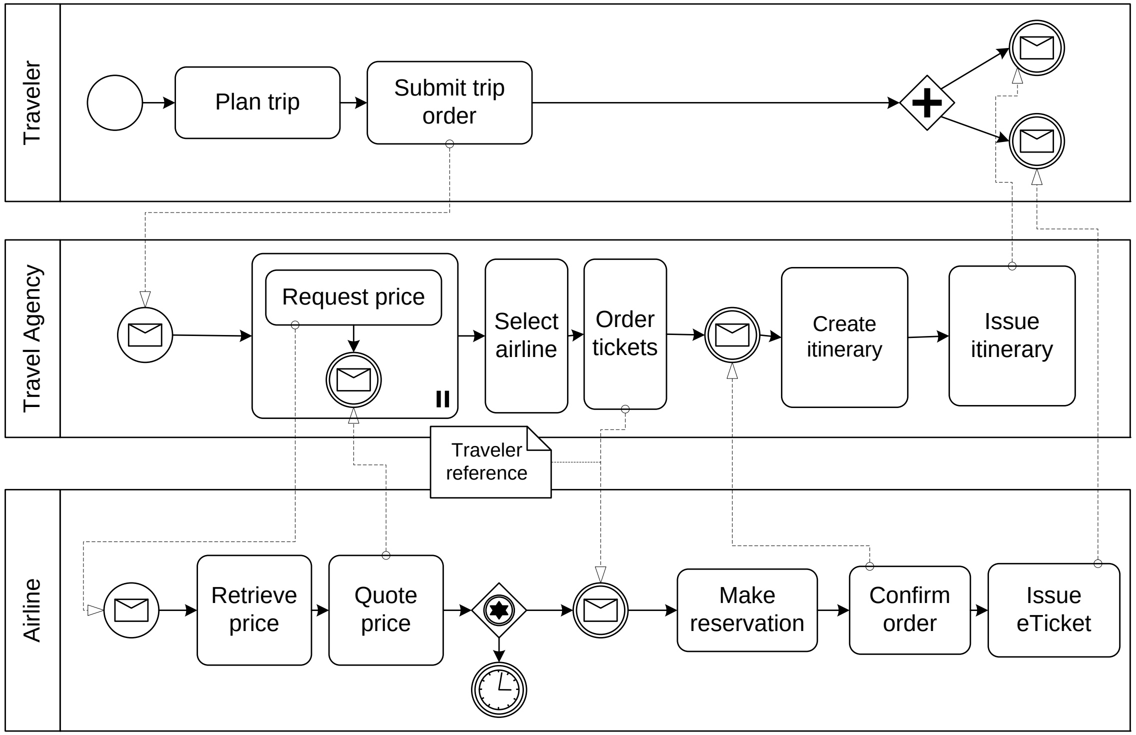


Figure A.5: Example Choreography II

A.8 Plots with pgfplots

The package pdfplots provides plotting of functions directly in LaTeX like with matlab or gnuplot. Some visual examples are available here[2].

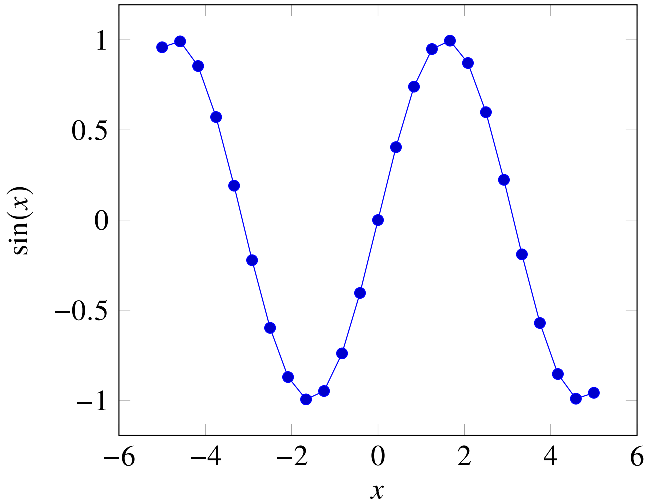


Figure A.6: Plot of $\sin(x)$ direclty inside the figure environment with pgfplots.

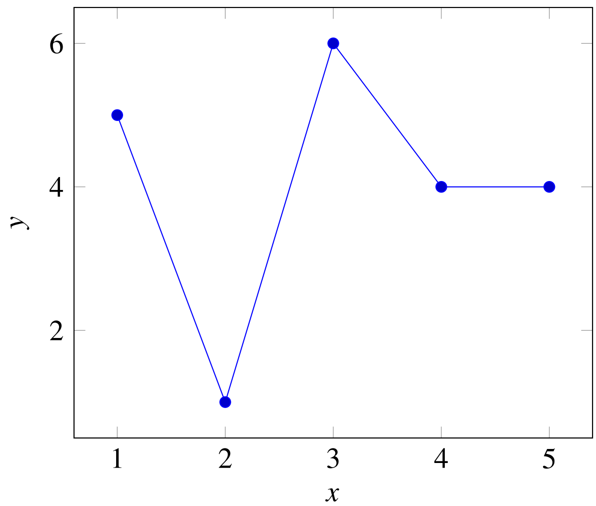


Figure A.7: Coordinates x and y read from csv file and plotted pgfplots.

A.9 Figures with tikz

The tikz is a package for creating graphics programmatically. With this package grids or other regular strucutres can be easliy generated.

[2]http://texdoc.net/pkg/visualtikz

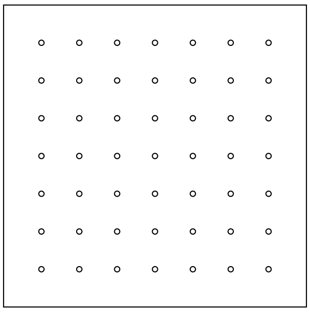


Figure A.8: A regular grid genrated with easily with two for loops.

A.10 UML diagrams using tikz-uml

Figure A.9 presents a class diagram typeset using tikz-uml.

A.11 UML diagrams using PlantUML

In case LuaLaTeX is used and PlantUML is installed, UML diagrams can be defined using PlantUML.

A.12 Linguistic Forests

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

A.13 Tables

Table A.1 shows results and Table A.2 shows how numerical data can be represented in a table.

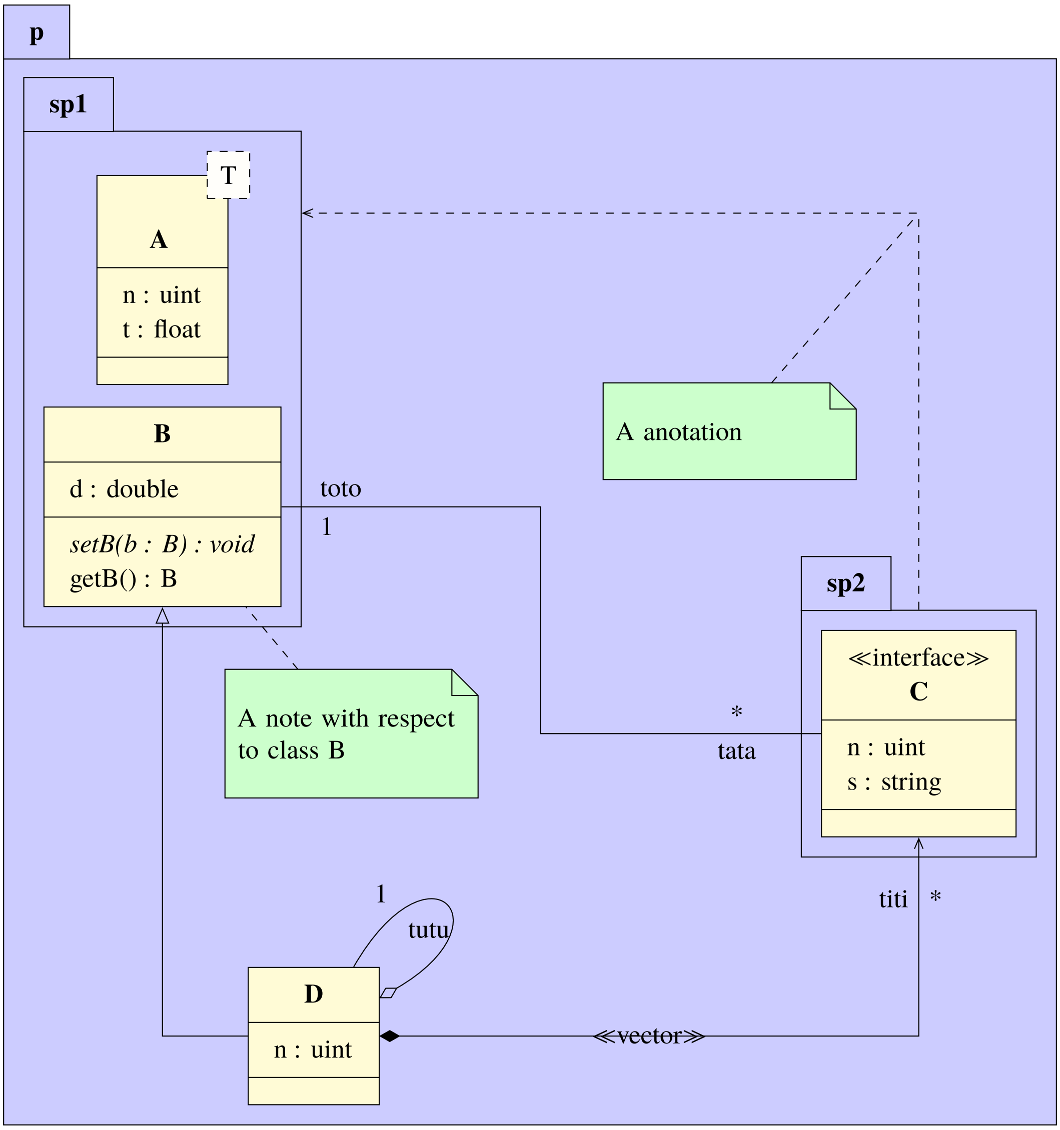


Figure A.9: Class diagram generated with tikz-uml. Example adapted from Nicolas Kielbasiewicz.

summed		Title
Table	as	in
`tabsatz.pdf`	recommended	gesetzt
Example	a nice example for using “multirow”	

Table A.1: Exampe Table – see `http://www.ctan.org/tex-archive/info/german/tabsatz/`

	Parameter 1		Parameter 2		Parameter 3		Parameter 4	
Bedingungen	**M**	**SD**	**M**	**SD**	**M**	**SD**	**M**	**SD**
W	1.1	5.55	6.66	.01				
X	22.22	0.0	77.5	.1				
Y	333.3	.1	11.11	.05				
Z	4444.44	77.77	14.06	.3				

Table A.2: Example table for 4 constraints (W-Z), each having 4 parameters with (M und SD). Note: use always the same number of decimal places.

A.13.1 Tables with pgfplots

With the pgfplotstable package tables can be directly generated from a csv file.

	b	c	d
1	4	5	1
2	3	1	5
3	5	6	1
4	1	4	9
5	3	4	7

Table A.3: Table direclty generated from the values of a csf file.

A.14 Tables spanning multiple pages

Table A.4: A sample long table.

First column	Second column	Third column
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D

Continued on next page

Table A.4 – continued from previous page

First column	Second column	Third column
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D

Continued on next page

Table A.4 – continued from previous page

First column	Second column	Third column
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D
A	BC	D

A.15 Abbreviations

At the first pass the Fehlerrate (FR) was 5. At the second pass was FR 3. The plural form can be seen here: error rates (ERs). To demonstrate what the list of abbreviations looks like for longer description texts, Relational Database Management Systems (RDBMS) must be mentioned here.

With `\gls{...}` you can enter abbreviations, the first time you call it, the long form is used. When reusing `\gls{..}` the short form is automatically displayed. The abbreviation is also automatically inserted in the abbreviation list. With `\glspl{...}` the plural form is used. If you want the short form to appear directly at the first use, you can use `\glsunset{..}` to mark an abbreviation as already used. The opposite is achieved with `\glsreset{..}`.

Abbreviations are defined in `\content\ausarbeitung.tex` by means of `\newacronym{...}{...}{...}`.

More information at: http://tug.ctan.org/macros/latex/contrib/glossaries/glossariesbegin.pdf

A.16 References

For distant sections "varioref" is recommended: "See Appendix A.3 on page 43". The command `\vref` works similar to `\cref` the difference beeing that a reference to the page is additionally added. `vref`: "Appendix A.1 on page 41", `cref`: "Appendix A.1", `ref`: "A.1".

If "varioref" causes difficulties, then "cref" can be used instead. This also creates the word "section" automatically: Appendix A.3. This is also possible for illustrations etc. In English please use `\Cref{...}` (with large "C" at the beginning).

A.17 Definitions

Definition A.17.1 (Title)
Definition Text

Definition A.17.1 shows ...

A.18 Footnotes

Footnotes are provided by the command `\footnote{...}`[3]. Citing footnotes is possible by provinding a label`\footnote{\label{...}...}` and cite the footnote with `\cref{...}` in the text[3].

A.19 Various Things

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix "van der" von "Wil M. P. van der Aalst" steht.

[3] Example footnote.

The words “workflow” and “dwarflike” can be copied from the PDF and pasted to a text file.

Code:

```
\begin{inparaenum}[1.]
  \item die Großschreibung von Autorennamen
am Satzanfang,
  \item die richtige Zitation unter
Verwendung von Autorennamen und der Referenz,
  \item dass die Autorennamen ein Hyperlink
auf das Literaturverzeichnis sind sowie
  \item dass in dem Literaturverzeichnis der
Namenspräfix \qq{van der} von \qq{Wil M.\,P.\
 van der Aalst} steht.
\end{inparaenum}
```

Result:

1. die Großschreibung von Autorennamen am Satzanfang, 2. die richtige Zitation unter Verwendung von Autorennamen und der Referenz, 3. dass die Autorennamen ein Hyperlink auf das Literaturverzeichnis sind sowie 4. dass in dem Literaturverzeichnis der Namenspräfix “van der” von “Wil M. P. van der Aalst” steht.

A.20 Closing remarks

Please feel free to provide enhancements for this template and create a new ticket on GitHub (https://github.com/latextemplates/uni-stuttgart-computer-science-template/issues).

Declaration

I hereby declare that the work presented in this thesis is entirely my own and that I did not use any other sources and references than the listed ones. I have marked all direct or indirect statements from other sources contained therein as quotations. Neither this work nor significant parts of it were part of another examination procedure. I have not published this work in whole or in part before. The electronic copy is consistent with all submitted copies.

place, date, signature