# A Note on Short Invertible Ring Elements and Applications to Cyclotomic and Trinomial Number Fields

Thomas Attema[1,2,3,*], Ronald Cramer[1,3], Chaoping Xing[4,5]

[1]CWI, Cryptology Group, Amsterdam, The Netherlands
[2]TNO, Cyber Security and Robustness, The Hague The Netherlands
[3]Leiden University, Mathematical Institute, Leiden, The Netherlands
[4]NTU, School of Physical and Mathematical Sciences, Singapore, Singapore
[5]SJTU, School of Electronic Information and Electrical Engineering, Shanghai, China

*Received: 23rd June 2020 | Revised: 27th April 2021 | Accepted: 6th June 2021*

**Abstract** *Ring-SIS based Σ-protocols require a challenge set $C$ in some ring $\mathcal{R}$, usually an order in a number field $L$. These Σ-protocols impose various requirements on the subset $C$, and finding a good, or even optimal challenge set is a non-trivial task.*
*In particular, (1) the set $C$ should be 'large', (2) elements in $C$ should be 'small', and (3) differences of distinct elements in $C$ should be invertible modulo a rational prime $p$. Moreover, for efficiency purposes, it is desirable that (4) the prime $p$ is small, and that (5) it splits in many factors in the number field $L$.*
*These requirements on $C$ are subject to certain trade-offs, e.g., between the splitting behavior of the prime $p$ and its size. Lyubashevsky and Seiler (Eurocrypt 2018) have studied these trade-offs for subrings of cyclotomic number fields. Cyclotomic number fields possess convenient properties and as a result most Ring-SIS based protocols are defined over these specific fields. However, recent attacks have shown that, in certain protocols, these convenient properties can be exploited by adversaries, thereby weakening or even breaking the cryptographic protocols.*
*In this work, we revisit the results of Lyubashevsky and Seiler and show that they follow from standard Galois theory, thereby simplifying their proofs. Subsequently, this approach leads to a natural generalization from cyclotomic to arbitrary number fields. We apply the generalized results to construct challenge sets in trinomial number fields of the form $\mathbb{Q}[X]/(f)$ with $f = X^n + aX^k + b \in \mathbb{Z}[X]$ irreducible. Along the way we prove a conjectured result on the practical applicability for cyclotomic number fields and prove the optimality of certain constructions.*
*Finally, we find a new construction for challenge sets resulting in slightly smaller prime sizes.*

**Keywords:** Lattice, Zero-Knowledge Proof, Challenge Set, Invertibility, Trinomials, Number Theory.

**2010 Mathematics Subject Classification:** 94A60, 11Y40

## 1 INTRODUCTION

Many cryptographic protocols, such as identification and digital-signature schemes, require one party (prover $\mathcal{P}$) to convince another party (verifier $\mathcal{V}$) of knowing the pre-image of some element under a one-way function without leaking information about this pre-image, i.e., in zero-knowledge. In the discrete-logarithm setting, Schnorr suggested an elegant and efficient interactive protocol for producing these so-called zero-knowledge proofs [46]. Three-round interactive proofs, such as Schnorr's protocol, are called Σ-protocols. In turn, the Fiat-Shamir heuristic transforms any Σ-protocol into a non-interactive proof [28]. Recently the Fiat-Shamir transformation has proven to be secure against quantum adversaries [26, 35].

In contrast to discrete-log based Σ-protocols, lattice-based Σ-protocols require a proof that such a pre-image is 'short'. Because of this additional requirement, a straightforward adaptation of Schnorr's approach to the lattice setting introduces some challenges.

First, in this setting knowledge extractors, which are used to prove soundness of Σ-protocols, are typically only capable of extracting pre-images with norms larger than what is claimed by the prover. In other words, a prover that knows a pre-image in some set $S$ is only capable of proving knowledge of a pre-image in some strictly larger set $S'$. This discrepancy is called the *soundness slack* of the protocol. In contrast to the naive approach, Lyubashevsky's rejection sampling technique [36, 37] significantly reduces the soundness slack.

Second, in contrast to discrete-logarithm based protocols, many lattice-based Σ-protocols suffer from a large soundness error, i.e., even dishonest provers succeed in convincing a verifier with large probability. Therefore, these

*Corresponding Author: thomas.attema@tno.nl

protocols have to be repeated many times to reduce the soundness error and achieve the desired security level. The number of repetitions is also called the *overhead* of the protocol. While it is challenging to reduce the overhead for a single instance, the overhead can be amortized over many instances without increasing the soundness slack [17, 24, 4, 18, 3].

Another approach to limit the soundness slack and overhead of lattice-based Σ-protocols is by relaxing the statement that is proven. Instead of proving knowledge of a short pre-image of a public element, $\mathcal{P}$ proves knowledge of a pre-image of a related element. These relaxed protocols are called *approximate* Σ-protocols. For some cryptographic primitives approximate proofs of knowledge are sufficient, but others require exact proofs of knowledge [12, 53].

A key component in (approximate) Σ-protocols is the challenge set $C$. In this work we focus on the protocols based on the Ring-SIS assumption. These protocols are defined over a ring $\mathcal{R}/p\mathcal{R}$ where $\mathcal{R}$ is usually the ring of integers of a number field $L$ and $p$ is a rational prime. The field $L$ is often chosen to be cyclotomic, i.e., $L = \mathbb{Q}(\zeta_m)$ for some primitive $m^{th}$-root of unity $\zeta_m$ with minimal polynomial $\Phi_m(X)$.

The efficiency of these protocols critically depends on the choice of a good challenge set $C \subset \mathcal{R}/p\mathcal{R}$. The Ring-SIS hardness condition requires elements in $C$ to have small norm. The approximation factor is determined by the norms of the challenges in $C$. To achieve a small soundness error, the set $C$ should be large ($|C| \approx 2^{256}$).[1] Moreover, an element of the ring $\mathcal{R}/p\mathcal{R}$ has bit size $n \log_2(p)$ where $n$ is the degree of the number field $L$. For this reason, the communication complexity of the (approximate) Σ-protocols is $\Omega(n \log(p))$ and we aim to choose the prime $p$ as small as possible.

Additional (computational) efficiency improvements can be obtained by using the *Chinese Remainder Theorem* (CRT) or *Number Theoretic Transform* (NTT) [7]. The advantage of this technique depends on the splitting behavior of the rational prime $p$ in the ring $\mathcal{R}$. More precisely, the more distinct prime factors $p$ has in $\mathcal{R}$, the more efficient elementary operations in $\mathcal{R}/p\mathcal{R}$ can be implemented. Finally, when using these Σ-protocols as subroutines in other cryptographic protocols (e.g., group signature schemes), the differences $c - c'$ of elements in $c, c' \in C$ might be required to be invertible in $\mathcal{R}/p\mathcal{R}$ [6, 38, 5, 45].

Hence good challenge sets $C \subset \mathcal{R}/p\mathcal{R}$ satisfy the following properties:

1. elements in $C$ are 'small',
2. $C$ is large,
3. the prime $p$ is small,
4. $p$ splits in many factors in $\mathcal{R}$,
5. all non-zero elements in $C - C = \{c - c' | c, c' \in C\}$ are invertible.

When $\mathcal{R} = O_L$ is the ring of integers of a number field $L$, a subset $E \subset \mathcal{R}$ for which all mutual differences are invertible is called an *exceptional set*. The maximal cardinality of such a subset $E$ is called the *Lenstra constant* of $L$ [34] and finding number fields with large Lenstra constant has been of independent interest for many years. Exceptional sets also appear in cryptographic primitives, such as black-box secret sharing [25, 22, 23]. However, our situation is slightly different. First, we only require mutual differences to be invertible modulo a rational prime $p$ and, second, we additionally require elements to be of small norm.

The above requirements introduce compromises between, for example, the invertibility condition and the splitting behavior of the prime $p$. Lyubashevsky and Seiler [41] show that, when $\mathcal{R}$ is the ring of integers in a cyclotomic number field $L$, there exist primes $p$ that split in more than two factors and for which good challenge sets $C \subset \mathcal{R}/p\mathcal{R}$ exist. Their main result is stated in Theorem 1. In this theorem, $\Phi_m(X)$ is the $m^{th}$-cyclotomic polynomial, i.e., the minimal polynomial of an $m^{th}$-primitive root of unity $\zeta_m$, $\varphi$ is the Euler totient function and the quantities $s_1(m)$ and $s_1(z)$ are the largest singular values of matrices that will be defined in Section 2.

**Theorem 1** ([41]). *Let $m = \prod p_i^{e_i}$ for $e_i \geq 1$ and $z = \prod p_i^{f_i}$ for $1 \leq f_i \leq e_i$. If $p$ is a prime such that $p \equiv 1 \mod z$ and $\mathrm{ord}_m(p) = m/z$, then the polynomial $\Phi_m(X)$ factors as*

$$\Phi_m(X) \equiv \prod_{j=1}^{\varphi(z)} (X^{m/z} - r_j) \mod p,$$

*for distinct $r_j \in \mathbb{Z}_p^*$ where $X^{m/z} - r_j$ are irreducible in the ring $\mathbb{Z}_p[X]$. Furthermore, any $\mathbf{y} \in \mathbb{Z}_p[X]/(\Phi_m(X))$ that satisfies either*

$$0 < ||\mathbf{y}||_\infty < \frac{1}{s_1(z)} p^{1/\varphi(z)} \quad \text{or}$$

[1] As mentioned earlier, an alternative approach is to reduce the soundness error by repeating the protocol multiple times at the cost of introducing overhead and thereby increasing the communication and computation costs.

$$0 < ||\mathbf{y}|| < \frac{\sqrt{\varphi(m)}}{s_1(m)} p^{1/\varphi(z)}$$

*has an inverse in* $\mathbb{Z}_p[X]/(\Phi_m(X))$.

To prove this theorem, Lyubashevsky and Seiler construct a specific lattice $\mathcal{L}$ and show that an invertibility condition follows from a lower bound on the length of the shortest vector of this lattice. In addition, they explicitly express polynomials in the ring $\mathbb{Z}[X]/(\Phi_m(X))$ in terms of a basis over some subring and relate the invertibility to this subring.

As many other cryptographic constructions based on ideal lattices, the work of Lyubashevsky and Seiler focuses on cyclotomic number fields. However, a number of recent attacks have exposed certain vulnerabilities of some of these constructions. These vulnerabilities are due to additional structure of cyclotomic number fields. In general, the attacks consist of two steps:

1. Given a principal ideal $I$ in the ring $\mathcal{R}$, find an arbitrary generator $g \in \mathcal{R}$ of $I$;
2. Given a principal ideal $I$ and a generator $g$ of this ideal, find a short generator $h$ of $I$.

The first step in this attack is also referred to as solving the *Principal Ideal Problem* (PIP). For cyclotomic number fields $L$ with prime power conductor Biasse and Song [10] gave a quantum algorithm for solving this problem in time polynomial in the degree of $L/\mathbb{Q}$.

For the second step note that $g$ and $h$ generate the same ideal and hence differ by a unit, i.e., $g = hu$ for some unit $u \in \mathcal{R}^*$. For the number field $L$, with embeddings $\sigma_i : L \to \mathbb{R}$ for $1 \leq i \leq r$ and $\sigma_i, \bar{\sigma}_i : L \to \mathbb{C}$ for $r+1 \leq i \leq r+s$, we have the *logarithmic embedding*,

$$\mathrm{Log} : L^* \to \mathbb{R}^{r+s}, \quad \alpha \mapsto (\log(|\sigma_1(\alpha)|), \ldots, \log(|\sigma_{r+s}(\alpha)|)) .$$

It was remarked that since $h$ is small it follows that $\mathrm{Log}(g) = \mathrm{Log}(hu)$ lies close to the log-unit lattice $\mathrm{Log}(\mathcal{R}^*)$ [8, 15]. Using this observation, a polynomial-time algorithm for cyclotomic number fields with power-of-two conductor was found [15]. A generalization to prime-power cyclotomic number fields accompanied with a rigorous proof was given in [19]. Moreover, strong evidence was found that these types of attacks are not restricted to principal ideals [20, 21].

Fortunately, only a handful of cryptographic primitives [48, 30, 33, 15] rely directly on the hardness of the *Short Generator Principal Ideal Problem* (SG-PIP) and are therefore broken by this type of attack.

In addition, Bernstein [8] warned against the possibility of exploiting subfields. Subfield lattice attacks were originally proposed in [31] and generalized in [1]. The resulting attacks run in subexponential time and affect the asymptotic security of some fully homomorphic encryption schemes.

The main conclusion that can be drawn from these attacks is that some lattices contain structure that can be exploited by an attacker, thereby challenging the assumption that solving lattice problems for structured lattices is as hard as solving them for unstructured ones.

One approach to mitigate these potential threats is to define cryptographic schemes over unstructured lattices [13, 49]. Another approach is to only use number fields that contain no non-trivial subfields [9, 2]. Bernstein [8] proposed to define protocols over the trinomial number field $L = \mathbb{Q}[X]/(f(X))$ with $f = X^n - X - 1$ ($n$ prime) irreducible. Because $n$ is prime, $L$ has no proper subfields thereby ruling out subfield attacks. Moreover, the Galois group of $L$ is the non-Abelian group of permutations $S_n$ [43], i.e., it is maximal. Hence, $L$ does not have a lot of automorphisms and it is not contained in a cyclotomic number field. Additionally, [9] recommends the use of primes $p$ that are inert in $L$ to avoid the existence of homomorphisms from $O_L/pO_L$ to smaller rings. Such homomorphisms have been used to break specific instances of Ring-LWE based cryptosystems [16]. In this work, we consider the more general situation in which $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ ($k < n$) is an irreducible trinomial.

## 1.1 CONTRIBUTIONS

In this work we slightly reformulate Theorem 1 of [41] to obtain Theorem 2. The main difference is that we omit the explicit factorization of cyclotomic polynomials. Given the adapted invertibility theorem, the contributions of this work are summarized below.

1. The reformulation of Theorem 1 induces a simplified proof that follows from standard Galois theory. More precisely, we recognize the implicit use of decomposition fields in [41]. This observation immediately relates the invertibility of ring elements to their algebraic norms. From this observation the desired invertibility result follows naturally. This approach obviates the need for expressing ring elements, and a related lattice, explicitly. The reformulated theorem and its proof are given in Section 3.
2. In [41], it was additionally proven that there exist infinitely many primes satisfying the invertibility conditions of Theorem 1 and Theorem 2. We strengthen this result in two ways. First, we relax the conditions making it

more generally applicable. Second, instead of merely proving the existence of (infinitely many) primes, we determine the density of primes satisfying certain conditions, thereby enhancing the practical applicability. Our strengthened result is given in Lemma 3.

3. Theorem 2 induces a natural generalization from cyclotomic number fields to arbitrary number fields $L$. In Section 4, we present the generalization of Theorem 2 together with the modifications required for its proof. For readability the generalization is presented in two different theorems; Theorem 3 and Theorem 4.
4. The invertibility conditions of Section 3 and Section 4 are defined via the so-called coefficient embedding of the number field $L$. However, the proofs of the corresponding theorems suggest an alternative approach that, in some cases, results in better protocol parameters. More precisely, an alternative invertibility condition can be obtained via the canonical embedding of the number field $L$. We generalize this invertibility condition to norms $\|\cdot\|_k$ for arbitrary $k \in \mathbb{N} \cup \{\infty\}$. The alternative invertibility conditions are presented in Section 5.
5. The coefficient and the canonical embedding of the number field $L$ both equip the number field $L$ with a geometry. However, these geometries might differ. This difference is extremely important for the hardness of the underlying lattice problems and it can be quantified by certain singular values. Moreover, the invertibility results of Section 3 and Section 4 depend on the size of these singular values. For this reason, we study the singular values associated to cyclotomic and trinomial number fields in Section 6. In particular, we prove an upper-bound for certain cyclotomic singular values that was conjectured in [41].
6. Finally, in Section 7, we apply the invertibility result to construct challenge sets in a cyclotomic and a trinomial number field. We show that using the canonical embedding and defining challenges via the $\ell_1$-norm allows protocols to be instantiated with slightly smaller rational primes $p$.

# 2 PRELIMINARIES

## 2.1 NUMBER FIELDS

Let $L/\mathbb{Q}$ be a number field of degree $n$ with ring of integers $\mathcal{O}_L$ and integral basis $B = (\beta_1, \dots, \beta_n)$. The ring of integers $\mathcal{O}_L$ is the maximal order of $L$. In general, an order $\mathcal{O}$ of $L$ is a subring of $\mathcal{O}_L$ that spans $L$ over $\mathbb{Q}$, i.e., $\mathcal{O}$ contains a basis of $L/\mathbb{Q}$.

The coefficient embedding

$$\psi_B : L \to \mathbb{Q}^n, \quad \sum_{i=1}^{n} y_i \beta_i \mapsto \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \tag{1}$$

equips $L$ with a geometry, i.e., $\|\gamma\| := \|\psi_B(\gamma)\|$ for any norm $\|\cdot\|$ on $\mathbb{R}^n$. If not indicated otherwise, $\|\cdot\|$ is the $\ell_2$-norm. Note that $\psi_B$ depends on the basis $B$.

The field $L/\mathbb{Q}$ has $n$ complex embeddings $\sigma_i : L \to \mathbb{C}$. Given these complex embeddings, the canonical embedding is defined as follows:

$$\phi_L : L \to \mathbb{C}^n, \quad \gamma \mapsto \begin{pmatrix} \sigma_1(\gamma) \\ \vdots \\ \sigma_n(\gamma) \end{pmatrix}.$$

If $\sigma_i(L) \subset L$ for all $i$ we say $L/\mathbb{Q}$ is a Galois extension with a Galois group of automorphisms $G = \{\sigma_i : L \to L\}$.

The image $\phi_L(L) \subset \mathbb{C}^n$ is an $n$-dimensional $\mathbb{R}$-vector space denoted by $L_{\mathbb{C}}$. Moreover, $\phi_L(\mathcal{O}_L)$ is a full-rank lattice in $L_{\mathbb{C}}$ [42, Section 1.5]. The canonical embedding equips $L$ with another geometry that is independent of the basis $B$ of $L/\mathbb{Q}$. The relation between the coefficient and canonical embedding is depicted in Figure 1, where $\mathrm{M}_B$ is the unique linear mapping that makes this diagram commute. Hence, the matrix $\mathrm{M}_B$ is given by

$$\mathrm{M}_B = \left(\sigma_i(\beta_j)\right)_{1 \le i,j \le n} \in L^{n \times n}.$$

We let $s_1(\mathrm{M}_B)$ denote the largest singular value of $\mathrm{M}_B$, i.e.,

$$s_1(B) = \max_{u \in \mathbb{C}^n \setminus \{0\}} \frac{\|\mathrm{M}_B\, u\|}{\|u\|}.$$

Further, for a tower $\mathbb{Q} \subset K \subset L$ of number fields we have the following usefull lemma.

**Lemma 1.** *Let $\mathbb{Q} \subset K \subset L$ be a tower of number fields such that $\mathcal{O}_L = \beta_1 \mathcal{O}_K + \cdots + \beta_\ell \mathcal{O}_K$ for an integral basis $(\beta_1, \dots, \beta_\ell)$ of $L/K$. For $1 \le j \le \ell$, let the projection $\pi_j$ be defined as follows*

$$\pi_j : L \to K, \quad \gamma = \sum_{i=1}^{\ell} \gamma_i \beta_i \mapsto \gamma_j.$$

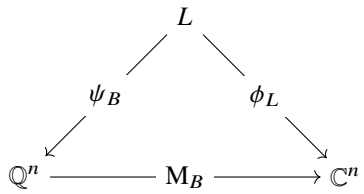


Figure 1: Coefficient and canonical embedding of $L/\mathbb{Q}$.

*Let $I$ be an ideal of $\mathcal{O}_K$. Then, for any $\gamma \in L$,*

$$\pi_j(\gamma) \in I \ \ \forall j \quad \Longleftrightarrow \quad \gamma \in I\mathcal{O}_L.$$

*Proof.* First, let $\gamma \in \mathcal{O}_L$ such that $\pi_j(\gamma) \in I$ for all $1 \le j \le \ell$. Then $\gamma = \sum_{j=1}^{\ell} \pi_j(\gamma)\beta_j$ with $\beta_j \in \mathcal{O}_L$. Hence, $\gamma \in I\mathcal{O}_L$, which proves the first implication.

Now let $\gamma \in I\mathcal{O}_L$, i.e., $\gamma = \sum_{i=1}^{k} a_i b_i$ for some $k \in \mathbb{N}$, $a_i \in I$ and $b_i \in \mathcal{O}_L$. Since $b_i \in \mathcal{O}_L$, it follows that $b_i = \sum_{j=1}^{\ell} b_{i,j}\beta_j$ for some $b_{i,j} \in \mathcal{O}_K$. Hence,

$$\gamma = \sum_{i=1}^{k} a_i \sum_{j=1}^{\ell} b_{i,j}\beta_j = \sum_{j=1}^{\ell} \beta_j \sum_{i=1}^{k} a_i b_{i,j}.$$

Therefore, for all $j$, $\pi_j(\gamma) = \sum_{i=1}^{k} a_i b_{i,j}$ with $a_i \in I$ and $b_{i,j} \in \mathcal{O}_K$. Hence, $\pi_j(\gamma) \in I$, which proves the second implication and completes the proof. □

**Remark 1.** *Lemma 1 assumes that the ring of integers $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module, i.e., $\mathcal{O}_L = \beta_1\mathcal{O}_K + \cdots + \beta_\ell\mathcal{O}_K$ for some $\beta_1, \ldots, \beta_\ell \in \mathcal{O}_L$. However, there exist towers of number fields $\mathbb{Q} \subset K \subset L$ for which $\mathcal{O}_L$ is not a free $\mathcal{O}_K$-module.*

## 2.2 CYCLOTOMIC NUMBER FIELDS

We are particularly interested in number fields $L = \mathbb{Q}(\zeta_m)$, where $\zeta_m$ is an $m^{th}$-primitive root of unity. We say $L$ is a cyclotomic number field of conductor $m$. Without loss of generality we assume the primitive roots of unity to satisfy $\zeta_k\zeta_l = \zeta_{kl}$ for all $k, l \in \mathbb{N}$ that are relatively prime and that $\zeta_z = \zeta_m^{m/z}$ for all $z \mid m$. The degree of $L$ over $\mathbb{Q}$ is $n = \varphi(m)$, where $\varphi$ is the Euler totient function. The field extension $L/\mathbb{Q}$ is Galois and it has integral (power) basis $B_m = \left(1, \ldots, \zeta_m^{\varphi(m)-1}\right)$. We will typically fix this power basis. In this case, we write $\psi_m := \psi_{B_m}$, $\mathrm{M}_m := \mathrm{M}_{B_m}$ and $s_1(m) := s_1(B_m)$.

Furthermore, for any $z \mid m$, we define $B_m^z = \left(1, \ldots, \zeta_m^{\varphi(m)/\varphi(z)-1}\right)$ as an integral basis for $L$ over $K = \mathbb{Q}(\zeta_z)$. The basis $B_m^z$ gives rise to natural projections

$$\pi_j \colon L \to K, \quad \sum_{i=0}^{\varphi(m)/\varphi(z)-1} \gamma_i \zeta_m^i \mapsto \gamma_j \quad (0 \le j \le \varphi(m)/\varphi(z) - 1)\,. \tag{2}$$

By Lemma 1, for all ideals $I$ of $K$ and for all $\gamma \in L$ it holds that

$$\pi_j(\gamma) = 0 \mod I \ \ \forall j \quad \Longleftrightarrow \quad \gamma = 0 \mod I\mathcal{O}_L.$$

Recall that the radical of an integer $n$ is given by

$$\mathrm{rad}(n) = \prod_{p \mid n,\ p \text{ prime}} p.$$

The following lemma shows that, for conductors $z \mid m$ with $\mathrm{rad}(m) = \mathrm{rad}(z)$, the coefficient embedding $\psi_m$ factors through $K^{m/z}$.

**Lemma 2.** *Let $m, z \in \mathbb{N}$, with $z|m$ and $\mathrm{rad}(m) = \mathrm{rad}(z)$, and let $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}(\zeta_z)$. Then the canonical embedding $\psi_m : L \to \mathbb{Q}^{\varphi(m)}$ factors through $K^{m/z}$. More precisely,*

$$\psi_m = \begin{pmatrix} \psi_z \circ \pi_0 \\ \vdots \\ \psi_z \circ \pi_{m/z-1} \end{pmatrix},$$

*where $\psi_m : L \to \mathbb{Q}^{\varphi(m)}$ and $\psi_z : K \to \mathbb{Q}^{\varphi(z)}$ are as defined in Equation 1 and $\pi_j : L \to K$ ($0 \leq j \leq m/z - 1$) are as defined in Equation 2.*

*Proof.* Recall that $B_z$, $B_m^z$ and $B_m$ are integral bases of $K/\mathbb{Q}$, $L/K$ and $L/\mathbb{Q}$, respectively, where

$$\begin{aligned} B_z &= (1, \zeta_z, \ldots, \zeta_z^{\varphi(z)-1}), \\ B_m^z &= (1, \zeta_m, \ldots, \zeta_m^{\varphi(m)/\varphi(z)-1}), \\ B_m &= (1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}). \end{aligned}$$

By assumption $\zeta_z = \zeta_m^{m/z}$ and, since $\mathrm{rad}(m) = \mathrm{rad}(z)$, $m/z = \varphi(m)/\varphi(z)$. Hence, it holds that $B_m = B_z \otimes B_z^m$, where $\otimes$ denotes the Kronecker product, and

$$\psi_m = \begin{pmatrix} \psi_z \circ \pi_0 \\ \vdots \\ \psi_z \circ \pi_{m/z-1} \end{pmatrix} : L \to \mathbb{Q}^{\varphi(m)},$$

which proves the lemma. □

Lemma 2 immediately implies the following useful corollary.

**Corollary 1.** *Let $m, z \in \mathbb{N}$, with $z|m$ and $\mathrm{rad}(m) = \mathrm{rad}(z)$, and let $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}(\zeta_z)$. Then, for any $\gamma \in L$ and $\alpha \in \mathbb{R}_{>0}$,*

$$\|\gamma\|_\infty \leq \alpha \quad \Longrightarrow \quad \left\|\pi_j(\gamma)\right\| < \varphi(z)\alpha \quad \forall 1 \leq j \leq m/z, \tag{3}$$

*where the projections $\pi_j : L \to K$ are as defined in Equation 2.*

**Remark 2.** *Lemma 2 and Corollary 1 crucially depend on the condition that $\mathrm{rad}(m) = \mathrm{rad}(z)$. In particular, if $\mathrm{rad}(m) \neq \mathrm{rad}(z)$ the equality $B_m = B_z \otimes B_z^m$ and the implication of Equation 3 do not hold.*

### 2.3 DECOMPOSITION FIELDS

Let $L/\mathbb{Q}$ be a Galois extension with Galois group $G$ and let $\mathfrak{p}$ be a prime ideal of $O_L$. The decomposition group $D_\mathfrak{p}$ is the subgroup of automorphisms in $G$ that fix $\mathfrak{p}$, i.e., $D_\mathfrak{p} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\}$. Its fixed field $L^{D_\mathfrak{p}}$ is called the decomposition field of $\mathfrak{p}$ and it is the largest subfield of $L$ in which the rational prime ideal $(p) = \mathfrak{p} \cap \mathbb{Q}$ completely splits. Decomposition fields allow us to represent a Galois extension $L/\mathbb{Q}$ as a tower of field extensions with well-understood splitting behavior of the primes under $\mathfrak{p}$. For simplicity let us assume that $p$ is unramified in $L$. Then we have the following tower of fields $\mathbb{Q} \subset L^{D_\mathfrak{p}} \subset L$, where the rational prime $(p)$ completely splits in $L^{D_\mathfrak{p}}$ and the prime $\mathfrak{p} \cap L^{D_\mathfrak{p}}$ of $L^{D_\mathfrak{p}}$ is inert in $L$.

The subgroups $D_\mathfrak{p}$ and $D_\mathfrak{q}$ are conjugate in $G$ for any two primes $\mathfrak{p}, \mathfrak{q} \subset O_L$ over the prime $p \in \mathbb{Q}$, i.e., $\mathfrak{p} \cap \mathbb{Q} = (p) = \mathfrak{q} \cap \mathbb{Q}$. Hence, if $G$ is Abelian it holds that $D_\mathfrak{p} = D_\mathfrak{q}$ and we can define $D_p := D_\mathfrak{p}$ for any $\mathfrak{p}|(p)$. In this case, we also speak of decomposition groups and fields of primes $p$ in $\mathbb{Q}$ rather than of primes $\mathfrak{p}$ in $L$. For more details on decomposition fields see [32, Chapter VII].

Let us now consider the cyclotomic case $L = \mathbb{Q}(\zeta_m)$. We aim to specify the rational primes $p$ with cyclotomic decomposition fields in $L$. The extension $L/\mathbb{Q}$ is Galois with an Abelian Galois group $G \cong (\mathbb{Z}/m\mathbb{Z})^*$. Let $z|m$ and let $p \nmid m$ be a rational prime with $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z)$, i.e., $\varphi(m)/\varphi(z)$ is the smallest positive integer such that $p^{\varphi(m)/\varphi(z)} = 1 \mod m$. Then $p$ splits into $\varphi(z)$ distinct primes in $L$ [52, Theorem 2.13]. Hence, the decomposition field $L^{D_p}$ is of degree $\varphi(z)$ over $\mathbb{Q}$. However, this does not necessarily imply that $L^{D_p}$ is cyclotomic. If, in addition, $p = 1 \mod z$, we find that $p$ splits in $\varphi(z)$ distinct factors, hence completely, in $\mathbb{Q}(\zeta_z) \subset L$. Hence, in this case $\mathbb{Q}(\zeta_z) = L^{D_p}$ is the decomposition field of $p$. Altogether, it follows that if $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z)$ and $p = 1 \mod z$ then the decomposition field of $p$ in $\mathbb{Q}(\zeta_m)$ is $\mathbb{Q}(\zeta_z)$.

## 3 INVERTIBILITY IN CYCLOTOMIC NUMBER FIELDS

We are now ready to prove the following adaptation of Theorem 1 from [41].

**Theorem 2** (Invertibility - Adaptation of Theorem 1)**.** *Let $O_L$ be the ring of integers in a cyclotomic number field $L = \mathbb{Q}(\zeta_m)$ of conductor $m$, let $z \mid m$ with $\mathrm{rad}(z) = \mathrm{rad}(m)$ and let $p$ be a rational prime with $p = 1 \mod z$ and $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z)$. Then any $\gamma \in O_L$ that satisfies either*

$$0 < \|\gamma\| < \frac{\sqrt{\varphi(m)}}{s_1(m)} p^{1/\varphi(z)} \tag{4}$$

*or*

$$0 < \|\gamma\|_\infty < \frac{1}{s_1(z)} p^{1/\varphi(z)} \tag{5}$$

*has a multiplicative inverse in* $O_L/pO_L$.

*Proof.* We first prove that inequality 4 gives a sufficient condition for $\gamma \in O_L$ to be invertible in $O_L/pO_L$. For any $\gamma \in O_L$ it follows, by the inequality of the arithmetic and the geometric mean, that

$$\left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right|^{2/\varphi(m)} \leq \frac{1}{\varphi(m)} \left\|\mathrm{M}_m \cdot \psi_m(\gamma)\right\|^2 .$$

Hence, by definition of $s_1(m)$,

$$\left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right|^{2/\varphi(m)} \leq \frac{s_1(m)^2}{\varphi(m)} \left\|\psi_m(\gamma)\right\|^2 = \frac{s_1(m)^2}{\varphi(m)} \|\gamma\|^2 . \tag{6}$$

Now suppose that Equation 4 holds. Substituting this equation in the inequality of Equation 6 and raising both sides to the power $\varphi(m)/2$ gives

$$0 < \left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right| < p^{\varphi(m)/\varphi(z)}.$$

Since $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z)$, it follows that the inertia degree of any prime $\mathfrak{p}$ above $p$ equals $\varphi(m)/\varphi(z)$ and thus $\mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p}) = p^{\varphi(m)/\varphi(z)}$. So if $\gamma$ satisfies Equation 4, it holds that

$$0 < \left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right| < \mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p}),$$

for all primes $\mathfrak{p} \subset O_L$ above $p$. Therefore $\gamma \notin \mathfrak{p}$ and $\gamma \in (O_L/\mathfrak{p})^*$ for all $\mathfrak{p} \mid p$. Hence, $\gamma$ is invertible in $O_L/pO_L$, which proves the first claim.

We now prove that, if $\mathrm{rad}(m) = \mathrm{rad}(z)$, then Equation 5 gives a sufficient condition for $\gamma$ to be invertible in $O_L/pO_L$. First note that $\mathrm{rad}(m) = \mathrm{rad}(z)$ implies that $\varphi(m)/\varphi(z) = m/z$. Now let $\mathfrak{p} \subset L$ be a prime above $p$ and let $K = \mathbb{Q}(\zeta_z) \subset L$. Since $p = 1 \mod z$ and $\mathrm{ord}_m(p) = m/z$, the decomposition field of $\mathfrak{p}$ is $K$ and the prime $\mathfrak{P} = \mathfrak{p} \cap K$ is inert in $L$, i.e., $\mathfrak{p} = \mathfrak{P}O_L$. Note in particular that $p \nmid m$, hence $p$ is unramified in $L$.

Let $\pi_j : K \to L$ for $0 \leq j \leq \varphi(m)/\varphi(z) - 1 = m/z - 1$ be the projections associated to basis $B_m^z$ of $L$ over $K$ and let $\gamma$ be such that it satisfies Equation 5. We will show that there exists a $j$ such that $\pi_j(\gamma) \in (O_K/\mathfrak{P})^*$ from which it follows that $\gamma \in (O_L/\mathfrak{p})^*$.

Since

$$0 < \|\gamma\|_\infty < \frac{1}{s_1(z)} p^{1/\varphi(z)},$$

and by Corollary 1, for all $j$ it holds that

$$\left\|\pi_j(\gamma)\right\| < \frac{\sqrt{\varphi(z)}}{s_1(z)} p^{1/\varphi(z)}.$$

Moreover, $\pi_j(\gamma) \neq 0$ for at least one $j$. For this $j$ we find, similar to the first part of this proof, that

$$0 < \left|\mathrm{N}_{K/\mathbb{Q}}(\pi_j(\gamma))\right| < \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}),$$

and therefore that $\pi_j(\gamma) \notin \mathfrak{P}$. By Lemma 1, $\gamma \notin \mathfrak{P}O_L = \mathfrak{p}$, and, hence, $\gamma \in (O_L/\mathfrak{p})^*$. Since $p$ is unramified in $L$ and $\mathfrak{p} \mid p$ was arbitrary, it follows that $\gamma \in (O_L/pO_L)^*$, which proves the second and final part of the theorem. □

**Remark 3.** *The proof of Theorem 2 shows that the second invertibility condition can be replaced by a stronger one. More precisely, if all the prerequisites of the theorem are satisfied, any* $\gamma \in O_L$ *that satisfies*

$$0 < \pi_j(\gamma) < \frac{\sqrt{\varphi(z)}}{s_1(z)} p^{1/\varphi(z)} \tag{7}$$

*for some* $1 \leq j \leq m/z - 1$, *has a multiplicative inverse in* $O_L/pO_L$. *Here,* $\pi_j : \mathbb{Q}(\zeta_m) \to \mathbb{Q}(\zeta_z)$ *are the projections defined in Equation 2.*

**Remark 4.** *The first invertibility condition of Theorem 2 (Equation 5) does not require that* $\mathrm{rad}(z) = \mathrm{rad}(m)$ *and* $p = 1 \mod z$. *The prerequisite* $\mathrm{rad}(z) = \mathrm{rad}(m)$ *ensures that the coefficient embedding factors through* $\mathbb{Q}(\zeta_z)$ *(Lemma 2). Using this fact, the second invertibility condition can be obtained from bounds on the projections* $\pi_j : \mathbb{Q}(\zeta_m) \to \mathbb{Q}(\zeta_z)$ *of* $\gamma \in O_L$. *The prerequisite* $p = 1 \mod z$ *ensures that the decomposition field of* $p$ *is* $\mathbb{Q}(\zeta_z)$, *allowing the invertibility condition to be expressed in terms of the largest singular value* $s_1(z)$ *instead of* $s_1(m)$. *The theorem can therefore be slightly strengthened by requiring these two prerequisites only for the second invertibility condition.*

The second invertibility condition of Theorem 2 crucially depends on the fact that $p$ has a cyclotomic decomposition field $\mathbb{Q}(\zeta_z)$. For this reason, we also refer to this invertibility condition as the *decomposition field approach*.

Next, we prove the existence of primes $p$ satisfying the conditions in Theorem 2, i.e., primes that have cyclotomic decomposition field $\mathbb{Q}(\zeta_z)$ in $\mathbb{Q}(\zeta_m)$. The following lemma gives sufficient conditions for the existence of infinitely many primes $p$ satisfying the conditions of Theorem 2. A similar result was given in Theorem 2.5 of [41]. However, we strengthen their result in two ways. First, we relax the conditions on the conductors $m$ and $z$. Second, instead of merely proving the existence of primes, we give the density of primes satisfying certain conditions. The experimental results of [41] indeed validate the exact densities given by the following lemma.

**Lemma 3** (Density of Primes with Cyclotomic Decomposition Field)**.** *Let $z \mid m$ be integers such that $2 \mid m$ implies that $4 \mid z$. Let $\delta(m,z)$ be the density of primes $p$ such that $p = 1 \mod z$ and $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z)$, i.e., the primes $p$ with decomposition field $\mathbb{Q}(\zeta_z)$ in $\mathbb{Q}(\zeta_m)$. Then*

$$\delta(m,z) = \begin{cases} \dfrac{\varphi(m/z)}{\varphi(m)}, & \text{if } \mathrm{rad}(m) = \mathrm{rad}(z), \\ \dfrac{\varphi\left(\varphi(m)/\varphi(z)\right)}{\varphi(m)}, & \text{if } \dfrac{\mathrm{rad}(m)}{\mathrm{rad}(z)} = p \text{ is prime, and } \gcd\left(p-1, \dfrac{m}{z}\right) = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

*Proof.* Let $m = \prod_{i=1}^{g} p_i^{e_i}$ and $z = \prod_{i=1}^{g} p_i^{f_i}$ with $0 \le f_i \le e_i$ and $e_i > 0$ be the prime factorizations of $m$ and $z$. Since $z \mid m$, we have the following well-defined exact sequence

$$0 \longrightarrow \mathrm{Ker} \longrightarrow (\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\psi} (\mathbb{Z}/z\mathbb{Z})^* \longrightarrow 1,$$

with $\psi(x) = x \mod z$ and $\mathrm{Ker} = \ker(\psi) = \{x \in (\mathbb{Z}/m\mathbb{Z})^* : x = 1 \mod z\}$. The elements of Ker of order $\varphi(m)/\varphi(z)$ are precisely the elements we are interested in. So let us determine the number of elements with these properties.

To this end, note that

$$\mathrm{Ker} \cong (\mathbb{Z}/m\mathbb{Z})^* / (\mathbb{Z}/z\mathbb{Z})^* \cong \prod_{i=1}^{g} \left(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\right)^* / \left(\mathbb{Z}/p_i^{f_i}\mathbb{Z}\right)^*.$$

Moreover, for all $i$ with $f_i \ge 1$,

$$\left(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\right)^* / \left(\mathbb{Z}/p_i^{f_i}\mathbb{Z}\right)^* \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e_i - f_i - 1}\mathbb{Z}, & \text{if } \quad p_i = 2,\ e_i > 2 \text{ and } f_i = 1, \\ \mathbb{Z}/p_i^{e_i - f_i}\mathbb{Z}, & \text{otherwise.} \end{cases}$$

Since $2 \mid m$ implies that $4 \mid z$, it follows that if there exists an $i$ with $p_i = 2$, then $f_i \ge 2$. Hence,

$$\mathrm{Ker} \cong \prod_{i:f_i \ge 1} \mathbb{Z}/p_i^{e_i - f_i}\mathbb{Z} \prod_{i:f_i = 0} \left(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\right)^*,$$

where the factors in this decomposition are all cyclic. Therefore, Ker is cyclic if the orders of these factors are coprime.

Let us now consider the cases for which Ker is cyclic. First, Ker is cyclic if $S := \{p_i : f_i = 0\} = \emptyset$, or equivalently if $\mathrm{rad}(m) = \mathrm{rad}(z)$. Second, note that all factors of the product

$$\prod_{i:f_i = 0} \left(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\right)^*$$

have orders divisible by 2. Therefore, if $S \neq \emptyset$, Ker can only be cyclic if $S = \{p\}$ for some prime $p$, or equivalently if $\mathrm{rad}(m)/\mathrm{rad}(z) = p$. Note that $p \neq 2$, because $2 \mid m$ implies that $4 \mid z$. Hence, in this case Ker is cyclic if $\gcd(p-1, m/z) = 1$, i.e., if there are no common divisors in the orders of the cyclic factors of Ker. This proves that Ker is cyclic *only* in the first two cases of Equation 8.

The order of Ker is $\varphi(m)/\varphi(z)$, which equals $m/z$ if $\mathrm{rad}(m) = \mathrm{rad}(z)$. Hence, if it is cyclic it contains exactly $\varphi(\varphi(m)/\varphi(z))$ generators. By Dirichlet's theorem on arithmetic progressions the lemma now follows. □

**Remark 5.** *The densities of Lemma 3 do not necessarily sum to* 1*. The reason is that this lemma only considers the primes with a cyclotomic decomposition field $\mathbb{Q}(\zeta_z)$ in $\mathbb{Q}(\zeta_m)$. There may also exist primes for which the decomposition field is not cyclotomic, i.e., primes with $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z)$ but $p \neq 1 \mod z$.*

# 4 GENERALIZATION TO ARBITRARY NUMBER FIELDS

Our proof of Theorem 2 paves the road to a generalization from the ring of integers in a cyclotomic number field to arbitrary orders $\mathcal{O}$ in arbitrary number fields $L$. In this section, we therefore prove a generalized invertibility result.

To this end, we first introduce some (generalized) notation. For an integral basis $B_{L/\mathbb{Q}} = (\beta_1, \dots, \beta_n)$ of $L/\mathbb{Q}$, let us define the matrix

$$\mathrm{M}(B_{L/\mathbb{Q}}) := \left(\sigma_i(\beta_j)\right)_{1 \le i,j \le n} \in \mathbb{C}^{n \times n}, \tag{9}$$

where $\sigma_i : L \to \mathbb{C}$ are the complex embeddings of $L$. Moreover, we define $s_1(B_{L/\mathbb{Q}})$ to be the largest singular value associated to this matrix, i.e.,

$$s_1(B_{L/\mathbb{Q}}) := s_1(\mathrm{M}(B_{L/\mathbb{Q}})).$$

In the cyclotomic case we inherited an Euclidean norm from the coefficient embedding that in turn was defined by the choice of basis $B_m = \left(1, \zeta_m, \dots, \zeta_m^{\varphi(m)-1}\right)$. This cyclotomic basis has the useful property that for all $z \mid m$ with $\mathrm{rad}(m) = \mathrm{rad}(z)$, there exists a basis $B_m^z$ of $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_z)$ such that $B_m = B_m^z \otimes B_z$. Recall that $\otimes$ denotes the Kronecker product. For general number fields $K \subset L$, and arbitrary bases $B_{L/\mathbb{Q}}$, we can not expect the existence of bases of $K/\mathbb{Q}$ and $L/K$ with this convenient property. For this reason we make the dependence of the norm on the basis $B_{L/\mathbb{Q}} = (\beta_1, \dots, \beta_n)$ explicit and denote by $||\cdot||_{B_{L/\mathbb{Q}}}$ the $\ell_2$-norm associated to the coefficient embedding

$$\psi_{B_{L/\mathbb{Q}}} \colon L \to \mathbb{Q}^n, \quad \sum_{i=1}^{n} y_i \beta_i \mapsto \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

For the ease of notation we present the generalization of Theorem 2 in two different theorems. Theorem 3 generalizes the first and Theorem 4 generalizes the second invertibility condition of Theorem 2. The proofs are analogous to the proof of Section 3. However, we are required to handle a number of subtleties.

First, the extension $L/\mathbb{Q}$ is not necessarily a Galois extension. When $L/\mathbb{Q}$ is not Galois, the primes $\mathfrak{p}$ above a rational prime $p$ can have different inertia degrees and ramification indices.

Second, in contrast to the ring of integers $\mathcal{O}_L$, an order $\mathcal{O}$ might not be a unique factorization domain. For this reason, we must be careful when considering factorizations of ideals in $\mathcal{O}$. Fortunately, the following lemma shows that invertibility in $\mathcal{O}_L/p\mathcal{O}_L$ implies invertibility $\mathcal{O}/p\mathcal{O}$, i.e., we merely have to consider factorizations in the unique factorization domain $\mathcal{O}_L$.

**Lemma 4.** *Let $\mathcal{O} \subset \mathcal{O}_L$ be an order in a number field $L$ and let $\alpha, \gamma \in \mathcal{O}$. Then $\gamma \in (\mathcal{O}/\alpha\mathcal{O})^*$ if and only if $\gamma \in (\mathcal{O}_L/\alpha\mathcal{O}_L)^*$.*

*Proof.* First note that,

$$\gamma \in \mathcal{O}^* \quad \Longleftrightarrow \quad |\mathcal{O}/\gamma\mathcal{O}| = \mathrm{N}_{L/\mathbb{Q}}(\gamma) = 1 \quad \Longleftrightarrow \quad \gamma \in \mathcal{O}_L^*.$$

From this it follows that

$$\begin{aligned} \gamma \in (\mathcal{O}_L/\alpha\mathcal{O}_L)^* &\iff \mathcal{O}_L = \gamma\mathcal{O}_L + \alpha\mathcal{O}_L = (\gamma\mathcal{O} + \alpha\mathcal{O})\mathcal{O}_L, \\ &\iff \exists x \in (\gamma\mathcal{O} + \alpha\mathcal{O}) \cap \mathcal{O}_L^* = (\gamma\mathcal{O} + \alpha\mathcal{O}) \cap \mathcal{O}^*, \\ &\iff \gamma\mathcal{O} + \alpha\mathcal{O} = \mathcal{O}, \\ &\iff \gamma \in (\mathcal{O}/\alpha\mathcal{O})^*, \end{aligned}$$

which proves the lemma. □

**Remark 6.** *If the ideal $\alpha\mathcal{O}$ is relatively prime to the conductor $\mathfrak{f}_\mathcal{O} = \{\gamma \in \mathcal{O}_L : \gamma\mathcal{O}_L \subset \mathcal{O}\}$ of $\mathcal{O}$, it can be shown that $\alpha\mathcal{O} = \alpha\mathcal{O}_K \cap \mathcal{O}$ and $\mathcal{O}/\alpha\mathcal{O} \cong \mathcal{O}_L/\alpha\mathcal{O}_L$. However, in general this is not the case.*

We are now ready to prove the following generalization of the first invertibility condition of Theorem 2.

**Theorem 3** (Invertibility of Integral Elements)**.** *Let $L/\mathbb{Q}$ be a number field of degree $n$ containing an order $\mathcal{O} \subset \mathcal{O}_L$ with $\mathbb{Z}$-basis $B_{L/\mathbb{Q}}$. Further, let $p$ be a rational prime such that $p\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i$, where $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_L$ with inertia degree $f_i$ for all $i$. Then any $\gamma \in \mathcal{O}$ that satisfies*

$$0 < ||\gamma||_{B_{L/\mathbb{Q}}} < \frac{\sqrt{n}}{s_1(B_{L/\mathbb{Q}})} p^{\min_{1 \le i \le g} f_i/n}, \tag{10}$$

*has a multiplicative inverse in $\mathcal{O}/p\mathcal{O}$.*

*Proof.* We prove that inequality 10 gives a sufficient condition for $\gamma \in O/pO$ to be invertible. For any $\gamma \in O \subset O_L$ it follows, by the inequality of the arithmetic and the geometric mean, that

$$\left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right|^{2/n} \leq \frac{1}{n}\left\|\mathrm{M}(B_{L/\mathbb{Q}}) \cdot \psi_{B_{L/\mathbb{Q}}}(\gamma)\right\|^2 .$$

Hence, by definition of $s_1(B_{L/\mathbb{Q}})$,

$$\left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right|^{2/n} \leq \frac{s_1(B_{L/\mathbb{Q}})^2}{n}\left\|\psi_{B_{L/\mathbb{Q}}}(\gamma)\right\|^2 = \frac{s_1(B_{L/\mathbb{Q}})^2}{n}\|\gamma\|^2_{B_{L/\mathbb{Q}}} . \tag{11}$$

Substituting Equation 10 in the inequality of Equation 11 and raising both sides to the power $n/2$ gives

$$0 < \left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right| < p^{\min_{1\leq i\leq g} f_i} = \min_{1\leq i\leq g} \mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p}_i) .$$

Hence, $\gamma \notin \mathfrak{p}_i$ and $\gamma \in (O_L/\mathfrak{p}_i)^*$ for all $1 \leq i \leq g$. Therefore, $\gamma$ is invertible in $O_L/pO_L$. By Lemma 4 this implies that $\gamma \in (O/pO)^*$, which proves the theorem. □

To generalize the second invertibility condition of Theorem 2 we must restrict to Galois extensions. Moreover, we assume that the Galois group is Abelian. In this case, primes $\mathfrak{p} \subset O_L$ above the rational prime $p$ all have the same decomposition field and therefore the decomposition field of $p$ is well-defined. Furthermore, we assume that the order $O$ is free over $O_K$, i.e., $O = \beta_1 O_K + \cdots \beta_f O_K$ for some basis $(\beta_1, \ldots, \beta_f)$ of $L/K$. In general, such a basis does not need to exist (see also Remark 1).

**Theorem 4** (Decomposition Field Invertibility Condition)**.** *Let $L/\mathbb{Q}$ be an Abelian Galois extension of degree $n$ containing an order $O \subset O_L$. Moreover, let $p$ be a rational prime that is unramified in $L$ and splits in $g$ factors of inertia degree $f = n/g$. Let $K$ be the decomposition field of $p$ with integral basis $B_{K/\mathbb{Q}}$, and assume that $O = \beta_1 O_K + \cdots \beta_f O_K$ with $\beta_j \in O_L$. Let $\pi_j$ denote the projections associated to basis $(\beta_1, \ldots, \beta_f)$ of $L/K$, i.e., $\gamma = \sum_{j=1}^{f} \pi_j(\gamma)\beta_j$ for all $\gamma \in L$.*

*Then any $\gamma \in O$ that satisfies*

$$0 < \left\|\pi_j(\gamma)\right\|_{B_{K/\mathbb{Q}}} < \frac{\sqrt{g}}{s_1(B_{K/\mathbb{Q}})} p^{1/g} \tag{12}$$

*for some $1 \leq j \leq f$, has a multiplicative inverse in $O/pO$.*

*Proof.* Let $\mathfrak{p} \subset L$ be a prime above $p$. Because $K$ is the decomposition field of $p$, the prime ideal $\mathfrak{P} = \mathfrak{p} \cap K$ of $K$ is inert in $L$, i.e., $\mathfrak{p} = \mathfrak{P}O_L$.

Let $j$ be such that

$$0 < \left\|\pi_j(\gamma)\right\|_{B_{K/\mathbb{Q}}} < \frac{\sqrt{g}}{s_1(B_{K/\mathbb{Q}})} p^{1/g}.$$

Then by the inequality of the arithmetic and geometric mean, we find that

$$\begin{aligned} 0 < \left|\mathrm{N}_{K/\mathbb{Q}}\left(\pi_j(\gamma)\right)\right|^{2/g} &\leq \frac{1}{g}\left\|\mathrm{M}(B_{K/\mathbb{Q}}) \cdot \psi_{B_{K/\mathbb{Q}}}\left(\pi_j(\gamma)\right)\right\|^2 \\ &\leq \frac{s_1(B_{K/\mathbb{Q}})^2}{g}\left\|\pi_j(\gamma)\right\|^2_{B_{K/\mathbb{Q}}} \\ &< p^{2/g}. \end{aligned}$$

Therefore,

$$0 < \left|\mathrm{N}_{L/\mathbb{Q}}\left(\pi_j(\gamma)\right)\right| < p = \mathrm{N}_{L/\mathbb{Q}}(\mathfrak{P}) ,$$

which implies that $\pi_j(\gamma) \notin \mathfrak{P}$.

By Lemma 1, it follows that $\gamma \notin \mathfrak{P}O_L = \mathfrak{p}$, and, hence, $\gamma \in (O_L/\mathfrak{p})^*$. Since $p$ is unramified in $L$ and $\mathfrak{p} \mid p$ was arbitrary, it holds that $\gamma \in (O_L/pO_L)^*$, which proves theorem. □

The invertibility result of Theorem 3 requires that the rational prime $p$ factors as $(p) = \prod_{i=1}^{g} \mathfrak{p}_i$ with, for all $i$, $\mathfrak{p}_i$ prime in $L$ with inertia degree $f_i$. We say that $p$ has decomposition type $(f_1, \ldots, f_g)$ in $L$. Cyclotomic number fields are Galois and for this reason all rational primes $p$ have decomposition type $f_1 = \cdots = f_g = n/g$ for some $g \mid n$. For cyclotomic number fields, the distribution over the different decomposition types follows from

Table 1: Distribution of the decomposition types of rational primes $p$ in the cyclotomic number field $\mathbb{Q}(\zeta_{16})$ with Galois group $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

| Number of prime factors ($g$) | Decomposition type | Frobenius's Density (Thm. 5) | Density of Primes with Decomposition field $\mathbb{Q}(\zeta_{2g})$ (Lem. 3) |
|---|---|---|---|
| 1 | (8) | 0 | 0 |
| 2 | (4, 4) | 1/2 | 1/4 |
| 4 | (2, 2, 2, 2) | 3/8 | 1/8 |
| 8 | (1, 1, 1, 1) | 1/8 | 1/8 |

Dirichlet's theorem on arithmetic progression. In Lemma 3, this distribution was described, while restricting to rational primes that have a cyclotomic decomposition field $\mathbb{Q}(\zeta_z)$ in $\mathbb{Q}(\zeta_m)$.

For general number fields $L/\mathbb{Q}$, the density of primes $p$ with a decomposition type $(f_1, \ldots, f_g)$ in $L$ follows from *Frobenius' density theorem* [29]. The Galois group $G$ of $L/\mathbb{Q}$ is a subgroup of the permutation group $S_n$. Therefore, every element $\sigma \in G$ has a well-defined cycle structure. Note that $L/\mathbb{Q}$ is not required to be Galois, in which case the Galois group $G$ of $L$ refers to the Galois group of the Galois closure of $L$ and satisfies $|G| > n$. Frobenius' theorem shows that there is a relation between the cycle structures of elements $\sigma \in G$ and the decomposition types of rational primes $p$. More precisely, the density of primes with decomposition type $(f_1, \ldots, f_g)$ in $L$ can derived from the Galois group $G$ of $L/\mathbb{Q}$.

**Theorem 5** (Frobenius' Density Theorem [29])**.** *Let $L/\mathbb{Q}$ be a number field of degree $n$ with Galois group $G \subset S_n$. Let $A$ be the number of elements $\sigma \in G$ with cycle structure $(f_1, \ldots, f_g)$. Then, the density of rational primes $p$ with decomposition type $(f_1, \ldots, f_g)$ in $L$ equals $A/|G|$.*

Chebotarev's density theorem [51] is perhaps better known than its predecessor by Frobenius. It generalizes both Dirichlet's theorem on arithmetic progression and Frobenius' density theorem. However, for our purposes, Frobenius' theorem suffices.

Let us now consider two concrete examples. First, let $L := \mathbb{Q}(\zeta_{16})$ with Galois group $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We compare the densities from Theorem 5 with those from Lemma 3. Note that Lemma 3 is only applicable to cyclotomic number fields. Moreover, since Lemma 3 additionally requires the decomposition field of $p$ to be cyclotomic, its densities are always smaller than or equal to the ones obtained by Theorem 5. Table 1 displays the densities associated to $L/\mathbb{Q}$. In particular, it follows that there exist infinitely many primes with decomposition type $(4, 4)$ or $(2, 2, 2, 2)$ that do not have a cyclotomic decomposition field.

Second, we consider the trinomial number field $L = \mathbb{Q}[X]/(f)$ with $f = X^n - X - 1 \in \mathbb{Z}[X]$. The trinomials of the form $f = X^n - X - 1 \in \mathbb{Z}[X]$ are irreducible [47] and their Galois group is the full symmetry group $S_n$ [43]. Therefore, for all partitions $(f_1, \ldots, f_g)$ of $n$ (i.e., $f_1 + \cdots + f_g = n$) there exist infinitely many primes with a corresponding decomposition type. Moreover, the density of rational primes $p$ with decomposition type $(n/g, \ldots, n/g)$ for $g \mid n$ is equal to

$$\frac{g^g}{g! \cdot n^g}.$$

In particular, the density of primes that completely split in $L$ is $1/n!$.

## 5 INVERTIBILITY CONDITION VIA THE CANONICAL EMBEDDING

Thus far, the invertibility conditions have been stated in terms of $\ell_2$- and $\ell_\infty$-norms obtained via the coefficient embedding $\psi_B : L \to \mathbb{Q}^n$. However, a crucial step in the proofs of these theorems is to derive a bound on the $\ell_2$-norm of the canonical embedding $\phi_L(\gamma) \in \mathbb{C}^n$ of $\gamma$. In particular, both proofs use that for all $\gamma \in L$

$$\|\phi_L(\gamma)\| \leq s_1(B) \, \|\psi_B(\gamma)\| = s_1(B) \, \|\gamma\| \,,$$

where $B$ is a basis of $L/\mathbb{Q}$. A more natural approach would therefore be to state the invertibility condition in terms of the canonical embedding *directly*. This omits the need for the transformation $M_B$ from the coefficient to the canonical embedding (Figure 1). Therefore, such an invertibility condition does not depend on a basis $B$ and its largest singular value $s_1(B)$.

Actually, for some number fields $L$, the canonical embedding results in much tighter invertibility conditions. The largest singular value $s_1(B)$ namely represents the *worst-case* behavior of the transformation $M_B : \psi_B(L) \to \phi_L(L)$. More precisely, it shows how much the $\ell_2$-norm of a vector increases at most under the transformation $M_B$. However, this worst-case bound can be quite loose on *average*, i.e., there may exist $\gamma \in L$ with

$$\|\phi_L(\gamma)\| < s_1(B) \, \|\psi_B(\gamma)\| = s_1(B) \, \|\gamma\| \,.$$

An even more important argument for using the canonical embedding $\phi_L$ directly is that the hardness assumptions of ring-based lattice problems stem from the geometry derived from $\phi_L(L) \in \mathbb{C}^n$ [39]. Cryptographic protocols using the coefficient embedding must account for the geometric differences with the canonical embedding. In particular, if these embeddings induce very different geometries, cryptographic protocols using the coefficient embedding may become quite inefficient when instantiated with appropriate (secure) parameters.

For these reasons, we present another invertibility condition, in terms of the canonical embedding, in Theorem 6. Because the new invertibility condition is independent of the transformation $M_B$, it is easily generalized to arbitrary $\ell_k$-norms $\|\cdot\|_k$.

**Theorem 6** (Invertibility Condition via the Canonical Embedding)**.** *Let $L/\mathbb{Q}$ be a number field of degree $n$ with canonical embedding $\phi_L : L \to \mathbb{C}^n$. Further, let $k \in \mathbb{N} \cup \{\infty\}$, let $\mathcal{O} \subset \mathcal{O}_L$ be an order and let $p$ be a rational prime such that $p\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i$, where $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_L$ with inertia degree $f_i$ for all $i$. Then any $\gamma \in \mathcal{O}/p\mathcal{O}$ that satisfies*

$$0 < \|\phi_L(\gamma)\|_k < \sqrt[k]{n} \cdot p^{\min_{1 \le i \le g} f_i/n} \tag{13}$$

*has a multiplicative inverse in $\mathcal{O}/p\mathcal{O}$.*

*Proof.* For any $\gamma \in \mathcal{O}_L$ it follows, by the inequality of the arithmetic and the geometric mean, that

$$\left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right| \le \left(\frac{\|\phi_L(\gamma)\|_k}{\sqrt[k]{n}}\right)^n.$$

From Equation 13, it therefore follows that

$$0 < \left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right| < p^{\min_{1 \le i \le g} f_i} = \min_{1 \le i \le g} \mathrm{N}_{L/\mathbb{Q}}(\mathfrak{p}_i).$$

Hence, $\gamma \notin \mathfrak{p}_i$ and $\gamma \in (\mathcal{O}_L/\mathfrak{p}_i)^*$ for all $1 \le i \le g$. Therefore, $\gamma$ is invertible in $\mathcal{O}_L/p\mathcal{O}_L$. By Lemma 4 this implies that $\gamma \in (\mathcal{O}/p\mathcal{O})^*$, which proves the theorem.

□

Similarly, we present an adaptation of the invertibility result from Theorem 4. This adaptation uses the decomposition field techniques and is stated in terms of the canonical embedding directly.

**Theorem 7** (Decomposition Field Invertibility Condition via Canonical Embedding)**.** *Let $L/\mathbb{Q}$ be an Abelian Galois extension of degree $n$ containing an order $\mathcal{O} \subset \mathcal{O}_L$. Moreover, let $p$ be a rational prime that is unramified in $L$ and splits in $g$ factors of inertia degree $f = n/g$. Let $K$ be the decomposition field of $p$ with integral basis $B_{K/\mathbb{Q}}$, and assume that $\mathcal{O} = \beta_1\mathcal{O}_K + \cdots \beta_f\mathcal{O}_K$ with $\beta_j \in \mathcal{O}_L$. Let $\pi_j$ denote the projections associated to basis $(\beta_1, \ldots, \beta_f)$ of $L/K$, i.e., $\gamma = \sum_{j=1}^{f} \pi_j(\gamma)\beta_j$ for all $\gamma \in L$.*

*Then any $\gamma \in \mathcal{O}$ that satisfies*

$$0 < \left\|\phi_K(\pi_j(\gamma))\right\|_k < \sqrt[k]{g} \cdot p^{1/g}, \tag{14}$$

*for some $1 \le j \le f$, has a multiplicative inverse in $\mathcal{O}/p\mathcal{O}$.*

*Proof.* Let $\mathfrak{p} \subset L$ be a prime above $p$. Because $K$ is the decomposition field of $p$, the prime ideal $\mathfrak{P} = \mathfrak{p} \cap K$ of $K$ is inert in $L$, i.e., $\mathfrak{p} = \mathfrak{P}\mathcal{O}_L$. Moreover, the extension $K/\mathbb{Q}$ is of degree $g$.

Let $j$ be such that

$$0 < \left\|\phi_K(\pi_j(\gamma))\right\|_k < \sqrt[k]{g} \cdot p,$$

Then by the inequality of the arithmetic and geometric mean, we find that

$$0 < \left|\mathrm{N}_{K/\mathbb{Q}}(\pi_j(\gamma))\right|^{k/g} \le \frac{1}{g}\left\|\phi_K(\pi_j(\gamma))\right\|_k^k < p^{k/g}.$$

Therefore,

$$0 < \left|\mathrm{N}_{K/\mathbb{Q}}(\pi_j(\gamma))\right| < p = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}),$$

which implies that $\pi_j(\gamma) \notin \mathfrak{P}$.

By Lemma 1, it follows that $\gamma \notin \mathfrak{P}\mathcal{O}_L = \mathfrak{p}$, and, therefore, $\gamma \in (\mathcal{O}_L/\mathfrak{p})^*$. Since $p$ is unramified in $L$ and $\mathfrak{p} \mid p$ was arbitrary, it holds that $\gamma \in (\mathcal{O}_L/p\mathcal{O}_L)^*$, which proves the theorem. □

We have argued why the canonical embedding equips a number field with the 'appropriate' geometry. One might therefore wonder why we would consider the coefficient embedding at all. The main reason is that if $B$ is an integral basis of $L/\mathbb{Q}$, then $\psi_B(O_L) = \mathbb{Z}^n$, i.e., integral elements of $L$ can be represented by vectors in $\mathbb{Z}^n$. By contrast, the coordinates of elements in the canonical embedding $\phi_L(O_L) \in \mathbb{C}^n$ are, not necessarily integral, complex numbers. This increases the practical complexity of sampling (short) ring elements [27]. For this reason most lattice-based protocols use the coefficient embedding. To achieve strong security properties, they are typically defined over number fields $L$ that have a basis equipping $L$ with a coefficient geometry very similar to the canonical geometry.

Particularly popular are power-of-two cyclotomic number fields $L = \mathbb{Q}(\zeta_m)$ with power basis $B = (1, \zeta_m, \ldots, \zeta_m^{m/2-1})$. For power-of-two cyclotomic number fields the matrix $M_B$ is a scaled rotation and $\|\phi_L(\gamma)\| = s_1(m)\,\|\gamma\|$ for all $\gamma \in L$, i.e, the coefficient and canonical geometry are equivalent.

# 6 LARGEST SINGULAR VALUES

The geometry induced by the coefficient embedding can be viewed as a distortion of the canonical geometry; distorted by the matrix $\mathrm{M}_B$. Both geometries are equivalent if and only if the matrix $\mathrm{M}_B$ defines a scaled rotation. For number fields $L/\mathbb{Q}$ with basis $B$, $\mathrm{M}_B$ is a scaled rotation if and only if all its singular values are equal, or equivalently if

$$s_1(B) = \det(\mathrm{M}_B)^{1/n}.$$

This is the case for power-of-two cyclotomic number fields $L = \mathbb{Q}(\zeta_m)$ with power basis $B = (1, \zeta_m, \ldots, \zeta_m^{m/2-1})$. Note that if $B$ is an integral basis of $O_L$ then $\det(\mathrm{M}_B) = \sqrt{\Delta_{L/\mathbb{Q}}}$, where $\Delta_{L/\mathbb{Q}}$ is the discriminant of $L/\mathbb{Q}$. Moreover, for all fields $L/\mathbb{Q}$ and bases $B$, it holds that $s_1(B) \geq \det(\mathrm{M}_B)^{1/n}$. Hence, the value $s_1(B)$ is a good indicator for difference between the canonical and the coefficient geometry. Larger values $s_1(B)$ indicate larger distortions. For this reason, we aim to find fields and bases minimizing the largest singular value $s_1(B)$. A secondary motivation for studying the largest singular value $s_1(B)$ is that they directly influence the applicability of the invertibility conditions of Theorem 2 and Theorem 3. More precisely, smaller values $s_1(B)$ result in stronger invertibility conditions.

In this section, we derive upper bounds for largest singular values associated to cyclotomic and trinomial number fields. For cyclotomic number fields $\mathbb{Q}(\zeta_m)$ with power basis $B = (1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1})$, we prove an upper bound on $s_1(m)$ that was conjectured to hold in [41] (Section 6.1). Subsequently, we prove a lower bound on $s_1(B)$ that holds for all bases $B$ of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, i.e., not necessarily the power basis (Section 6.2). Using this lower bound we prove that, for prime-power conductors $m$, the power basis minimizes the largest singular value $s_1(B)$ and is in that sense optimal. Finally, we consider trinomial number fields of the form $\mathbb{Q}[X]/(f)$ with $f = X^n + aX^k + b \in \mathbb{Z}[X]$ ($k < n$) an irreducible trinomial and provide an upper bound on the largest singular values associated to these fields (Section 6.3).

## 6.1 CYCLOTOMIC NUMBER FIELDS

Let us consider the cyclotomic number field $\mathbb{Q}(\zeta_m)$ of conductor $m$ and degree $n = \varphi(m)$. Recall that $s_1(m)$ is the largest singular value of the matrix

$$\mathrm{M}_m = \left(\sigma_i(\zeta_m^{j-1})\right)_{1 \leq i,j \leq n}.$$

In [40] it was shown that for prime powers $m = p^k$,

$$s_1(m) = \sqrt{\tau(m)}, \tag{15}$$

where

$$\tau : \mathbb{Z} \to \mathbb{Z}, \quad \tau(m) = \begin{cases} m, & \text{if} \quad m \text{ is odd,} \\ m/2, & \text{if} \quad m \text{ is even.} \end{cases}$$

In general Equation 15 does not hold, but Lyubashevsky and Seiler [41] conjectured the following inequality:

$$s_1(m) \leq \sqrt{\tau(m)}, \quad \forall m \in \mathbb{Z}_{>0}.$$

Our proof of this conjectured inequality uses techniques similar to the ones used in the proof of Equation 15 [40]. To this end, let us consider the $n \times m$ matrix

$$\mathcal{A}_m = \left(\sigma_i(\zeta_m^k)\right)_{1 \leq i \leq n,\ 0 \leq k \leq m-1}. \tag{16}$$

Note that the matrix $\mathrm{M}_m$ is an $n \times n$ submatrix of $\mathcal{A}_m$. Therefore, it holds that

$$s_1(m) \leq s_1(\mathcal{A}_m), \quad \forall m \in \mathbb{Z}_{>0}.$$

Moreover, let $m = p_1^{e_1} \dots p_g^{e_g}$ be the prime factorization of $m$, then it is easily seen that, up to permutation of rows and columns,

$$\mathcal{A}_m = \mathcal{A}_{p_1^{e_1}} \otimes \cdots \otimes \mathcal{A}_{p_g^{e_g}}, \tag{17}$$

where $\otimes$ denotes a Kronecker product. Recall that (w.l.o.g.) primitive roots of unity are chosen to satisfy $\zeta_{kl} = \zeta_k \zeta_l$ for all $k, l \in \mathbb{Z}_{>0}$ that are relatively prime.

Let us now consider the $m \times m$ matrix $\mathcal{B}_m := \mathcal{A}_m^\dagger \mathcal{A}_m$. Then the largest singular value $s_1(\mathcal{A}_m)$ of $\mathcal{A}_m$ is equal to the square root of the largest eigenvalue of $\mathcal{B}_m$. We will find the largest singular value of $\mathcal{A}_m$ by determining the eigenvalues of $\mathcal{B}_m$. First, by the following lemma, we find the coefficients of $\mathcal{B}_m$.

**Lemma 5.** *Let $\mathcal{B}_m = \mathcal{A}_m^\dagger \mathcal{A}_m$, then*

$$\mathcal{B}_m = \left(\mathrm{Tr}_{L/\mathbb{Q}}\left(\zeta_m^{l-k}\right)\right)_{1 \leq k,l \leq m}. \tag{18}$$

*Moreover*

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\zeta_m^k\right) = \frac{\varphi(m)}{\varphi(m/\gcd(m,k))}\mu(m/\gcd(m,k)), \tag{19}$$

*where $\mu(l)$ equals the sum of the primitive $l^{th}$-root of unities.*

*Proof.* The $(k,l)^{th}$-entry of $\mathcal{A}_m^\dagger \mathcal{A}_m$ equals

$$\sum_{\sigma \in G} \overline{\sigma(\zeta_m^k)}\sigma(\zeta_m^l) = \sum_{\sigma \in G} \sigma(\zeta_m^{l-k}) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\zeta_m^{l-k}\right),$$

proving Equation 18.

Moreover, $\zeta_m^k$ is a primitive $l^{th}$-root of unity with $l = m/\gcd(m,k)$, and $G = \mathrm{Gal}\left(\mathbb{Q}(\zeta_m)/\mathbb{Q}\right)$ acts transitively on the set of primitive $l^{th}$-root of unities. Hence, the size of the orbit of this group action is $\varphi(l)$ and

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\zeta_m^k\right) = \frac{\varphi(m)}{\varphi(l)}\mu(l),$$

proving Equation 19 and completing the proof of Lemma 5. □

The function $\mu(l)$ is called the Möbius function and it is given by

$$\mu(l) = \begin{cases} 1, & \text{if } l \text{ is square-free with an even number of prime factors,} \\ -1, & \text{if } l \text{ is square-free with an odd number of prime factors,} \\ 0, & \text{if } l \text{ is divisible by a square.} \end{cases}$$

In particular, it follows from Lemma 5 that for prime powers $m = p^e$

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\zeta_m^k\right) = \begin{cases} (p-1)p^{e-1}, & \text{if } k = 0, \\ 0, & \text{if } p^{e-1} \nmid k, \\ -p^{e-1}, & \text{otherwise.} \end{cases}$$

Hence, for prime powers,

$$\mathcal{B}_m = \mathcal{B}_{p^e} = p^{e-1}\mathcal{B}_p \otimes \mathbb{I}_{p^{e-1}}, \tag{20}$$

and

$$\mathcal{B}_p = p\mathbb{I}_p - \mathbf{1}_p \mathbf{1}_p^T, \tag{21}$$

where $\mathbb{I}_k$ is the $k \times k$ identity matrix and $\mathbf{1}_k \in \mathbb{Z}^k$ is the all-ones vector.

From this decomposition we can find the eigenvalues of $\mathcal{B}_m$. More precisely the following lemma shows that the matrix $\mathcal{B}_m$ only has two different eigenvalues.

**Lemma 6.** *The matrix $\mathcal{B}_m$ has eigenvalues 0 and $m$, with multiplicities $m - \varphi(m)$ and $\varphi(m)$, respectively.*

*Proof.* Let $m = p_1^{e_1} \dots p_g^{e_g}$ be the prime factorization of $m$, then by Equation 17 it follows that

$$\mathcal{B}_m = \mathcal{B}_{p_1^{e_1}} \otimes \dots \otimes \mathcal{B}_{p_g^{e_g}}.$$

Hence, the eigenvalues of $\mathcal{B}_m$ are of the form $\lambda = \lambda_1 \cdots \lambda_g$ with $\lambda_i$ an eigenvalue of $\mathcal{B}_{p_i^{e_i}}$ for all $1 \leq i \leq g$. Therefore, it suffices to prove the statement for prime powers. So let us assume $m = p^e$ for some prime $p$ and positive integer $e$.

We have already seen that in this case $\mathcal{B}_m = p^{e-1}\mathcal{B}_p \otimes \mathbb{I}_{p^{e-1}}$ and $\mathcal{B}_p = p\mathbb{I}_p - \mathbf{1}_p^T\mathbf{1}_p$. The eigenvalues of $\mathcal{B}_p$ can easily be shown to be equal to 0 and $p$, with multiplicities 1 and $p-1$, respectively. Hence the eigenvalues of $\mathcal{B}_m$ are 0 and $p^e$ with multiplicities $p^{e-1}$ and $(p-1)p^{e-1}$ respectively, which proves the lemma. □

We are now ready to prove an upper bound for the largest singular value $s_1(m)$. This proves an inequality conjectured in [41, Conjecture 2.6].

**Proposition 1.** *For all positive integers m, $s_1(m) \leq \sqrt{\tau(m)}$.*

*Proof.* Let $\mathcal{A}_m \in \mathbb{C}^{n\times m}$ be as in Equation 16 and let $\mathcal{B}_m = \mathcal{A}_m^\dagger \mathcal{A}_m \in \mathbb{C}^{m\times m}$. Then by Lemma 6 it follows that

$$s_1(m) \leq s_1(\mathcal{A}_m) = \sqrt{s_1(\mathcal{B}_m)} = \sqrt{m},$$

which proves the proposition for all odd $m$.

Now assume that $m$ is even. Then, for some matrix $A \in \mathbb{C}^{n\times m/2}$ containing $\mathrm{M}_m \in \mathbb{C}^{n\times n}$ as a submatrix, it holds that $\mathcal{A}_m = (A, -A)$. Hence, $s_1(\mathcal{A}_m) = \sqrt{2} \cdot s_1(A)$ and

$$s_1(m) \leq s_1(A) = s_1(\mathcal{A}_m)/\sqrt{2} = \sqrt{m/2} = \sqrt{\tau(m)},$$

which completes the proof of the proposition. □

Since all columns of the matrix $\mathrm{M}_m$ have norm $\sqrt{\varphi(m)}$ we also obtain a lower bound for the largest singular value $s_1(m)$. In fact, we obtain

$$\sqrt{\varphi(m)} \leq s_1(m) \leq \sqrt{\tau(m)}, \tag{22}$$

with an equality on both sides of $s_1(m)$ if and only if $m$ is a power of 2.

## 6.2 OPTIMAL BASIS FOR CYCLOTOMIC NUMBER FIELDS

In Section 6.1, we have proven an upper and a lower bound for the largest singular value $s_1(m)$ of the matrix $\mathrm{M}_m$. The matrix $\mathrm{M}_m$ is derived from the power basis $1, \zeta_m, \dots, \zeta_m^{\varphi(m)-1}$ of $L = \mathbb{Q}(\zeta_m)$. A question that remains is whether we can find another integral basis $B = \{\alpha_1, \dots, \alpha_{\varphi(m)}\}$ with the same or even a smaller largest singular value associated to it. In this section, we find a lower bound that holds for all integral bases of cyclotomic number fields. Moreover, we show that, for prime power conductors, the power basis is indeed optimal.

Let us consider the matrix

$$\mathrm{M}_B = \left(\sigma_i(\alpha_j)\right)_{1\leq i,j\leq\varphi(m)} \in L^{\varphi(m)\times\varphi(m)},$$

and define $s_1(B)$ to be its largest singular value. From the following lemma it follows that the lower bound of Equation 22 does not only hold for the power basis, but for all integral bases of $L$.

**Lemma 7.** *Let $B$ be an integral basis of $\mathbb{Q}(\zeta_m)$, then for all $\alpha \in B$, it holds that*

$$\left\|(\sigma_i(\alpha))_{1\leq i\leq\varphi(m)}\right\| \geq \sqrt{\varphi(m)}.$$

*Moreover, we have equality if and only if $\alpha^m = \pm 1$.*

*Proof.* By the inequality of the arithmetic and geometric mean we have

$$\frac{1}{n}\left\|(\sigma_i(\alpha))_{1\leq i\leq\varphi(m)}\right\|^2 \geq \left|\mathrm{N}_{L/\mathbb{Q}}(\alpha)\right|^{1/\varphi(m)},$$

with equality if and only if $|\sigma_i(\alpha)| = \left|\sigma_j(\alpha)\right|$ for all $i, j$. Moreover, since $\alpha$ is integral and non-zero it holds that $|\,\mathrm{N}_{L/\mathbb{Q}}(\alpha)\,| \geq 1$ and therefore that

$$\left\|(\sigma_i(\alpha))_{1\leq i\leq\varphi(m)}\right\| \geq \sqrt{\varphi(m)},$$

with equality if and only if $|\sigma_i(\alpha)| = 1$ for all $i$ or equivalently $\alpha^m = \pm 1$, which proves the lemma.

□

**Corollary 2.** *Let $B$ be an integral basis of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, then $s_1(B) \geq \sqrt{\varphi(m)}$.*

*Proof.* Let $\alpha \in B$, then $(\sigma_i(\alpha))_{1 \leq i \leq \varphi(m)}$ is a column of $\mathrm{M}_B$ and

$$s_1(B) \geq \left\| (\sigma_i(\alpha))_{1 \leq i \leq \varphi(m)} \right\|.$$

The corollary now follows from Lemma 7. □

The following theorem shows, for $m$ a prime power, that any basis $B$ with $s_1(B) \leq \sqrt{\tau(m)}$ can only contain roots of unity. Its proof uses the fact that, for prime powers $m$, all non-zero elements of the complex lattice

$$\phi_L(\mathcal{O}_L) = \{\gamma \in \mathbb{C}^n : \gamma = \mathrm{M}_m\, x \text{ for some } x \in \mathbb{Z}^n\}$$

with norm $\leq \sqrt{m}$ have norm $\sqrt{\varphi(m)}$ and therefore correspond to roots of unity (up to sign).

**Theorem 8.** *Let $m = p^e$ be a prime power and let $B$ be a basis of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ with $s_1(B) \leq \sqrt{\tau(m)}$, then for all $\alpha \in B$ it holds that $\alpha^m = \pm 1$.*

*Proof.* Let $\alpha \in B$ be one of the basis vectors. Then there exists a non-zero $x \in \mathbb{Z}^n$ such that

$$\mathrm{M}_m\, x = \left(\sigma_1(\alpha), \ldots, \sigma_{\varphi(m)}(\alpha)\right)^T.$$

Moreover, $s_1(B) \leq \sqrt{\tau(m)}$ implies that

$$\|\mathrm{M}_m\, x\| \leq \sqrt{\tau(m)}.$$

If $\|\mathrm{M}_m\, x\| = \sqrt{\varphi(m)}$ the theorem follows from Lemma 7, so we are left to consider the case

$$\sqrt{\varphi(m)} < \|\mathrm{M}_m\, x\| \leq \sqrt{\tau(m)}. \tag{23}$$

If $p = 2$, then $\tau(m) = \varphi(m) = m/2$ and Equation 23 results in a contradiction. So let us assume that $p$ is an odd prime and therefore $\tau(m) = m$.

Analogous to the deduction of Equations 20 and 21 it can be shown that

$$G_m := \mathrm{M}_m^\dagger\, \mathrm{M}_m = \left(p^e \mathbb{I}_{p-1} - p^{e-1} \mathbf{1}_{p-1} \mathbf{1}_{p-1}^T\right) \otimes \mathbb{I}_{p^{e-1}}.$$

Hence all entries of the Gram matrix $G_m$ are divisible by $p^{e-1}$ and, together with Equation 23, it follows that

$$x^T G_m x = 0 \mod p^{e-1} \quad \text{and} \quad (p-1)p^{e-1} < x^T G_m x \leq p^e,$$

which implies that

$$x^T G_m x = p^e.$$

If we let $y_i = \left(x_i, x_{i+p^{e-1}}, \ldots, x_{i+(p-2)p^{e-1}}\right) \in \mathbb{Z}^{p-1}$ for $1 \leq i \leq p^{e-1}$, we can rewrite this equation as follows

$$x^T G_m x = p^{e-1} \sum_{i=1}^{p^{e-1}} y_i^T G_p\, y_i = p^e.$$

Since for all non-zero $y \in \mathbb{Z}^{p-1}$ it holds that $y^T G_p\, y \geq p - 1$ (Lemma 7), we see that there is exactly one $i$ such that $y_i$ is non-zero (recall that $p$ is odd). Hence,

$$x^T G_m x = p^{e-1} y_i^T G_p\, y_i = p^e \|y_i\|^2 - p^{e-1} \left(\sum_{j=1}^{p-1} y_{ij}\right)^2 = p^e. \tag{24}$$

It now follows that

$$\sum_{j=1}^{p-1} y_{ij} = kp, \quad \text{for some } k \in \mathbb{Z}.$$

Hence,

$$|kp| \leq \sum_{j=1}^{p-1} |y_{ij}| = \|y_i\|_1 \leq \sqrt{p-1}\, \|y_i\|.$$

Substituting in Equation 24 then gives

$$p^e = x^T G_m x \geq p^e \frac{k^2 p^2}{p-1} - p^{e-1} k^2 p^2 = \frac{k^2 p}{p-1} p^e,$$

which implies $k = 0$ and, again by Equation 24, $\|y_i\| = \|x\| = 1$ contradicting the assumption that $\|\mathrm{M}_m x\| > \sqrt{\varphi(m)}$. Hence, there does not exist an $x \in \mathbb{Z}^n$ such that $\sqrt{\varphi(m)} < \|\mathrm{M}_m x\| \leq \sqrt{\tau(m)}$ which proves the theorem. □

**Remark 7.** *The proof of Theorem 8 does not generalize to composite conductors m. As a counterexample take $m = 15$, i.e., $L = \mathbb{Q}(\zeta_{15})$. Then $\alpha = 1 + \zeta_{15}^3$ is not a root of unity and*

$$\sqrt{\varphi(m)} = 2\sqrt{2} < \left\|(\sigma_i(\alpha))_{1 \leq i \leq \varphi(15)}\right\| = 2\sqrt{3} < \sqrt{15} = \sqrt{\tau(m)}.$$

At this point we have shown that for prime powers $m = p^e$, any integral basis $B$ of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ with $s_1(B) \leq \sqrt{\tau(m)}$ can only contain roots of unity. Next, we aim to differentiate between bases of this form and show that, for prime powers $m$, all of them result in the same largest singular value $s_1(B) = \sqrt{\tau(m)}$. The following theorem enumerates all bases $B$ of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ containing only roots of unity.

**Theorem 9.** *Let $m = p^e$ be an odd prime power and let*

$$R_m := \left\{ \zeta_m^{p^{e-1}i+j} : 0 \leq i \leq p-1, 0 \leq j \leq p^{e-1}-1 \right\}$$

*be the set of $m^{th}$-roots of unity. Then a subset $S \subset R_m$ of cardinality $\varphi(m)$ forms a basis of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ if and only if, for all $0 \leq j \leq p^{e-1}-1$, the following set forms a basis for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$,*

$$\left\{ \zeta_m^{p^{e-1}i} : \zeta_m^{p^{e-1}i+j} \in S \right\}.$$

*Proof.* This theorem follows directly from Theorem 3.2 of [14]. □

Theorem 9 shows that any basis containing only $m^{th}$-roots of unity can be constructed by, for all $0 \leq j \leq p^{e-1}-1$, choosing a basis of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ containing only $p^{th}$-roots of unity. There are $p$ bases of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ of this form and, therefore, $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ has precisely $p^{p^{e-1}}$ bases containing only roots of unity.

Now that we have enumerated all bases $B$ with $s_1(B) \leq \sqrt{\tau(m)}$, let us consider their largest singular values $s_1(B)$. The following theorem shows that all these bases have a largest singular value $s_1(B) = \sqrt{\tau(m)}$ and that there does not exist an integral basis of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ with $s_1(B) < \sqrt{\tau(m)}$.

**Theorem 10.** *Let $m = p^e$ be a prime power and let $B$ be a basis of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ containing only $m^{th}$-roots of unity. Then $s_1(B) = \sqrt{\tau(m)}$.*

*Proof.* Let us first consider the case $p = 2$. Then the set of $m^{th}$-roots of unity is given by

$$\left\{ \pm 1, \pm\zeta_m^1, \ldots, \pm\zeta_m^{\varphi(m)} \right\}.$$

Hence, any basis $B$ of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ containing only $m^{th}$-roots of unity can be obtained by taking the power basis and changing the sign of some of its elements. From this it follows that $s_1(B) = \sqrt{\tau(m)}$, which proves the theorem for $p = 2$.

Let us now now consider the case where $p$ is an odd prime, then $\tau(m) = m$ and $s_1(B)^2$ is the largest eigenvalue of the Gram matrix $G_B = \mathrm{M}_B^\dagger \mathrm{M}_B$. Since $B$ only contains roots of unity, $G_B$ is submatrix of the matrix $\mathcal{B}_m$ of Lemma 5. Hence for all $1 \leq i, j \leq \varphi(m)$ the $ij^{th}$-entry of $G_B$ is equal to

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\zeta_m^{k_{ij}}\right) = \frac{\varphi(m)}{\varphi(m/\gcd(m,k_{ij}))}\mu(m/\gcd(m,k_{ij})),$$

for some $-m < k_{ij} < m$. For a different basis $\tilde{B}$ we obtain, by Theorem 9, that the Gram matrix $G_{\tilde{B}}$ has its $ij^{th}$-entry equal to

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\zeta_m^{k_{ij}+p^{e-1}l}\right),$$

for some $l \in \mathbb{Z}$. Hence, if $i \neq j$ then $k_{ij} \neq 0$ and $\gcd(m, k_{ij}) = \gcd(m, k_{ij} + p^{e-1}l)$ from which it follows that the $ij^{th}$-entries of the Gram matrices $G_B$ and $G_{\tilde{B}}$ are equal. Moreover, the diagonal elements of the Gram matrices $G_B$ and $G_{\tilde{B}}$ are all equal to $\varphi(m)$. Hence, $G_B = G_{\tilde{B}}$ and $s_1(B) = s_1(\tilde{B})$. By Equation 15 it follows that $s_1(B) = \sqrt{m}$ which proves the theorem. □

**Remark 8.** *Theorem 10 does not generalize to arbitrary conductors m, i.e., conductors that are not prime powers. As a counterexample we can take* $m = 105 = 3 \times 5 \times 7$ *with largest singular value* $s_1(m) = 9,95.. < \sqrt{105}$. *When we take B to be the powerful basis [40], also containing only roots of unity, we obtain a largest singular value* $s_1(B) = \sqrt{105}$. *Hence for* $m = 105$, *not all bases containing only roots of unity result in the same largest singular value.*

## 6.3 TRINOMIAL NUMBER FIELDS

Let us now consider trinomial number fields $L = \mathbb{Q}/(f)$ with $f = X^n + aX^k + b \in \mathbb{Z}[X]$ $(k < n)$ irreducible. More precisely, we consider the order $\mathcal{O} = \mathbb{Z}[X]/(f)$ in $L$ and derive bounds on the largest singular values associated to the order $\mathcal{O}$. More precisely, for a root $\alpha \in \mathcal{O}$ of $f$, we show that the largest singular value associated to the power basis $B_f = \left(1, \alpha, \ldots, \alpha^{n-1}\right)$ of $\mathcal{O}$ only grows linearly in the degree $n$ of $f$.

Let $L = \mathbb{Q}(\alpha)$ with complex embeddings $\sigma_i$ for $0 \leq i \leq n-1$. Then the matrix $\mathrm{M}(B_f)$ is defined as

$$\mathrm{M}(B_f) = \left(\sigma_i(\alpha^{j-1})\right)_{1 \leq i,j \leq n} \in \bar{L}^{n \times n}.$$

Note that for a different choice of root $\alpha$, the rows of the matrix $\mathrm{M}(B_f)$ are permuted and its singular value stays the same, which justifies our abuse of notation.

In the remainder of this section we prove an upper bound for the largest singular value $s_1(B_f) = s_1(\mathrm{M}(B_f))$. To this end we state a theorem that was originally proven in 1908 by Bohl [11] and later reformulated in [50].

**Theorem 11** ([11, 50])**.** *Let* $f = X^n + aX^k + b \in \mathbb{C}[X]$. *Let* $\beta \in \mathbb{R}_{>0}$ *and N be the number of roots of f with absolute value smaller than or equal to* $\beta$. *Then the following holds:*

1. *If* $|b| \geq \beta^n + |a|\beta^k$, *then* $N = 0$,
2. *If* $\beta^n \geq |a|\beta^k + |b|$, *then* $N = n$,
3. *If* $|a|\beta^k \geq \beta^n + |b|$, *then* $N = k$.

From this theorem the following result is obtained.

**Corollary 3.** *Let* $f = X^n + aX^k + b \in \mathbb{Z}[X]$ *with roots* $\alpha_0, \ldots, \alpha_{n-1}$. *Then*

$$\max_i(|\alpha_i|) \leq (|a| + |b|)^{\frac{1}{n-k}}.$$

*Proof.* If $\beta = (|a| + |b|)^{\frac{1}{n-k}} \geq 1$ it follows that

$$\beta^n = \beta^k \beta^{n-k} = \beta^k(|a| + |b|) \geq |a|\beta^k + |b|.$$

Hence, in this case, the corollary immediately follows from Theorem 11.

If $\beta = 0$ it follows that $a = b = 0$ and therefore that $\alpha_i = 0$ for all $i$, which completes the proof. □

We are now ready to give an upper bound for the largest singular value $s_1(B_f)$.

**Lemma 8.** *Let* $f = X^n + aX^k + b \in \mathbb{Z}[X]$ *be an irreducible polynomial. Then*

$$s_1(B_f) \leq n\,(|a| + |b|)^{\frac{n-1}{n-k}}.$$

*Proof.* Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f$ and define $\vec{\alpha}^\ell := \left(\alpha_1^\ell, \ldots, \alpha_n^\ell\right)^T$. Then $\vec{\alpha}^\ell$, for $0 \leq \ell \leq n-1$, are precisely the columns of $\mathrm{M}(B_f)$. Moreover, by Corollary 3 it follows that for all $0 \leq \ell \leq n-1$

$$\begin{aligned} ||\alpha^\ell||_\infty &\leq (|a| + |b|)^{\frac{\ell}{n-k}}, \\ &\leq (|a| + |b|)^{\frac{n-1}{n-k}}. \end{aligned} \tag{25}$$

Hence for all $1 \leq i, j \leq n$

$$\left|\mathrm{M}(B_f)_{ij}\right| \leq (|a| + |b|)^{\frac{n-1}{n-k}},$$

and

$$\begin{aligned} s_1(B_f) &\leq ||\,\mathrm{M}(B_f)||_{HS}, \\ &= \sqrt{\sum_{i,j=1}^{n} \left|\mathrm{M}(B_f)_{ij}\right|^2}, \\ &\leq n\,(|a| + |b|)^{\frac{n-1}{n-k}}, \end{aligned} \tag{26}$$

where $||\cdot||_{HS}$ denotes the Hilbert-Schmidt norm. This proves the lemma. □

A similar upper bound is given in Lemma 5.5 of [44]. They consider a more general class of polynomials and derive a slightly larger upper bound. The following lemma yields a minor improvement over Lemma 8.

**Lemma 9.** *Let $f = X^n + aX^k + b \in \mathbb{Z}[X]$ be an irreducible polynomial. Then*

$$s_1(B_f) \leq n \sqrt{\frac{(|a| + |b|)^{\frac{2n}{n-k}} - 1}{n\left((|a| + |b|)^{\frac{2}{n-k}} - 1\right)}},$$

*with for fixed $k$*

$$\lim_{n\to\infty} \frac{(|a| + |b|)^{\frac{2n}{n-k}} - 1}{n\left((|a| + |b|)^{\frac{2}{n-k}} - 1\right)} = \frac{(|a| + |b|)^2 - 1}{2\log(|a| + |b|)}$$

*Proof.* The first part of the proof of this theorem is analogous to the proof of Lemma 8. We use the first inequality of Equation 25 to obtain the following upper bound:

$$\begin{aligned} s_1(B_f) &\leq ||\,\mathrm{M}(B_f)||_{HS}, \\ &= \sqrt{\sum_{i,j=1}^{n} \left|\mathrm{M}(B_f)_{ij}\right|^2}, \\ &\leq \sqrt{n \sum_{\ell=0}^{n-1} (|a| + |b|)^{\frac{2\ell}{n-k}}}, \end{aligned}$$

from which the first claim of the theorem follows by the summation formula for geometric series.

Now we prove the second claim of the theorem. For the numerator in the limit we have

$$\begin{aligned} \lim_{n\to\infty} (|a| + |b|)^{\frac{2n}{n-k}} - 1 &= \lim_{n\to\infty} (|a| + |b|)^{\frac{2}{1-k/n}} - 1 \\ &= (|a| + |b|)^2 - 1, \end{aligned}$$

and for the denominator we have

$$\begin{aligned} \lim_{n\to\infty} n\,(|a| + |b|)^{\frac{2}{n-k}} - n &= \lim_{N\to 0} \frac{(|a| + |b|)^{\frac{2N}{1-kN}} - 1}{N}, \\ &= \lim_{N\to 0} \frac{\frac{d}{dN}\left[(|a| + |b|)^{\frac{2N}{1-kN}} - 1\right]}{\frac{d}{dN}\,[N]}, \\ &= \lim_{N\to 0} \frac{(|a| + |b|)^{\frac{2N}{1-kN}} \log\left(|a| + |b|\right)^{\frac{2}{(1-kN)^2}}}{1}, \\ &= 2\log(|a| + |b|), \end{aligned}$$

where the second equality follows from L'Hôpital's rule. This proves the second claim of the lemma and concludes the proof. □

Hence, the largest singular value $s_1(B_f)$ grows at most linearly in the degree $n$ of $f$. For cyclotomic number fields $L$ of conductor $m$ an upper bound on the largest singular value $s_1(m)$ could have been obtained by applying the same proof technique. This would have resulted in the sub-optimal upper bound $s_1(m) \leq \varphi(m)$. In comparison, in Section 6.1 we proved the upper bound $s_1(m) \leq \sqrt{\tau(m)}$. The main difference is that in the proofs of Lemmas 8 and 9 we merely considered the size of the entries of $\mathrm{M}(B_f)$ and not the orthogonality of its columns. This observation suggests that there might be room for improving the upper bound of $s_1(B_f)$ for trinomials $f$.

## 7 CONSTRUCTING CHALLENGE SETS

In this section, we apply the invertibility theorems to construct challenge sets $C$ in the rings of integers of either the cyclotomic number field $\mathbb{Q}(\zeta_{512})$ or the trinomial number field $\mathbb{Q}[X]/\left(X^{256} - X - 1\right)$. These fields have rings of integers $\mathbb{Z}[\zeta_{512}]$ and $\mathbb{Z}[X]/\left(X^{256} - X - 1\right)$, respectively. The challenge sets contain ring elements of bounded norm. For post-quantum security a challenge set of size approximately $2^{256}$ is typically required. In [41], a challenge set of cardinality $2^{237}$ is constructed. To be able to compare our challenge sets to the one from [41], we

choose the norm bound such that our challenge sets are of size at least $2^{237}$. Subsequently, the invertibility theorems give a lower bound on the size of primes $p$ for which non-zero challenge differences are guaranteed to be invertible. This lower bound depends on the splitting behavior of $p$. In particular, if $p$ splits into $g$ factors with inertia degrees $f$ the prime $p$ is required to be larger than if the prime splits into less factors ($g' < g$) with larger inertia degrees ($f' > f$). We consider this trade-off by displaying the prime sizes for different decomposition types.

We start by constructing challenge sets via the coefficient embedding in Section 7.1. This is the preferred embedding because it allows challenges to be efficiently sampled. For a more detailed discussion see Section 5. However, in some cases, constructing challenge sets via the canonical embedding directly results in a stronger invertibility condition with smaller primes $p$. For this reason, we construct challenge sets via the canonical embedding in Section 7.2.

## 7.1 COEFFICIENT EMBEDDING

In this section, challenge sets are constructed via the coefficient embedding. The invertibility theorems suggest that a challenge set $C$ should simply contain all ring elements $c$ of bounded norm $\|c\| \leq R$ for some appropriately chosen $R \in \mathbb{R}_{\geq 0}$. However, we apply two adaptations to this approach. First, we additionally restrict challenge sets to elements $c$ with $\|c\|_\infty = 1$. Second, we only consider challenges $c$ with norm exactly equal to $R$, i.e., $\|c\| = R$. These adaptations were already applied in the ad-hoc example of [41]. Challenge sets of this form have a convenient closed form expression for their cardinality. Moreover, in this case, a minor ad-hoc improvement applies (see Lemma 10). Finally, since for appropriately chosen $R$ the vast majority of elements of norm at most $R$ have norm *exactly* equal to $R$, restricting the challenges $c$ to $\|c\| = R$ does not significantly reduce the size of the challenge set.

Altogether, for both the cyclotomic ring $\mathbb{Z}[\zeta_{512}] = \mathbb{Z}[X]/(X^{256}+1)$ and the trinomial ring $\mathbb{Z}[X]/(X^{256}-X-1)$ with power basis $B = (1, X, \ldots, X^{255})$, challenge sets of the following form are considered,

$$C(R) = \left\{ \gamma = \sum_{i=0}^{255} a_i X^i : a \in \mathbb{Z}^{256},\ \|a\| = R,\ \|a\|_\infty = 1 \right\}, \quad \text{with } |C| = \binom{256}{R^2} 2^{R^2}, \tag{27}$$

where $R$ is an appropriately chosen norm bound. More precisely, $R$ only depends on the required size of the challenge set. In our case, we choose $R = \sqrt{53}$ such that $|C(R)| \geq 2^{237}$.

Any non-zero challenge difference $\bar{c} \in C(R) - C(R) = \{c - c' : c, c' \in C(R),\ c \neq c'\}$ has norm $\|\bar{c}\| \leq 2R$. Let $p \in \mathbb{N}$ be a prime that splits in $g$ factors in $\mathcal{O}$ that all have inertia degree $f$. By Theorem 2 and Theorem 3, it follows that if

$$p > \left( \frac{s_1(B) \cdot 2R}{\sqrt{n}} \right)^g = \begin{cases} (2R)^g\,, & \text{if } L = \mathbb{Q}(\zeta_{512}), \\ (3{,}91..R)^g\,, & \text{if } L = \mathbb{Q}[X]/(X^{256} - X - 1), \end{cases} \tag{28}$$

then any non-zero challenge difference $\bar{c}$ has a multiplicative inverse in $\mathcal{O}_L/p\mathcal{O}_L$. Here, we have used the fact that $s_1(B) = \sqrt{256} = 16$ in the cyclotomic case and $s_1(B) = 31{,}33..$ in the trinomial case.

The following lemma shows that a slightly smaller lower bound on the prime $p$ is also sufficient to guarantee the invertibility of challenge differences. The applicability of this lemma crucially depends on the specific form of our challenges sets, i.e., for all $c \in C(R)$ it holds that $\|c\| = R$ and $\|c\|_\infty = 1$.

**Lemma 10** ([41])**.** *Let $n \in \mathbb{N}$, $R \in \mathbb{R}_{>0}$ and let $x, x' \in \mathbb{Z}^n$ such that $\|x\| = \|x'\| = R$ and $\|x\|_\infty = \|x'\|_\infty = 1$. Then either $\exists y$ with such that $\|y\| = R$ and $x - x' = 2y$ or $\|x - x'\| \leq \sqrt{4R^2 - 2}$.*

*Proof.* First note that $\|x - x'\| \leq 2R$ with equality if and only if $x = -x' = y$ for some $y \in \mathbb{Z}^n$ with $\|y\| = R$, i.e., $x - x' = 2y$.

So let us assume that $x \neq -x'$. The existence of an $x \in \mathbb{Z}^n$ with $\|x\| = R$ and $\|x\|_\infty = 1$ implies that $n \geq R^2$. Moreover, it holds that $\|x - x'\|_\infty \leq 2$ and $\|x - x'\|_1 \leq 2R^2$. Therefore, in this case, the norm of $x - x'$ is maximal when it has exactly $R^2 - 1$ entries equal to $\pm 2$, one or two entries equal to $\pm 1$ (depending on the dimension $n$) and all other entries equal to 0. Hence, $\|x - x'\| \leq \sqrt{4R^2 - 2}$, which proves the lemma. □

If $p$ is an odd prime, then 2 is invertible modulo $p$. Hence, by Lemma 10, it follows that for any odd prime $p$ with

$$p > \begin{cases} \left(\sqrt{4R^2 - 2}\right)^g\,, & \text{if } \mathcal{O} = \mathbb{Z}[\zeta_{512}], \\ \left(1{,}95..\sqrt{4R^2 - 2}\right)^g\,, & \text{if } \mathcal{O} = \mathbb{Z}[X]/(X^{256} - X - 1), \end{cases} \tag{29}$$

non-zero challenge differences are invertible in $\mathcal{O}_L/p\mathcal{O}_L$. This bound is a minor improvement of Equation 28.

For the cyclotomic number field we also consider the *decomposition field* approach, i.e., the second invertibility condition of Theorem 2. In this approach we require the prime $p$ to have a cyclotomic decomposition field $\mathbb{Q}(\zeta_z)$

in $L = \mathbb{Q}(\zeta_{512})$. Note that in this case, the prime $p$ splits in $g = \varphi(z) = z/2$ factors of the same inertia degree $f = 256/g$. Using the decomposition field approach, challenge sets $\mathcal{D}_g(R)$ are defined as all elements $\gamma \in \mathcal{O}_L$ with short projections $\pi_j \colon L = \mathbb{Q}(\zeta_{512}) \to \mathbb{Q}(\zeta_z)$ for all $1 \leq j \leq 256/g$. Recall that these projections have been defined in Equation 2. In particular, the challenge sets depend on the decomposition type of the prime $p$, i.e.,

$$\mathcal{D}_g(R) = \left\{\gamma \in \mathcal{O}_L : \|\gamma\|_\infty = 1,\ \left\|\pi_j(\gamma)\right\| = R\ \forall 1 \leq j \leq 256/g\right\}. \tag{30}$$

These challenge sets can be viewed as an $256/g$-fold Cartesian product of challenge sets in the smaller cyclotomic number ring $\mathbb{Z}[\zeta_z] = \mathbb{Z}[\zeta_{2g}]$. For this reason, it follows that

$$\left|\mathcal{D}_g(R)\right| = \binom{g}{R^2}^{256/g} 2^{256R^2/g}.$$

In contrast to the challenge sets $C(R)$ the cardinality of $\mathcal{D}_g(R)$ depends on the decomposition type of $p$. More precisely, it depends on the number of prime factors $g$ of the ideal $p\mathcal{O}_L$. Hence, for different decomposition types we choose different norm bounds $R$ such that $\left|\mathcal{D}_{n,g}(R)\right| \geq 2^{237}$. In Table 2, the required norm bounds $R$ are displayed.

Table 2: Norm bounds $R$ to guarantee that challenge sets have cardinality at least $2^{237}$.

| Number of Prime Factors ($g$) | Inertia Degree ($f$) | Decomposition Type | Radius $R$ s.t. $\lvert C(R)\rvert \geq 2^{237}$ | Radius $R$ s.t. $\lvert \mathcal{D}_g(R)\rvert \geq 2^{237}$ |
|---|---|---|---|---|
| 1 | 256 | (256) | $\sqrt{53}$ | 1 |
| 2 | 128 | (128, 128) | $\sqrt{53}$ | 1 |
| 4 | 64 | (64, 64, 64, 64) | $\sqrt{53}$ | $\sqrt{2}$ |
| 8 | 32 | (32, ..., 32) | $\sqrt{53}$ | $\sqrt{3}$ |
| 16 | 16 | (16, ..., 16) | $\sqrt{53}$ | 2 |
| 32 | 8 | (8, ..., 8) | $\sqrt{53}$ | $2\sqrt{2}$ |
| 64 | 4 | (4, ..., 4) | $\sqrt{53}$ | $\sqrt{14}$ |
| 128 | 2 | (2, ..., 2) | $\sqrt{53}$ | $3\sqrt{3}$ |
| 256 | 1 | (1, ..., 1) | $\sqrt{53}$ | $\sqrt{53}$ |

From the invertibility condition of Equation 7, it follows that if

$$p > \left(\sqrt{4R^2 - 2}\right)^g,$$

then challenge differences are invertible in $\mathcal{O}_L/p\mathcal{O}_L$. This is exactly the same bound as we found in Equation 29. However, as displayed in Table 2, the norm bounds $R$ can chosen much smaller for most decomposition types.

In the analysis above we have only considered rational primes $p$ that split in factors with the same inertia degree $f = 256/g$. The cyclotomic number field $\mathbb{Q}(\zeta_{512})$ is Galois with Galois group $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/128\mathbb{Z}$. Hence, in this case, the above analysis covers all primes $p$. By contrast, the trinomial number field $\mathbb{Q}[X]/\left(X^{256} - X - 1\right)$ is not Galois. In particular, the Galois group of its Galois closure is the entire group $S_{256}$ containing 256! permutations and not all primes $p$ split into factors with the same inertia degree. By Frobenius' density theorem (Theorem 5), the density of primes that have a particular decomposition type can be determined.

In Table 3 the resulting prime sizes for the cyclotomic number field $L = \mathbb{Q}(\zeta_{512})$ are displayed. Both for the standard approach, resulting in challenge set $C(\sqrt{53}) \subset \mathcal{O}_L$, and the decomposition field approach, resulting in challenge sets $\mathcal{D}_g(R)$ are treated. In the latter approach, the norm bound $R$ depends on the decomposition type and can be found in Table 2. Moreover, this approach requires rational primes to have a cyclotomic decomposition field. The density of primes with a cyclotomic decomposition field follows from Lemma 3.

For the decomposition field approach we have computed the smallest primes $p_g$ that split in $g$ factors and are larger than the associated prime bound $P$. In particular,

$$p_2 = 5 = 2^{2,32..}, \qquad p_{16} = 2^{30,45..}, \qquad p_{128} = 2^{430,58..},$$
$$p_4 = 41 = 2^{5,35..}, \qquad p_{32} = 2^{78,51..}, \qquad p_{128} = 2^{987,42..},$$
$$p_8 = 10193 = 2^{13,31..}, \qquad p_{64} = 2^{184,15..}.$$

Hence, only for small $g$ the actual primes are slightly larger than their lower bounds $P$.

Table 3: Minimal size of primes $p$ such that non-zero challenge differences are invertible in $O_L/pO_L$, where $L = \mathbb{Q}(\zeta_{512})$. The logarithm of the prime bounds $P$ are displayed. Challenge sets are either of the form $C(\sqrt{53}) \subset O_L$, or of the form $\mathcal{D}_g(R) \subset O_L$ in the decomposition field approach.

| Number of Prime Factors ($g$) | Decomposition Type | Frobenius' Density | Prime Bound $P$ for $C(\sqrt{53})$ ($\log_2(P)$) | Density of Primes with Decomposition Field $\mathbb{Q}(\zeta_{2g})$ | Prime Bound $P$ for $\mathcal{D}_{256,g}(R)$ ($\log_2(P)$) |
|---|---|---|---|---|---|
| 1 | $(256)$ | 0 | – | 0 | – |
| 2 | $(128, 128)$ | 1/2 | 7,71.. | 1/4 | 1 |
| 4 | $(64, 64, 64, 64)$ | 1/4 | 15,42.. | 1/8 | 5,16.. |
| 8 | $(32, \ldots, 32)$ | 1/8 | 30,85.. | 1/16 | 13,28.. |
| 16 | $(16, \ldots, 16)$ | 1/16 | 61,71.. | 1/32 | 30,45.. |
| 32 | $(8, \ldots, 8)$ | 1/32 | 123,42.. | 1/64 | 78,51.. |
| 64 | $(4, \ldots, 4)$ | 1/64 | 246,85.. | 1/128 | 184,15.. |
| 128 | $(2, \ldots, 2)$ | 3/256 | 493,71.. | 1/256 | 430$v$58.. |
| 256 | $(1, \ldots, 1)$ | 1/256 | 987,42.. | 1/256 | 987,42.. |

Lyubashevsky and Seiler [41] introduced the decomposition field approach and gave an ad-hoc example of a challenge set in $\mathbb{Q}(\zeta_{512})$ in which they considered primes with $g = f = 16$. They showed that in this case primes $p$ larger than $2^{30,5}$ achieve the desired invertibility. This result can also be retrieved from Table 3.

In Table 4 the resulting prime sizes for the trinomial challenge set $C(\sqrt{53}) \subset O_L$ with $L = \mathbb{Q}[X]/(X^{256} - X - 1)$ are displayed. Since the trinomial field is not Galois we can not apply the decomposition field approach. Note that, in this case, the sum of Frobenius' densities is not equal to 1, because many other decomposition types are possible. Moreover, the densities for some decomposition types are extremely small, making it hard to find primes of these specific decomposition types. In particular, it is extremely unlikely that a rational prime $p$ completely splits in the trinomial number field $L$. Additionally these small densities are likely to cause the actual primes to be larger than the lower bounds given by Table 4.

Table 4: Minimal size of primes $p$ such that non-zero challenge differences are invertible in $O_L/pO_L$. The logarithm of the prime bounds $P$ are displayed. The challenge set is of the form $C(\sqrt{53}) \subset O_L$ with $L = \mathbb{Q}[X]/(X^{256} - X - 1)$.

| Number of Prime Factors ($g$) | Decomposition Type | Frobenius' Density | Prime Bound $P$ for $C(\sqrt{53})$ ($\log_2(P)$) |
|---|---|---|---|
| 1 | $(256)$ | $2^{-8}$ | 4,82.. |
| 2 | $(128, 128)$ | $2^{-15}$ | 9,65.. |
| 4 | $(64, 64, 64, 64)$ | $2^{-28,..}$ | 19,30.. |
| 8 | $(32, \ldots, 32)$ | $2^{-55,..}$ | 38,61.. |
| 16 | $(16, \ldots, 16)$ | $2^{-108,..}$ | 77,22.. |
| 32 | $(8, \ldots, 8)$ | $2^{-213,..}$ | 154,45.. |
| 64 | $(4, \ldots, 4)$ | $2^{-423,..}$ | 308,91.. |
| 128 | $(2, \ldots, 2)$ | $2^{-844,..}$ | 617,83.. |
| 256 | $(1, \ldots, 1)$ | $2^{-1683,..}$ | 1235,67.. |

## 7.2 CANONICAL EMBEDDING

Thus far challenge sets have been defined via the coefficient embedding $\psi_B \colon L \to \mathbb{Q}^n$ of the number field $L$. This embedding depends on the choice of (integral) basis $B = (\beta_1, \ldots, \beta_n)$ of $L/\mathbb{Q}$. These challenge sets correspond to sets of elements in the lattice $\mathbb{Z}^n$ of bounded norm. The cardinality is easily computed and with some additional restrictions we even find the closed-form expressions of Equation 27 and Equation 30. In this section we describe another approach and define challenge sets directly in the canonical embedding $\phi_L \colon L \to \mathbb{C}^n$ and use the canonical invertibility condition from Theorem 7. It turns out that, in some cases, this approach allows the protocols to be instantiated with smaller primes $p$.

We apply this approach to the cyclotomic example $L = \mathbb{Q}(\zeta_{512})$ of Section 7.1 and we directly apply the decomposition field approach. Challenge sets defined via this approach depend on the decomposition type of the prime $p$. We consider rational primes $p$ that are unramified in $L$ and have cyclotomic decomposition field $K_g = \mathbb{Q}(\zeta_{2g})$, where $g$ is the number of prime factors of the ideal $pO_L$. As before we fix the integral basis

$\left(1, \ldots, \zeta_{512}^{256/g-1}\right)$ of $L/K_g$ and, for $1 \leq j \leq 256/g$, let $\pi_j \colon L \to K_g$ be the projections associated to this basis. The canonical challenge sets are defined as follows

$$\mathcal{E}_{g,k}(R) = \left\{\gamma \in \mathcal{O}_L : \left\|\phi_{K_g}(\pi_j(\gamma))\right\|_k \leq R \ \ \forall 1 \leq j \leq 256/g\right\}, \tag{31}$$

where $\phi_{K_g} \colon L \to \mathbb{C}^g$ is the canonical embedding of $K_g$ and the radius $R \in \mathbb{R}_{\geq 0}$ is chosen such that $\left|\mathcal{E}_{g,k}(R)\right| \geq 2^{237}$. Note that the invertibility result of Theorem 7 allows us to consider norms $\|\cdot\|_k$ for arbitrary $k \in \mathbb{N} \cup \{\infty\}$. In particular, we consider the $\ell_1$- and $\ell_2$-norm.

Table 5 shows the norm bounds $R$ that are required to guarantee that challenge sets are sufficiently large. Because this cardinality lacks a closed-form expression, the norm bounds have been computed by a brute-force search. The challenge set $\mathcal{E}_{g,k}(R)$ can be viewed as an $256/g$ Cartesian product of challenge sets in the $g$-dimensional lattice $\phi_{K_g}(\mathcal{O}_{K_g})$. Hence, the computational complexity of the brute-force search depends on the number of prime factors $g$. For this reason, we have restricted this brute-force search to $g \in \{1, 2, 4, 8, 16\}$. Note that for large $R$ the cardinality of $\mathcal{E}_{g,k}(R)$ is easily approximated, for instance, by considering the volume of the fundamental domain of the lattice $\phi_{K_g}(\mathcal{O}_{K_g})$. However, for small bounds $R$ these approximations are inaccurate.

For power-of-two-cyclotomic number fields $L = \mathbb{Q}(\zeta_m)$ with power basis $B = (1, \zeta_m, \ldots, \zeta m^{m/2-1})$, the mapping $\mathrm{M}_B \colon \psi_B(L) \to \phi_L(L)$ from the canonical to the coefficient embedding is a scaled rotation, i.e., the geometries induced from these different embeddings are the same. The scaling factor of this rotation equals $s_1(m) = \sqrt{m/2}$. For this reason, the norm bounds $R_2$ of Table 5, associated to the $\ell_2$-challenge sets $\mathcal{E}_{g,2}(R_2)$, are exactly a factor $\sqrt{g}$ larger than the norm bounds $R$, associated to the challenge set $\mathcal{D}_g(R)$ of Table 2.

Table 5: Norm bounds $R_1$ and $R_2$ to guarantee that challenge sets have cardinality at least $2^{237}$.

| Number of Prime Factors ($g$) | Inertia Degree ($f$) | Decomposition Type | Radius $R_1$ s.t. $\lvert\mathcal{E}_{g,1}(R_1)\rvert \geq 2^{237}$ | Radius $R_2$ s.t. $\lvert\mathcal{E}_{g,2}(R_2)\rvert \geq 2^{237}$ |
|---|---|---|---|---|
| 1 | 256 | (256) | 1 | 1 |
| 2 | 128 | (128, 128) | 2 | $\sqrt{2}$ |
| 4 | 64 | (64, 64, 64, 64) | $2\sqrt{4+2\sqrt{2}} \approx 5{,}22..$ | $2\sqrt{2}$ |
| 8 | 32 | (32, ..., 32) | $4+4\sqrt{2+\sqrt{2}} \approx 11{,}39..$ | $2\sqrt{6}$ |
| 16 | 16 | (16, ..., 16) | 29,37.. | 8 |

From the invertibility result of Theorem 7 it follows that all non-zero challenge differences $\bar{c} \in \mathcal{E}_{g,k}(R) - \mathcal{E}_{g,k}(R)$ are invertible in $\mathcal{O}_L/p\mathcal{O}_L$ if

$$p > \left(\frac{2R}{\sqrt[k]{g}}\right)^g.$$

Hence, this expression suggests that we want to choose $k$ as small as possible, i.e., $k = 1$. However, Table 5 shows that, for all $g \in \{1, 2, 4, 8, 16\}$, the norm bound $R$ is required to be larger for $k = 1$ than for $k = 2$. This causes some instantiations to result in smaller prime bounds for $k = 1$ and others for $k = 2$.

The resulting prime sizes are displayed in Table 6. For reference, the prime size associated to challenge sets $\mathcal{D}_g(R)$ defined via the coefficient embedding are also included.

Table 6: Minimal size of primes $p$ such that non-zero challenge differences $\bar{c} \in \mathcal{E}_{g,k}(R) - \mathcal{E}_{g,k}(R)$ are invertible in $\mathcal{O}_L/p\mathcal{O}_L$. The logarithm of the prime bounds $P$ are displayed. The prime sizes associated to challenge sets $\mathcal{D}_g(R)$ defined via the coefficient embedding are also included.

| Number of Prime Factors ($g$) | Decomposition Type | Density of Primes with Decomposition Field $\mathbb{Q}(\zeta_{2g})$ | Prime Bound $P$ for $\mathcal{E}_{g,1}(R_1)$ ($\log_2(P)$) | Prime Bound $P$ for $\mathcal{E}_{g,2}(R_2)$ ($\log_2(P)$) | Prime Bound $P$ for $\mathcal{D}_g(R)$ ($\log_2(P)$) |
|---|---|---|---|---|---|
| 1 | (256) | 0 | – | – | – |
| 2 | (128, 128) | 1/4 | 2 | 2 | 1 |
| 4 | (64, 64, 64, 64) | 1/8 | 5, 54.. | 6 | 5, 16.. |
| 8 | (32, ..., 32) | 1/16 | 12, 07.. | 14, 33.. | 13, 28.. |
| 16 | (16, ..., 16) | 1/32 | 30, 01.. | 32 | 30, 45.. |

Table 6 shows that the prime sizes for canonical $\ell_2$-challenge set $\mathcal{E}_{g,2}(R_2)$ are very similar to the ones for the challenge sets $\mathcal{D}_g(R)$. This is because both the canonical and coefficient geometry are equivalent for power-of-two cyclotomic number fields. However, there still is a difference between the two columns. This difference can be

explained by the fact that the challenges sets $\mathcal{D}_g(R)$ of Section 7.1 were defined slightly differently to make them amenable for the ad-hoc improvement of Lemma 10. Further, Table 6 shows that for primes that split in at least 8 factors in $L$, we can indeed achieve slightly smaller prime sizes by considering the $\ell_1$-norm in the canonical embedding.

## 8 ACKNOWLEDGEMENTS

We would like to thank Koen de Boer, Benjamin Wesolowski and Léo Ducas for their comments and the insightful discussions we had on this topic. Moreover, we would especially like to thank Wessel van Woerden for his help in the implementation of the computations required for Section 7.2. Further, we are extremely grateful for the extensive review comments, helping us to improve the paper significantly. Thomas Attema has been supported by EU H2020 project No 780701 (PROMETHEUS). Ronald Cramer has been supported by ERC ADG project No 74079 (ALGSTRONGCRYPTO) and by the NWO Gravitation project QSC.

## REFERENCES

[1] Martin R. Albrecht, Shi Bai, and Léo Ducas. "A Subfield Lattice Attack on Overstretched NTRU Assumptions - Cryptanalysis of Some FHE and Graded Encoding Schemes". In: *CRYPTO (1)*. Vol. 9814. Lecture Notes in Computer Science. Springer, 2016, pp. 153–178.

[2] Hayo Baan, Sauvik Bhattacharya, Scott R. Fluhrer, Óscar García-Morchón, Thijs Laarhoven, Ronald Rietman, Markku-Juhani O. Saarinen, Ludo Tolhuizen, and Zhenfei Zhang. "Round5: Compact and Fast Post-quantum Public-Key Encryption". In: *PQCrypto*. Vol. 11505. Lecture Notes in Computer Science. Springer, 2019, pp. 83–102.

[3] Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafaël del Pino, Jens Groth, and Vadim Lyubashevsky. "Sublinear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits". In: *CRYPTO (2)*. Vol. 10992. Lecture Notes in Computer Science. Springer, 2018, pp. 669–699.

[4] Carsten Baum, Ivan Damgård, Kasper Green Larsen, and Michael Nielsen. "How to Prove Knowledge of Small Secrets". In: *CRYPTO (3)*. Vol. 9816. Lecture Notes in Computer Science. Springer, 2016, pp. 478–498.

[5] Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. "More Efficient Commitments from Structured Lattice Assumptions". In: *SCN*. Vol. 11035. Lecture Notes in Computer Science. Springer, 2018, pp. 368–385.

[6] Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. "Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings". In: *ESORICS (1)*. Vol. 9326. Lecture Notes in Computer Science. Springer, 2015, pp. 305–325.

[7] Daniel J Bernstein. "Multidigit Multiplication for Mathematicians". In: *Advances in Applied Mathematics* (2001), pp. 1–19.

[8] Daniel J. Bernstein. *A Subfield-Logarithm Attack Against Ideal Lattices*. http://blog.cr.yp.to/20140213-ideal.html. Blog. 2014.

[9] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. "NTRU Prime: Reducing Attack Surface at Low Cost". In: *SAC*. Vol. 10719. Lecture Notes in Computer Science. Springer, 2017, pp. 235–260.

[10] Jean-François Biasse and Fang Song. "Efficient Quantum Algorithms for Computing Class Groups and Solving the Principal Ideal Problem in Arbitrary Degree Number Fields". In: *SODA*. SIAM, 2016, pp. 893–902.

[11] Piers Bohl. "Zur Theorie der trinomischen Gleichungen". In: *Mathematische Annalen* 65.4 (1908), pp. 556–566.

[12] Jonathan Bootle, Vadim Lyubashevsky, and Gregor Seiler. "Algebraic Techniques for Short(er) Exact Lattice-Based Zero-Knowledge Proofs". In: *CRYPTO (1)*. Vol. 11692. Lecture Notes in Computer Science. Springer, 2019, pp. 176–202.

[13] Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. "Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE". In: *ACM Conference on Computer and Communications Security*. ACM, 2016, pp. 1006–1018.

[14] Wieb Bosma. "Canonical Bases for Cyclotomic Fields". In: *Appl. Algebra Eng. Commun. Comput.* 1 (1990), pp. 125–134.

[15] Peter Campbell, Michael Groves, and Dan Shepherd. "Soliloquy: A cautionary tale". In: *ETSI 2nd Quantum-Safe Crypto Workshop*. 2014, pp. 1–9.

[16] Hao Chen, Kristin E. Lauter, and Katherine E. Stange. "Vulnerable Galois RLWE Families and Improved Attacks". In: *IACR Cryptol. ePrint Arch.* 2016 (2016), p. 193.

[17] Ronald Cramer and Ivan Damgård. "On the Amortized Complexity of Zero-Knowledge Protocols". In: *CRYPTO*. Vol. 5677. Lecture Notes in Computer Science. Springer, 2009, pp. 177–191.

[18] Ronald Cramer, Ivan Damgård, Chaoping Xing, and Chen Yuan. "Amortized Complexity of Zero-Knowledge Proofs Revisited: Achieving Linear Soundness Slack". In: *EUROCRYPT (1)*. Vol. 10210. Lecture Notes in Computer Science. 2017, pp. 479–500.

[19] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. "Recovering Short Generators of Principal Ideals in Cyclotomic Rings". In: *EUROCRYPT (2)*. Vol. 9666. Lecture Notes in Computer Science. Springer, 2016, pp. 559–585.

[20] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. "Short Stickelberger Class Relations and Application to Ideal-SVP". In: *EUROCRYPT (1)*. Vol. 10210. Lecture Notes in Computer Science. 2017, pp. 324–348.

[21] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. "Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time". In: *J. ACM* 68.2 (2021), 8:1–8:26.

[22] Ronald Cramer and Serge Fehr. "Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups". In: *CRYPTO*. Vol. 2442. Lecture Notes in Computer Science. Springer, 2002, pp. 272–287.

[23] Ronald Cramer, Serge Fehr, and Martijn Stam. "Black-Box Secret Sharing from Primitive Sets in Algebraic Number Fields". In: *CRYPTO*. Vol. 3621. Lecture Notes in Computer Science. Springer, 2005, pp. 344–360.

[24] Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart. "Practical Covertly Secure MPC for Dishonest Majority - Or: Breaking the SPDZ Limits". In: *ESORICS*. Vol. 8134. Lecture Notes in Computer Science. Springer, 2013, pp. 1–18.

[25] Yvo Desmedt and Yair Frankel. "Perfect Homomorphic Zero-Knowledge Threshold Schemes over any Finite Abelian Group". In: *SIAM J. Discret. Math.* 7.4 (1994), pp. 667–679.

[26] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. "Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model". In: *CRYPTO (2)*. Vol. 11693. Lecture Notes in Computer Science. Springer, 2019, pp. 356–383.

[27] Léo Ducas and Alain Durmus. "Ring-LWE in Polynomial Rings". In: *Public Key Cryptography*. Vol. 7293. Lecture Notes in Computer Science. Springer, 2012, pp. 34–51.

[28] Amos Fiat and Adi Shamir. "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *CRYPTO*. Vol. 263. Lecture Notes in Computer Science. Springer, 1986, pp. 186–194.

[29] Ferdinand G. Frobenius. "Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe". In: *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1896), pp. 689–703.

[30] Sanjam Garg, Craig Gentry, and Shai Halevi. "Candidate Multilinear Maps from Ideal Lattices". In: *EUROCRYPT*. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 1–17.

[31] Craig Gentry and Michael Szydlo. "Cryptanalysis of the Revised NTRU Signature Scheme". In: *EUROCRYPT*. Vol. 2332. Lecture Notes in Computer Science. Springer, 2002, pp. 299–320.

[32] Serge Lang. *Algebra*. 3rd ed. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag New York, 2002. ISBN: 978-0-387-95385-4. DOI: 10.1007/978-1-4613-0041-0.

[33] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. "GGHLite: More Efficient Multilinear Maps from Ideal Lattices". In: *EUROCRYPT*. Vol. 8441. Lecture Notes in Computer Science. Springer, 2014, pp. 239–256.

[34] Hendrik W. Lenstra. "Euclidean Number Fields of Large Degree". In: *Inventiones Mathematicae* 38.3 (1976), pp. 237–254.

[35] Qipeng Liu and Mark Zhandry. "Revisiting Post-quantum Fiat-Shamir". In: *CRYPTO (2)*. Vol. 11693. Lecture Notes in Computer Science. Springer, 2019, pp. 326–355.

[36] Vadim Lyubashevsky. "Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures". In: *ASIACRYPT*. Vol. 5912. Lecture Notes in Computer Science. Springer, 2009, pp. 598–616.

[37] Vadim Lyubashevsky. "Lattice Signatures without Trapdoors". In: *EUROCRYPT*. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 738–755.

[38] Vadim Lyubashevsky and Gregory Neven. "One-Shot Verifiable Encryption from Lattices". In: *EUROCRYPT (1)*. Vol. 10210. Lecture Notes in Computer Science. 2017, pp. 293–323.

[39] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *EUROCRYPT*. Vol. 6110. Lecture Notes in Computer Science. Springer, 2010, pp. 1–23.

[40] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "A Toolkit for Ring-LWE Cryptography". In: *EUROCRYPT*. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 35–54.

[41] Vadim Lyubashevsky and Gregor Seiler. "Short, Invertible Elements in Partially Splitting Cyclotomic Rings and Applications to Lattice-Based Zero-Knowledge Proofs". In: *EUROCRYPT (1)*. Vol. 10820. Lecture Notes in Computer Science. Springer, 2018, pp. 204–224.

[42] Jürgen Neukirch. *Algebraic Number Theory*. 1st ed. Vol. 322. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag Berlin Heidelberg, 1999. ISBN: 978-3-540-65399-8.

[43] Hiroyuki Osada. "The Galois Groups of the Polynomials $X^n + aX^l + b$". In: *Journal of Number Theory* 25 (1987), pp. 230–238.

[44] Chris Peikert and Zachary Pepin. "Algebraically Structured LWE, Revisited". In: *TCC (1)*. Vol. 11891. Lecture Notes in Computer Science. Springer, 2019, pp. 1–23.

[45] Rafaël del Pino, Vadim Lyubashevsky, and Gregor Seiler. "Lattice-Based Group Signatures and Zero-Knowledge Proofs of Automorphism Stability". In: *ACM Conference on Computer and Communications Security*. ACM, 2018, pp. 574–591.

[46] Claus-Peter Schnorr. "Efficient Identification and Signatures for Smart Cards". In: *CRYPTO*. Vol. 435. Lecture Notes in Computer Science. Springer, 1989, pp. 239–252.

[47] Ernst S. Selmer. "On the Irreducibility of Certain Trinomials". In: *Mathematica Scandinavica* (1957), pp. 287–302.

[48] Nigel P. Smart and Frederik Vercauteren. "Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes". In: *Public Key Cryptography*. Vol. 6056. Lecture Notes in Computer Science. Springer, 2010, pp. 420–443.

[49] Ron Steinfeld, Amin Sakzad, and Raymond K. Zhao. *Titanium*. Tech. rep. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions`. National Institute of Standards and Technology, 2017.

[50] Thorsten Theobald and Timo de Wolff. "Norms of Roots of Trinomials". In: *Mathematische Annalen* 366.1 (2016), pp. 219–247.

[51] Nikolai Tschebotareff. "Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören". In: *Mathematische Annalen* 95.1 (1926), pp. 191–228.

[52] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. 2nd ed. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag New York, 1997. ISBN: 978-1-4612-7346-2.

[53] Rupeng Yang, Man Ho Au, Zhenfei Zhang, Qiuliang Xu, Zuoxia Yu, and William Whyte. "Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications". In: *CRYPTO (1)*. Vol. 11692. Lecture Notes in Computer Science. Springer, 2019, pp. 147–175.