A note on short invertible ring elements and applications to cyclotomic and trinomials number fields

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

[1] CWI, The Netherlands
[2] TNO, The Netherlands
[3] Leiden University, The Netherlands
[4] Nanyang Technological University, Singapore.

Abstract. Ring-SIS based Σ-protocols require the construction of a challenge set $\mathcal{C}$ in some ring R, usually an order in a number field L. These protocols impose various requirements on the subset $\mathcal{C}$, and constructing a good or even optimal challenge set is a non-trivial task that involves making various trade-offs.
In particular, the set $\mathcal{C}$ should be 'large', elements in $\mathcal{C}$ should be 'small', differences of distinct elements in $\mathcal{C}$ should be invertible modulo a rational prime p, this prime p should be small, and finally primes p that split in many factors are favorable. Clearly, these requirements on $\mathcal{C}$ require certain trade-offs. The splitting behavior and size of the prime p, for example, influence the invertibility condition.
Given an order $\mathcal{O}$ in an arbitrary number field L, this work aims at constructing subsets $\mathcal{C} \subset \mathcal{O}$ with precisely the above mentioned properties. Cyclotomic number fields possess some convenient properties and as a result most protocols are defined over these specific fields. However, recent attacks have shown that these convenient properties might also be of use to an attacker, thereby weakening or even breaking the cryptographic schemes.
In this paper, we show that a known result on constructing challenge sets in cyclotomic number fields [LS18] follows from standard Galois theory, thereby simplifying the proof. In addition, this approach leads to a natural generalization from cyclotomic to arbitrary number fields. Along the way we prove a conjectured result on the practical applicability for cyclotomic number fields and prove the optimality of certain constructions. We apply the generalization 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. Finally, we find a new construction for challenge sets resulting in smaller prime sizes at the cost of slightly increasing the ℓ_2-norm of the challenges.

Keywords: Lattice, zero-knowledge proof, challenge set, invertibility, trinomials, number theory.

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 number-theoretic setting, Schnorr suggested an elegant and efficient interactive protocol for producing these so-called zero-knowledge proofs [Sch89]. 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 [FS86]. Recently the Fiat-Shamir transformation has proven to be secure in the Quantum Random Oracle Model [DFMS19, LZ19].

Lattice based Σ-protocols require, in addition, a proof that the pre-image is 'short'. Because of this additional requirement, it has proven to be challenging to adopt Schnorr's approach to the lattice setting.

Firstly an honest prover might be restricted to choose pre-images from a set that is smaller than the set the pre-image can be proven to belong to, i.e. $\mathcal{P}$ knows a pre-image in some set S but can only prove 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 [Lyu09, Lyu12] significantly reduces the soundness slack.

Secondly, in contrast to the number-theoretic protocols, many lattice based Σ-protocols suffer from a large soundness error and have to be repeated many times to achieve the desired security level. The number of repetitions is also called the *overhead* of the protocol and until recently no approaches were known to significantly reduce this overhead. The first Ring-SIS based protocols achieving a small soundness error were proposed at CRYPTO '19 [BLS19, YAZ+19]. The proposed solutions do result in larger proof sizes and still have to be repeated a small number of times.

In contrast to proving knowledge of a single pre-image, when proving the knowledge of many pre-images the amortized overhead can be reduced significantly without increasing the soundness slack [CD09, DKL+13, BDLN16, CDXY17, BBC+18].

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 [LS18].

A key component in (approximate) Σ-protocols is the challenge set $\mathcal{C}$. In this work we focus on the protocols based on the Ring-SIS assumption. These protocols work over a ring R/p where 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 ζ_m with minimal polynomial $\Phi_m(X)$.

The efficiency of these protocols critically depends on the choice of a good challenge set $\mathcal{C} \subset R/p$. The Ring-SIS hardness condition requires elements in $\mathcal{C}$ to have small norm. The approximation factor is determined by the norms of the challenges in $\mathcal{C}$. To achieve a small soundness error, the set $\mathcal{C}$ should be large ($|\mathcal{C}| \approx 2^{256}$). And for practical efficiency the prime p should be as small as possible. Additional efficiency improvements can be obtained by using the Chinese-Remainder Theorem [Ber01], for which the added value depends on the splitting behavior of the rational prime p in the ring R. In fact, the more distinct prime factors p has in R, the more efficient elementary operations in R/p 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 $c, c' \in \mathcal{C}$ might be required to be invertible in R/p [BKLP15, LN17, BDL+18, dPLS18].

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

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

When R is the ring of integers of a number field K, a subset $E \subset R$ 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 $L(K)$ of K [Len76] 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 [DF94, CF02, CFS05]. However, our situation is slightly different. Firstly, we only require mutual differences to be invertible modulo a rational prime p and, secondly, we additionally require elements to be small.

The above requirements introduce compromises between, for example, the invertibility condition and the splitting behavior of the prime p. Lyubashevsky and Seiler [LS18] showed that, when 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 $\mathcal{C} \subset R/p$ 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 ζ_m, φ 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 ([LS18]). *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 $\mathbb{Z}[X]/(p)$. Furthermore, any $\mathbf{y} \in \mathbb{Z}[X]/(p, \Phi_m(X))$ that satisfies either

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

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

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

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 R, find an arbitrary generator $g \in R$ 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 [BS16] 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 $u \in R^*$. 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 $\mathrm{Log}(R^*)$ [Ber14, CGS14]. Using this observation, a polynomial time algorithm for cyclotomic number fields with power-of-two conductor was claimed to be found [CGS14]. A generalization to prime-power cyclotomic number fields accompanied with a rigorous proof was given in [CDPR16]. Moreover, strong evidence was found that these types of attacks are not restricted to principal ideals [CDW17].

Fortunately, only a handful of cryptographic primitives [SV10, GGH13, LSS14, CGS14] rely directly on the hardness of of the *Short Generator Principal Ideal Problem* (SG-PIP) and are therefore broken by this type of attack.

In addition, Bernstein [Ber14] warned for the possibility of exploiting subfields. Subfield lattice attacks were originally proposed in [GS02] and generalized in [ABD16]. 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 by removing all ring structure and to work over unstructured lattices [BCD+16, SSZ17]. Another approach is to only use number fields that contain no

non-trivial subfields [BCLvV17, BGL+18]. Bernstein [Ber14] proposed the use of the ring $\mathbb{Z}[X]/(p, f)$ with $f = X^n - X - 1$ (n prime) irreducible modulo the rational prime p. The field of fractions of this ring has no proper subfields. In this work, we will consider the more general situation in which $f = X^n + aX^k + b \in \mathbb{Z}[X]$ ($k < n$) is an irreducible trinomial.

1.1 Contributions

In this work we slightly reformulate Theorem 1 to obtain Theorem 2. The differences between the two are that the original theorem contains additional conditions required for the existence of primes of the appropriate form, and that it treats the explicit factorization of cyclotomic polynomials. Besides these differences both Theorems are equivalent.

The main contribution of this work is fourfold:

1. The reformulation of Theorem 1 induces a simplified proof that follows from standard Galois theory. Firstly, we recognize the implicit use of decomposition fields in [LS18]. Utilizing known results on decomposition fields allows us to avoid the use of explicit expressions of field elements. Secondly, we relate the invertibility condition of the theorem to the algebraic norm of number field elements, which avoids the construction of a lattice $\mathcal{L}$ and the use of lattice theory to prove invertibility.
2. The practical applicability of this theorem depends on size of the values $s_1(m)$ and $s_1(z)$. In [LS18], an upper bound for these values is conjectured and in this work we prove this upper bound. Moreover, we show precisely which bases of cyclotomic number fields with prime power conductor are optimal.
3. Moreover, this new formulation induces a natural generalization from cyclotomic number fields to arbitrary number fields. In Section 6, we present the generalization of Theorem 2 and in Section 7 we show the applicability to the class of rings $R \cong \mathbb{Z}[X]/(f)$ where f is a trinomial. Finally, we compare the resulting parameters of a specific trinomial number field to those of a power-of-two cyclotomic number field.
4. Finally, we introduce a new method for defining challenge sets directly in the canonical embedding of the number field. This opens the possibility to consider challenges that are bounded in the ℓ_1-norm which indeed gives us better bounds for the rational primes of the considered Σ-protocols at the cost of increasing the ℓ_2-norm of the challenges. This trade-off is considered for a power-of-two cyclotomic number field.

Theorem 2 (Invertibility). *Let $\mathcal{O}_L$ be the ring of integers in a cyclotomic number field $L = \mathbb{Q}(\zeta_m)$ of conductor m, let $z \mid m$ and let p be a rational prime with $p \equiv 1 \mod z$ and $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z)$. Then for $\gamma \in \mathcal{O}_L/p$, it holds that if*

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

$$0 < ||\gamma||_\infty < \frac{1}{s_1(z)} p^{1/\varphi(z)}, \tag{2}$$

then γ is invertible in $\mathcal{O}_L/p$.

2 Preliminaries

Let $L = \mathbb{Q}(\zeta_m)$ be 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 $k, l \in \mathbb{Z}_{>0}$ that are relatively prime. The degree of L over $\mathbb{Q}$ is $n = \varphi(m)$, $L/\mathbb{Q}$ is Galois with Galois group $G = \{\sigma_i : 0 \le i \le n-1\}$ and $L/\mathbb{Q}$ has integral basis $B_m = \left(\zeta_m^i\right)_{0 \le i \le n-1}$. Moreover, for any $z \mid m$ we define $B_m^z = \left(\zeta_m^i\right)_{0 \le i \le \varphi(m)/\varphi(z)-1}$ as a basis for L over $K = \mathbb{Q}(\zeta_z)$. The basis B_m^z gives rise to natural projections

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

Since B_m^z is a basis, for all ideals I of K and for all $\gamma \in L$ it holds that

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

The coefficient embedding

$$\psi_m : L \to \mathbb{Q}^n, \quad \sum_{i=0}^{n-1} y_i \zeta_m^i \mapsto \begin{pmatrix} y_0 \\ \vdots \\ y_{n-1} \end{pmatrix},$$

equips L with a geometry. Note that if $z \mid m$ and $\gamma \in K = \mathbb{Q}(\zeta_z)$, the ℓ_2-norms defined over K and over L are identical, and the same holds for the ∞-norm. Moreover, it clearly holds that

$$||\gamma||_\infty := ||\psi_m(\gamma)||_\infty = \max_{0 \le j \le \varphi(m)/\varphi(z)-1} ||\pi_j(\gamma)||_\infty,$$
$$||\gamma|| := ||\psi_m(\gamma)|| = \sqrt{\sum_{j=0}^{\varphi(m)/\varphi(z)-1} ||\pi_j(\gamma)||^2}.$$

Another way of equipping the number field L with a geometry is via the canonical embedding

$$f : L \to \mathbb{C}^n, \quad \gamma \mapsto \begin{pmatrix} \sigma_0(\gamma) \\ \vdots \\ \sigma_{n-1}(\gamma). \end{pmatrix}$$

The relation between the coefficient and canonical embedding is depicted in Figure 1, where M_m is the unique linear mapping that makes this diagram commute. Hence, the matrix M_m is given by

$$\mathrm{M}_m = \left(\sigma_i(\zeta_m^j)\right)_{0 \le i,j \le n-1} \in L^{n \times n}.$$

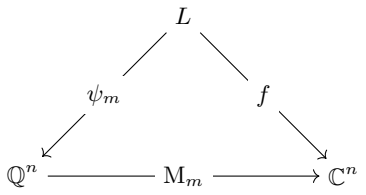

Fig. 1. Coefficient and canonical embedding of $L = \mathbb{Q}(\zeta_m)$.

Moreover, we let $s_1(m) := s_1(\mathrm{M}_m)$ denote the largest singular value of M_m, i.e.

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

Let now $z \mid m$ be some integer and suppose that $p \nmid m$ is 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 $p^{\varphi(m)/\varphi(z)} \equiv 1 \mod m$. Then p splits into $\varphi(z)$ distinct primes in L [Was97, Theorem 2.13]. If, in addition, $p \equiv 1 \mod z$, we find that p splits in $\varphi(z)$ distinct factors, hence completely, in $K = \mathbb{Q}(\zeta_z) \subset L$. In particular, K is the decomposition field of all primes $\mathfrak{p}|p$ in L. Recall that the decomposition group of a prime $\mathfrak{p}$ is the subgroup of G that fixes $\mathfrak{p}$ and its fixed field is the decomposition field of $\mathfrak{p}$. In this case, it follows that p splits completely in K and $\mathfrak{p} \cap K$ is inert in L for all $\mathfrak{p}|p$.

3 Invertibility of integral elements in a cyclotomic number field

We are now ready to prove Theorem 2.

Proof (Proof of Theorem 2). We first prove that inequality 1 gives a sufficient condition for $\gamma \in \mathcal{O}_L$ to be invertible in $\mathcal{O}_L/p$. For any $\gamma \in \mathcal{O}_L$ it follows, by the inequality of the arithmetic and the geometric mean, that

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

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

$$\begin{aligned} \left|\mathrm{N}_{L/\mathbb{Q}}(\gamma)\right|^{2/\varphi(m)} &\leq \frac{s_1(m)^2}{\varphi(m)} ||\psi_m(\gamma)||^2, \\ &= \frac{s_1(m)^2}{\varphi(m)} ||\gamma||^2. \end{aligned} \tag{3}$$

Now suppose Equation 1 holds. Substituting this equation in inequality 3 and raising both sides to the power $\varphi(m)/2$ gives

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

But 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 γ satisfies Equation 1, it holds that

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

for any prime $\mathfrak{p} \subset \mathcal{O}_L$ above p. Therefore $\gamma \notin \mathfrak{p}$ and thus $\gamma \in (\mathcal{O}_L/\mathfrak{p})^*$ for all $\mathfrak{p} \mid p$. Hence, γ is invertible in $\mathcal{O}_L/p$, which proves the first claim.

We now prove that inequality 2 gives a sufficient condition for γ to be invertible in $\mathcal{O}_L/p$. Let $\mathfrak{p} \subset L$ be a prime above p and let $K = \mathbb{Q}(\zeta_z) \subset L$. Since $p \equiv 1 \mod z$ and $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z)$, the decomposition field of $\mathfrak{p}$ is K and the prime $\mathfrak{P} = \mathfrak{p} \cap K$ is inert in L, i.e. $\mathfrak{p} = \mathfrak{P}\mathcal{O}_L$.

Let $\pi_j : K \to L$ for $0 \leq j \leq \varphi(m)/\varphi(z) - 1$ be the projections associated to basis B_m^z of L over K and let γ be such that it satisfies Equation 2. We will show that there exists a j such that $\pi_j(\gamma) \in (\mathcal{O}_K/\mathfrak{P})^*$ from which it follows that $\gamma \in (\mathcal{O}_L/\mathfrak{p})^*$.

Since

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

there exists a j such that

$$0 < ||\pi_j(\gamma)|| < \frac{\sqrt{\varphi(z)}}{s_1(\mathrm{M}_z)} p^{1/\varphi(z)}.$$

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 $\pi_j(\gamma)$ is invertible in $\mathcal{O}_K/\mathfrak{P}$. Since $\mathfrak{P}$ is inert in L, it follows that $\pi_j(\gamma) \in (\mathcal{O}_L/\mathfrak{p})^*$ and, hence, $\gamma \in (\mathcal{O}_L/\mathfrak{p})^*$. Since $\mathfrak{p} \mid p$ was arbitrary, it follows that $\gamma \in (\mathcal{O}_L/p)^*$, which proves the second part of the theorem.

To show that Theorem 2 is not an empty statement, we prove the existence of primes p satisfying the conditions in this theorem. The following lemma gives sufficient conditions for the existence of infinitely many primes p satisfying the conditions of Theorem 2. A similar proof of this lemma was already given in [LS18]. Recall that the radical of an integer n is given by

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

Lemma 1 (Existence). *Let z, m be integers such that $z \mid m$. If $\mathrm{rad}(m) = \mathrm{rad}(z)$, and $8 \mid m$ only if $4 \mid z$, then there exist infinitely many primes p such that $p = 1 \mod z$ and $\mathrm{ord}_m(p) = \varphi(m)/\varphi(z) = m/z$.*

Proof. Let $m = \prod_{i=1}^{g} p_i^{e_i}$ and $z = \prod_{i=1}^{g} p_i^{f_i}$ with $0 \leq f_i \leq e_i$ 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 $\mathrm{Ker} = \ker(\psi) = \{x \in (\mathbb{Z}/m\mathbb{Z})^* : x \equiv 1 \mod z\}$. We first show that Ker contains an element of order $\varphi(m)/\varphi(z)$. Note that $\varphi(m)/\varphi(z) = m/z$, because $\mathrm{rad}(m) = \mathrm{rad}(z)$.

Now note that

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

Since $\mathrm{rad}(m) = \mathrm{rad}(z)$, it follows that $f_i \geq 1$ for all i, and

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

Since $8 \mid m$ only if $4 \mid z$, it follows that

$$\mathrm{Ker} \cong \prod_{i=1}^{g} \mathbb{Z}/p_i^{e_i - f_i}\mathbb{Z}.$$

Hence Ker is cyclic and contains an element of order m/z. By Dirichlet's theorem on arithmetic progressions it follows that there are infinitely many primes p with $\mathrm{ord}_m(p) = m/z$ and $p \equiv 1 \mod z$, which proves the lemma.

4 Singular values for cyclotomic number fields

The applicability of Theorem 2 depends on the size of the values $s_1(m)$ and $s_1(z)$, and in [LS18] an upper bound for these values was conjectured. In this section we prove this upper bound.

Recall that $s_1(m)$ is the largest singular value of the matrix

$$\mathrm{M}_m = \left(\sigma_i(\zeta_m^j)\right)_{0 \leq i,j \leq n-1}.$$

In [LPR13] it was already shown that the following equality holds for prime powers $m = p^k$:

$$s_1(m) = \sqrt{\tau(m)}, \tag{4}$$

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 4 does not hold, but Lyubashevsky and Seiler [LS18] 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 4 [LPR13]. To this end, let us consider the $n \times m$ matrix

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

Recall that $n = \varphi(m)$ and note that the matrix M_m is an $n \times n$ submatrix of $\mathcal{A}_m$, and therefore

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

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,

$$\mathcal{A}_m = \mathcal{A}_{p_1^{e_1}} \otimes \cdots \otimes \mathcal{A}_{p_g^{e_g}}. \tag{5}$$

Recall that primitive roots of unity are chosen such that $\zeta_{kl} = \zeta_k \zeta_l$ for all $k, l \in \mathbb{Z}_{>0}$ that are relatively prime.

Lemma 2. *Let $\mathcal{B}_m := \mathcal{A}_m^\dagger \mathcal{A}_m$, then*

$$\mathcal{B}_m = \left(\mathrm{Tr}_{L/\mathbb{Q}}\left(\zeta_m^{l-k}\right)\right)_{0 \leq k,l \leq m-1}. \tag{6}$$

Moreover

$$\mathrm{Tr}_{L/\mathbb{Q}}\left(\zeta_m^k\right) = \frac{\varphi(m)}{\varphi(m/\gcd(m,k))}\mu(m/\gcd(m,k)), \tag{7}$$

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 6.

Moreover, ζ_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 7.

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 2 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,

$$\mathcal{B}_m = \mathcal{B}_{p^e} = p^{e-1}\mathcal{B}_p \otimes \mathbb{I}_{p^{e-1}}, \tag{8}$$

and

$$\mathcal{B}_p = p\mathbb{I}_p - \mathbf{1}_p \mathbf{1}_p^T, \tag{9}$$

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

The $m \times m$ matrix $\mathcal{B}_m$ of Lemma 2 is of interest since the largest singular value of any matrix A equals the square root of the largest eigenvalue of $A^\dagger A$. The following lemma shows that the matrix $\mathcal{B}_m$ only has two different eigenvalues.

Proposition 1. *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 5 it follows that

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

Hence, it suffices to prove the statement for prime powers m. 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 proposition.

By Proposition 1 it therefore follows that

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

Now note that if $2 \mid m$, the following identity holds for some matrix $A \in \mathbb{C}^{n/2 \times m}$:

$$\mathcal{A}_m = (A, -A).$$

Hence, instead of the matrix $\mathcal{A}_m$ we can also consider the matrix

$$\tilde{\mathcal{A}}_m = \left(\mathrm{M}(\zeta_m^k)\right)_{1 \leq k \leq \tau(m)},$$

and obtain the following slightly stronger result that was conjectured in [LS18].

Proposition 2 (Conjecture 2.6 of [LS18]). *For all positive integers m, $s_1(m) \leq \sqrt{\tau(m)}$.*

Since all columns of the matrix 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

$$\sqrt{\varphi(m)} \leq s_1(m) \leq \sqrt{\tau(m)}, \tag{10}$$

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

5 Optimal basis for cyclotomic number fields

In the previous section we have proven an upper and a lower bound for the largest singular value $s_1(m)$ of the matrix M_m. This matrix was constructed from the power basis $1, \zeta_m, \dots, \zeta_m^{n-1}$ of $L = \mathbb{Q}(\zeta_m)$. A question that remains is whether we can find another integral basis $B = \{\alpha_0, \dots, \alpha_{n-1}\}$ with the same or even a smaller largest singular value associated to it. To this end, let us consider the matrix

$$\mathrm{M}_B = (\sigma_i(\alpha_j))_{0 \leq i,j \leq n-1} \in L^{n \times n},$$

and define $s_1(B)$ to be its largest singular value. From the following lemma it follows that the lower bound of Equation 10 does not only hold for the power basis, but for all integral bases of L.

Lemma 3. *Let B be an integral basis of $\mathbb{Q}(\zeta_m)$, then for all $\alpha \in B$, it holds that*

$$\left\| (\sigma_i(\alpha))_{0 \leq i \leq n-1} \right\| \geq \sqrt{\varphi(m)}.$$

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

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

$$\frac{1}{n}\left\|(\sigma_i(\alpha))_{0\le i\le n-1}\right\|^2 \ge \left|\mathrm{N}_{L/\mathbb{Q}}(\alpha)\right|^{1/n},$$

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

$$\left\|(\sigma_i(\alpha))_{0\le i\le n-1}\right\| \ge \sqrt{n} = \sqrt{\varphi(m)},$$

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

Corollary 1. *Let B be an integral basis of $\mathbb{Q}(\zeta_m)$, then $s_1(B) \ge \sqrt{\varphi(m)}$.*

Proof. Let $\alpha \in B$, then $(\sigma_i(\alpha))_{0\le i\le n-1}$ is a column of M_B and

$$s_1(B) \ge \left\|(\sigma_i(\alpha))_{0\le i\le n-1}\right\|.$$

The corollary now follows from Lemma 3.

The following theorem shows, for m a prime power, that any basis B with $s_1(B) \le \sqrt{\tau(m)}$ can only contain roots of unity (up to sign).

Theorem 3. *Let $m = p^e$ be a prime power and let B be a basis of $\mathbb{Q}(\zeta_m)$ with $s_1(B) \le \sqrt{\tau(m)}$, 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

$$\mathrm{M}_m\, x = (\sigma_0(\alpha), \ldots, \sigma_{n-1}(\alpha))^T.$$

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

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

If $\|\mathrm{M}_m\, x\| = \sqrt{\varphi(m)}$ the theorem follows from Lemma 3, so we are left to consider the case

$$\sqrt{\varphi(m)} < \|\mathrm{M}_m\, x\| \le \sqrt{\tau(m)}. \tag{11}$$

If $p = 2$, then $\tau(m) = \varphi(m) = m/2$ and Equation 11 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 8 and 9 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 11, it follows that

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

which implies

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

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 $1 \le i \le p^{e-1}$, 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 3), we see that there is exactly one i such that y_i is non-zero (recall that p is odd). Hence,

$$x^T G_m x = p^{e-1} y_i^T G_p y_i = p^e \|y_i\|^2 - p^{e-1} \left(\sum_{j=1}^{p-1} y_{ij} \right)^2 = p^e. \tag{12}$$

It now follows that

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

Hence,

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

Substituting in Equation 12 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 12, $\|y_i\| = \|x\| = 1$ 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.

The proof of Theorem 3 uses the fact that, for prime powers m, all non-zero elements of the complex lattice

$$\{\gamma \in \mathbb{C}^n : \gamma = \mathrm{M}_m\, x \text{ for some } x \in \mathbb{Z}^n\}$$

with norm less than or equal to $\sqrt{m}$ have norm $\sqrt{\varphi(m)}$ and therefore correspond to roots of unity (up to sign). This proof does not 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 $\left\| (\sigma_i(\alpha))_{0 \leq i \leq n-1} \right\|^2 = 12$, hence

$$\varphi(m) = 8 < \left\| (\sigma_i(\alpha))_{0 \leq i \leq n-1} \right\|^2 < 15 = \tau(m).$$

At this point we have shown that for prime powers $m = p^e$, any integral basis of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ with $s_1(B) \leq \sqrt{\tau(m)}$ can only contain roots of unity (up to sign). What remains to show is whether the remaining candidate bases are all optimal or whether some bases result in smaller singular values than others.

Theorem 4. *Let $m = p^e$ be an odd prime power and let*

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

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 $0 \leq j \leq p^e - 1$, 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 form Theorem 3.2 of [Bos90].

Theorem 4 shows that any basis containing only m^{th}-roots of unity can be constructed by choosing one of the p possible bases of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ for all $0 \leq j \leq p^{e-1}-1$. Hence, there exist precisely $p^{p^{e-1}}$ of these bases. The following theorem shows that all these bases have a largest singular value of exactly $\sqrt{m}$ and that there does not exist an integral basis of $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ with $s_1(B) < \sqrt{m}$.

Theorem 5. *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 $s_1(B) = \sqrt{\tau(m)}$.

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 2. Hence for all $0 \leq i, j \leq n-1$ 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 4, 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 4 it follows that $s_1(B) = \sqrt{m}$ which proves the theorem.

When m a composite number the above theorem does not hold. As a counter example 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 [LPR13], 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 Generalization to arbitrary number fields

Our proof of Theorem 2 has paved 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.

To this end we define, for an integral basis $B_{L/\mathbb{Q}} = (\beta_0, \ldots, \beta_{n-1})$ of $L/\mathbb{Q}$, the matrix

$$\mathrm{M}\left(B_{L/\mathbb{Q}}\right) := \left(\sigma_i(\beta_j)\right)_{0 \leq i,j \leq n-1} \in \bar{L}^{n \times n}, \tag{13}$$

where $\bar{L}$ is an algebraic closure of L and $\sigma_i : L \to \bar{L}$ 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 a Euclidean norm from the coefficient embedding that in turn was defined by the choice of basis $B_m = \left(1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}\right)$. This cyclotomic basis has the useful property that for all $z \mid m$, there exists a basis B_m^z of $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_z)$ such that $B_m = B_m^z \otimes B_z$ ($\otimes$ 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 property. For this reason we make the dependence of the norm on the basis $B_{L/\mathbb{Q}} = (\beta_0, \dots, \beta_{n-1})$ explicit and denote by $||\cdot||_{B_{L/\mathbb{Q}}}$ the ℓ_2-norm associated to the coefficient embedding

$$\psi : L \to \mathbb{Q}^n, \quad \sum_{i=0}^{n-1} y_i \beta_i \mapsto \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

The proof of the generalization of Theorem 2 is analogous to the proof in Section 1. However, we do encounter a number of subtleties. Firstly, the extension $L/\mathbb{Q}$ is not necessarily a Galois extension. In this case the primes $\mathfrak{p}$ above a rational prime p can have different inertia degrees and ramification indices. Moreover, decomposition fields are only defined for Galois extensions. Hence, the second invertibility condition of Theorem 2 is not applicable to number fields that are not Galois.

Secondly, 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 only consider rational primes p such that the ideal (p) is relatively prime to the conductor

$$\mathfrak{f}_{\mathcal{O}} = \{\gamma \in \mathcal{O}_L : \gamma \mathcal{O}_L \subset \mathcal{O}\}.$$

For these primes we have the following lemma.

Lemma 4. *Let $\mathcal{O}$ be an order in a number field L and let p be rational prime such that the ideal (p) is relatively prime to the conductor $\mathfrak{f}_{\mathcal{O}}$, then*

$$\mathcal{O}/(p) \cong \mathcal{O}_L/(p).$$

Proof. Since $\mathcal{O} \subset \mathcal{O}_L$, we have the following injective ring homomorphism,

$$f : \mathcal{O}/(p) \cong \mathcal{O}_L/(p), \quad x \mapsto x.$$

Moreover, since $\mathfrak{f}_{\mathcal{O}}$ and (p) are relatively prime, for every $y \in \mathcal{O}_L$ there exists a $\gamma \in \mathfrak{f}_{\mathcal{O}} \subset \mathcal{O}$ and an $\alpha \in (p)$ such that

$$\gamma + \alpha = y.$$

Hence $f(\gamma \mod (p)) = y \mod (p)$ showing that f is surjective and thereby an isomorphism.

Thirdly, for arbitrary towers of number fields fields $\mathbb{Q} \subset K \subset L$, the order $\mathcal{O}_L$ does not have to be free over $\mathcal{O}_K$. A sufficient condition for $\mathcal{O}_L$ to be free over $\mathcal{O}_K$ is that $\mathcal{O}_K$ is a principal ideal domain. This follows from the structure theorem for finitely generated modules over principal ideal domains and the fact that $\mathcal{O}_L$ is a torsion free $\mathcal{O}_K$-module (e.g. [Lan02, Theorem 7.3]).

However, even if $\mathcal{O}_L$ is not free over $\mathcal{O}_K$, the order $\mathcal{O}$ contains, by definition, a basis of $L/\mathbb{Q}$ and thus a basis $B_{L/K} = (\alpha_0, \dots, \alpha_{l-1})$ of L/K. Let $B^*_{L/K} = (\alpha_0^*, \dots, \alpha_{l-1}^*)$ be the trace dual basis that is uniquely defined by the following relation:

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha_j^*) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

Then we have the following inclusion [Sti93, Theorem 3.3.4]:

$$\sum_{i=0}^{l-1} \mathcal{O}_K \alpha_i \subset \mathcal{O} \subset \sum_{i=0}^{l-1} \mathcal{O}_K \alpha_i^*.$$

Hence, there exists a free $\mathcal{O}_K$-module $M = \sum_{i=0}^{l-1} \mathcal{O}_K \alpha_i^*$ that contains $\mathcal{O}$. To the dual basis $B^*_{L/K}$ we associate, as in the cyclotomic case, the projections

$$\pi_j : M \to \mathcal{O}_K, \quad \sum_{i=0}^{l-1} \gamma_i \alpha_i^* \mapsto \gamma_j, \quad \text{for } 0 \le j \le l-1.$$

The module M can in general be larger than the ring of integer $\mathcal{O}_L$ and the ring M/p does not have to be well-defined for all primes p. For this reason, we only consider primes p for which $p \nmid [M : \mathcal{O}]$.

Altogether we thus obtain the following generalization of Theorem 2.

Theorem 6. *Let $L/\mathbb{Q}$ be a number field of degree n containing an order $\mathcal{O}$ with $\mathbb{Z}$-basis $B_{L/\mathbb{Q}}$. Moreover, let p be a rational prime that is unramified and relatively prime to the conductor $\mathfrak{f}_{\mathcal{O}}$. Then p factors in L as*

$$(p) = \prod_{i=1}^{g} \mathfrak{p}_i,$$

where $\mathfrak{p}_i$ is a prime in L with inertia degree f_i for all i. Moreover, $\gamma \in \mathcal{O}/(p)$ is invertible if

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

Assume in addition that $L/\mathbb{Q}$ is Galois, hence $f_i = f$ for some f and for all i. Let K_i denote the decomposition field of $\mathfrak{p}_i$ with integral basis $B_{K_i/\mathbb{Q}}$ and let $M_i \supset \mathcal{O}$ be a free $\mathcal{O}_{K_i}$-module with independent projections $\pi_j^i : M_i \to \mathcal{O}_{K_i}$ for $1 \leq j \leq f$. Moreover, assume that $p \nmid [M_i : \mathcal{O}]$ for all $1 \leq i \leq g$. Then if for all i there exists a j such that

$$0 < ||\pi_j^i(\gamma)||_{B_{K_i/\mathbb{Q}}} < \frac{\sqrt{g}}{s_1(B_{K_i/\mathbb{Q}})} p^{1/g},$$

then γ is invertible in $\mathcal{O}/(p)$.

Note that if the Galois extension $L/\mathbb{Q}$ is Abelian, then for all i, $K_i = K$ for some $K \subset L$.

A final practical remark in generalizing these results is that the largest singular value $s_1(B)$ for certain bases B of cyclotomic number fields is small, resulting in favorable invertibility conditions. For bases of arbitrary number fields this largest singular value might very well become large rendering certain cryptographic schemes over these fields inefficient.

7 Trinomial number fields

In this section we discuss the construction of challenge sets in orders of the form $\mathcal{O} \cong \mathbb{Z}[X]/(f)$ with $f = X^n + aX^k + b \in \mathbb{Z}[X]$ $(k < n)$ an irreducible trinomial. 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 and that we are still able to construct good challenge sets.

Let α be a root of f and let $L = \mathbb{Q}(\alpha)$ with complex embeddings σ_i for $0 \leq i \leq n-1$. Then the matrix $\mathrm{M}(B_f)$ is defined as

$$\mathrm{M}(B_f) = \left(\sigma_i(\alpha^j)\right)_{0 \leq i,j \leq n-1} \in \bar{L}^{n \times n},$$

for some algebraic closure $\bar{L}$ of L. Note that for a different choice of root α, the rows of the matrix $\mathrm{M}(B_f)$ are permuted and its singular values stay the same, which justifies our slight abuse of notation.

In the remainder of this section we prove an upper bound for the largest singular value $s_1(\mathrm{M}(B_f))$. To this end we state a theorem that was originally proved in 1908 by Bohl [Boh08] and later reformulated in [TdW16].

Theorem 7 ([Boh08, TdW16]). *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 norm smaller than or equal to β. 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. For notational convenience we restrict ourselves to irreducible polynomials in $\mathbb{Z}[X]$.

Corollary 2. *Let $f = X^n + aX^k + b \in \mathbb{Z}[X]$ be irreducible with roots $\alpha_0, \ldots, \alpha_{n-1}$. Then*

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

Proof. Let $\beta = (|a| + |b|)^{\frac{1}{n-k}}$, then since f is irreducible it follows that $\beta \geq 1$. Hence

$$\beta^n \geq \beta^k(|a| + |b|) \geq |a|\beta^k + |b|,$$

and by Theorem 7 it follows that all n roots have their norm upper bounded by β, which proves the corollary.

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

Lemma 5. *Let $f = X^n + aX^k + b \in \mathbb{Z}[X]$ be an irreducible polynomial. Then*

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

Proof. Let $\alpha_0, \ldots, \alpha_{n-1}$ be the roots of f and define $\boldsymbol{\alpha}^l := \left(\alpha_0^l, \ldots, \alpha_{n-1}^l\right)^T$. Then $\boldsymbol{\alpha}^l$, for $0 \leq l \leq n-1$, are precisely the columns of $\mathrm{M}(B_f)$. Moreover, by Corollary 2 it follows that for all $0 \leq l \leq n-1$

$$\begin{aligned} ||\alpha^l||_\infty &\leq (|a| + |b|)^{\frac{l}{n-k}} , \\ &\leq (|a| + |b|)^{\frac{n-1}{n-k}} . \end{aligned} \tag{14}$$

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

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

and

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

A similar upper bound is given in Lemma 5.5 of [PP19]. They consider a more general class of polynomials and derive a slightly larger uppper bound. The following lemma yields a minor improvement of Lemma 5.

Lemma 6. *Let $f = X^n + aX^k + b \in \mathbb{Z}[X]$ be an irreducible polynomial. Then*

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

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 5. We use the first inequality of Equation 14 to obtain the following upper bound:

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

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

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

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

Hence, the largest singular value $s_1(\mathrm{M}(B_f))$ 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 4 we proved the upper bound $s_1(m) \leq \sqrt{\tau(m)}$. The main difference is that in the proofs of Lemmas 5 and 6 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 improvement in upper bounding the value $s_1(\mathrm{M}(B_f))$ for trinomials f.

8 Factorization pattern of rational primes in trinomial fields

The invertibility results, Theorem 2 and Theorem 6, depend on the factorization pattern of rational primes p in the field L. For cyclotomic number fields the factorization patterns were described by Lemma 1. In this section, we will do the same for certain trinomial fields, i.e. fields of the form $L = \mathbb{Q}[X]/(f)$ with $f = X^n + aX^k + b \in \mathbb{Z}[X]$ $(k < n)$. In particular, we restrict ourselves to trinomials of the following form $f = X^n - X - 1$. The trinomials of this form are irreducible [Sel57] and their Galois group is the symmetry group S_n [Osa87], which is maximal.

The NTRU Prime cryptosystem [BCLvV17], for example, recommends using polynomials of this form with n prime. Taking f to be of prime degree ensures that L only has trivial subfields, thereby ruling out possible subfields attacks. Moreover, the fact that the Galois group of L is S_n ensures that L is not contained in a cyclotomic field. In addition, a maximal Galois group will ensure L does not have a lot of automorphisms. Finally, [BCLvV17] recommends the use of primes p that are inert in L to avoid the existence of homomorphisms form $\mathcal{O}_L/(p)$ to smaller rings. Such homomorphisms have been used to break specific instances of Ring-LWE based cryptosystems [CLS16].

In this work, we have aimed to find suitable primes that split in as many factors as possible so that the Chinese Remainder Theorem (CRT) can be applied to implement efficient ring operations. This contradicts the recommendation of choosing rational primes p that are inert in L. For this reason we will consider different factorization patterns, ranging from inert primes to completely splitting primes.

8.1 Chebotarev's Density Theorem

For any number field $L/\mathbb{Q}$ of degree n the Galois group $G = \mathrm{Gal}\,(L/\mathbb{Q})$ is a subgroup of the symmetry group S_n. Moreover every rational prime p that is unramified in L corresponds to a conjugacy class of $G \subset S_n$, namely the conjugacy class of the Frobenius elements of the primes $\mathfrak{p}$ in L that lie over p. As permutations in S_n, the elements in a conjugacy class all have the same cycle structure.

Let us now write $(f_1, f_2, \ldots, f_g)$ with $f_1 \geq f_2 \geq \cdots \geq f_g$ for the decomposition type (or factorization pattern) of p in L, i.e. $p = \prod_{i=1}^{g} \mathfrak{p}_i$ where $\mathfrak{p}_i$ is prime in L and has inertia degree f_i. Then the decomposition type of p equals the cycle structure of the corresponding conjugacy class in $G \subset S_n$. Moreover, by Chebotarev's Density Theorem the density of unramified primes with a particular decomposition type is proportional to the size of the associated conjugacy class in G [Tsc26].

In our case, $L = \mathbb{Q}[X]/(f)$ with $f = X^n - X^k - 1$, the fact that the Galois group equals S_n thus implies that for every possible partition P of n there exists an infinite amount of primes with decomposition type P in L.

The density of unramified primes that are inert in L is, for example, equal to $1/n$ and if $k|n$ the density of unramified primes with decomposition type $(n/k, \ldots, n/k)$ (k times) is equal to

$$\frac{k^k}{k! n^k}.$$

9 Challenge sets

In this section we construct challenge sets in the number field L, where we let L be either the cyclotomic number field $\mathbb{Q}(\zeta_{512})$ or the trinomial field $\mathbb{Q}[X]/\left(X^{256} - X - 1\right)$. Our constructions follow the approach of [LS18] in which a challenge set of cardinality $\approx 2^{237}$ is constructed. For quantum security a challenge set of size approximately 2^{256} is typically chosen, but in [LS18] it is argued that 2^{237} should be large enough.

The challenge sets are constructed via the coefficient embedding, using a power basis $\left(1, \beta, \ldots, \beta^{n-1}\right)$ of $L/\mathbb{Q}$, allowing us to represent elements in $\mathcal{O}_L$ by vectors in $\mathbb{Z}^n$. For both the cyclotomic and the trinomial number field challenge sets of the following form are considered,

$$\mathcal{C}_n = \left\{ \gamma = \sum_{i=0}^{n-1} a_i \beta^i \in \mathcal{O}_L : \|a\|^2 = R, \|a\|_\infty = 1 \right\}, \quad \text{with } |\mathcal{C}_n| = \binom{n}{R} 2^R, \tag{15}$$

where $n = 256$ is the degree of the field extension and $R \in \mathbb{Z}_{\geq 0}$ is minimized under the condition that $|\mathcal{C}_n| \geq 2^{237}$. The size of the challenge set can be increased by including all elements with norm at most R, i.e. not only those with norm equal to R, and by dropping the condition on the infinity norm. However, it turns out that the minimal R for which $|\mathcal{C}| \geq 2^{237}$ is the same in both cases. Moreover, the cardinality of challenge sets of Equation 15 is easily computed and for these challenge sets Lemma 7 can be applied to achieve another minor improvement.

For the cyclotomic number field we also consider the following construction, which depends on the decomposition type of the rational prime p,

$$\mathcal{C} = \underbrace{\mathcal{C}_{n/f} \times \cdots \times \mathcal{C}_{n/f}}_{f\text{-times}}, \quad \text{with } |\mathcal{C}| = \binom{n/f}{R}^f 2^{fR}. \tag{16}$$

Each factor in the Cartesian product of Equation 16 corresponds to an element in the decomposition field L^{D_p} of a prime p with n/f distinct factors in L, all of inertia degree f. Together these factors define, via a basis of L/K, an element of $\mathcal{O}_L$. When referring to the decomposition field techniques challenge sets of this form are used. Again, R is chosen to be the smallest integer for which $|\mathcal{C}| \geq 2^{237}$.

Subsequently, we apply Theorem 2 and Theorem 6 to find the minimal size of rational primes p for which all elements in $\mathcal{C} - \mathcal{C} = \{c - c' | c, c' \in \mathcal{C}, c \neq c'\}$ are invertible modulo p. We only consider odd and unramified primes. These theorems relate the invertibility condition to the norms R of the elements in the

challenge set. We can immediately bound the norm of elements of elements in $\mathcal{C}-\mathcal{C}$ by $2R$, but the following lemma combined with the fact that 2 is invertible modulo any odd prime gives us a small improvement. This observation was already made in [LS18] and applied to their ad-hoc example.

Lemma 7. *Let $\mathcal{C}_n$ be as in Equation 15. Then for all $x \in \mathcal{C}_n - \mathcal{C}_n$, either $\exists y \in \mathbb{Z}^n$ such that $x = 2y$ and $\|y\| \leq \sqrt{R}$ or $\|x\| \leq \sqrt{4R-2}$.*

Proof. The norm of $x \in \mathcal{C}_n - \mathcal{C}_n$ is maximal if $x = y - (-y)$ for some $y \in \mathcal{C}$, i.e. $x = 2y$ with $\|y\| \leq \sqrt{R}$. Moreover, $\|x\|_\infty \leq 2$ and $\|x\|_1 = 2R$ for all $x \in \mathcal{C}_n - \mathcal{C}_n$. Therefore, the next largest element of $\mathcal{C}_n - \mathcal{C}_n$ contains $R-1$ entries equal to ± 2, two entries equal to ± 1 and all other entries equal to 0. Hence, the next largest element has ℓ_2-norm $\sqrt{4R-2}$, which proves the lemma.

Recall that the invertibility condition depends on the decomposition type of p in L. The decomposition types of unramified rational primes in the $\mathbb{Q}(\zeta_{512})$ follow from Lemma 1 and in Section 8.1 the decomposition types of primes in $\mathbb{Q}[X]/\left(X^{256}-X-1\right)$ were described. In particular, in $\mathbb{Q}(\zeta_{512})$ the decomposition type of p is uniquely determined by the number of prime factors in $\mathbb{Q}(\zeta_{512})$ and no rational prime is inert in $\mathbb{Q}(\zeta_{512})$. In contrast, for any partition of n there exists a rational prime p that factors accordingly in $\mathbb{Q}[X]/\left(X^{256}-X-1\right)$. For a fair comparison between the two fields only rational primes for which all prime factors in L have the same inertia degree are considered.

In Table 1 the resulting prime sizes for $L = \mathbb{Q}(\zeta_{512})$ are displayed. Both for the standard approach and the decomposition field approach. Each row in this table represents a decomposition type and Chebotarev's Density Theorem gives us the density of the unramified primes of the corresponding decomposition type. Note that the sum of these densities is 1 since all possible decomposition types are represented in this table.

Lyubashevsky and Seiler [LS18] 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 $2^{30,45..}$ achieve the desired invertibility. This result can also be retrieved from Table 1.

Number of prime factors (g)	Inertia degree (f)	Chebotarev's Density	Prime size ($\log_2(p)$)	Prime size (decomp. field)
1	256	0	–	–
2	128	1/2	$7, 71..$	1
4	64	1/4	$15, 42..$	$5, 16..$
8	32	1/8	$30, 85..$	$13, 28..$
16	16	1/16	$61, 71..$	$30, 45..$
32	8	1/32	$123, 42..$	$78, 51$
64	4	1/64	$246, 85..$	$184, 15..$
128	2	3/256	$493, 71..$	$430, 58..$
256	1	1/256	$987, 42..$	$987, 42..$

Table 1. Minimal size of p such that all elements in $\mathcal{C}-\mathcal{C} \subset \mathcal{O}_L$, with $L = \mathbb{Q}(\zeta_{512})$, are invertible modulo p. $\mathcal{C}$ is chosen of the form of Equation 15 in the standard approach and of the form of Equation 16 in the decomposition field approach.

In Table 2 the resulting prime sizes for $L = \mathbb{Q}[X]/\left(X^{256}-X-1\right)$ are displayed. The singular value $s_1(B_{L/\mathbb{Q}})$, associated to the power basis $B_{L/\mathbb{Q}} = \left(1, X, \ldots, X^{255}\right)$, is equal to $31, 33...$ In comparison, the singular value for the cyclotomic field equals 16. Hence the minimum prime sizes are larger for the trinomial field by an additive term

$$g \log_2\left(\frac{31, 33..}{16}\right) \approx g.$$

Moreover, since L is not Galois we can not apply the decomposition field technique.

Again each row represents a decomposition type and the densities of the unramified primes of the corresponding decomposition type are given. Note that, in this case, the sum of these densities is not equal to 1,

because many other decomposition types are possible in L. Moreover, the densities for some decomposition types are extremely small, making it probably very hard to find primes of these specific decomposition types. Additionally these small densities are likely to cause the actual primes to be much larger than the lower bounds given by Table 2.

Number of prime factors (g)	Inertia degree (f)	Chebotarev's Density	Prime size ($\log_2(p)$)
1	256	2^{-8}	$4, 82..$
2	128	2^{-15}	$9, 65..$
4	64	$2^{-28,58..}$	$19, 30..$
8	32	$2^{-55,29..}$	$38, 61..$
16	16	$2^{-108,25..}$	$77, 22..$
32	8	$2^{-213,66..}$	$154, 45..$
64	4	$2^{-423,99..}$	$308, 91..$
128	2	$2^{-844,16..}$	$617, 83..$
256	1	$2^{-1683,99..}$	$1235, 67..$

Table 2. Minimal size of p such that all elements in $\mathcal{C} - \mathcal{C} \subset \mathcal{O}_L$, with $L = \mathbb{Q}[X]/\left(X^{256} - X - 1\right)$, are invertible modulo p. $\mathcal{C}$ is chosen of the form of Equation 15.

10 Challenge sets in the canonical embedding

Thus far, challenge sets have been defined via the coefficient embedding $\psi_B : L \to \mathbb{Q}^n$ of our number field, which depends on the choice of integral basis B 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 expressions of equations 15 and 16.

However, the appropriate embedding to consider is actually the canonical embedding $f : L \to \mathbb{C}^n$. In contrast to the coefficient embedding, this embedding is basis independent and preserves products. Moreover, it induces other Euclidean norms on L and $\mathcal{O}_L$, which are directly related to the hardness of the Ring-SIS problem underlying the security of the cryptographic protocols.

The canonical embedding f maps L into an n-dimensional $\mathbb{R}$-vector space $K_{\mathbb{C}} \subset \mathbb{C}^n$. Moreover, the image $f(\mathcal{O}_L)$ is a full-rank lattice in $K_{\mathbb{C}}$ [Neu99, Section 1.5]. Challenge sets defined via the canonical embedding are of the form

$$\left\{ \gamma \in \mathcal{O}_L : \|f(a)\| = \sqrt{\sum_{i=0}^{n-1} |\sigma_i(\gamma)|^2} \leq R \right\},$$

for some radius $R \geq 0$. Hence, these challenge sets correspond to sets of elements in the lattice $f(\mathcal{O}_L)$ of bounded norm. Depending on the lattice $f(\mathcal{O}_L)$ and the radius R the cardinality of these challenge sets can be hard to compute.

The coefficient and canonical embedding are related via the matrix $\mathrm{M}(B)$ (Equation 13), namely $f(\gamma) = \mathrm{M}(B) \cdot \psi_B(\gamma)$ for all $\gamma \in L$. Moreover, we have the following inclusion

$$\mathcal{C} := \{\gamma \in \mathcal{O}_L : \|\psi_B(a)\| \leq R\} \subset \{\gamma \in \mathcal{O}_L : \|f(a)\| \leq s_1(B)R\} =: \tilde{\mathcal{C}},$$

where $s_1(B)$ is the largest singular value of the matrix $\mathrm{M}(B)$.

All previous challenge sets have been constructed via the coefficient embedding and an invertibility result has been obtained by an implicit mapping to the canonical embedding, which gave rise to the largest singular value $s_1(B)$ in the invertibility bounds of Theorem 2 and Theorem 6. The invertibility properties of the sets $\mathcal{C}$ and $\tilde{\mathcal{C}}$ are therefore the same, hence they both result in the same prime sizes. However, the set $\tilde{\mathcal{C}}$ can be strictly larger than $\mathcal{C}$, which means that the challenge set $\mathcal{C}$ might be suboptimal.

When L is a cyclotomic number field with conductor $m = 2^k$ and B is the power basis, the matrix $\mathrm{M}(B)$ is orthogonal and both embeddings result in similar challenge sets. In fact, in this case

$$\{\gamma \in \mathcal{O}_L : \|\psi_B(a)\| \leq R\} = \{\gamma \in \mathcal{O}_L : \|f(a)\| \leq s_1(m)R\},$$

where $s_1(m) = \sqrt{m/2}$. Power-of-two cyclotomic number fields thus have the convenient property that the ℓ_2-norms in the two different embeddings only differ by a factor $s_1(m)$.

The following lemma recaps the invertibility result used in our proof of Theorem 2. However, this lemma directly uses the canonical embedding which removes the largest singular value. Moreover, this lemma considers arbitrary ℓ_k-norms.

Lemma 8. *Let $L/\mathbb{Q}$ be a number field of degree n and let $f : L \to \mathbb{C}^n$ be the canonical embedding. Then for all $\gamma \in L$ and for all $k \geq 1$,*

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

Proof. The proof immediately follows from inequality of the arithmetic and the geometric mean.

Lemma 8 suggests the approach to define challenge sets using different ℓ_k-norms, i.e. challenge sets of the form

$$\{\gamma \in \mathcal{O}_L : \|f(a)\|_k \leq R\}.$$

In particular, if we take $k = 1$ the denominator in Lemma 8 is $n \geq \sqrt{n}$, which might give a stronger invertibility result. However, we will also have to increase the radius R, in comparison to the ℓ_2 approach, to achieve a sufficiently large cardinality. An additional downside of this approach is that we can not apply Lemma 7 to further reduce the prime size. However, it still turns out to be the case that we can obtain smaller prime bounds when applying this ℓ_1-norm approach.

We will apply this approach to our running example $L = \mathbb{Q}(\zeta_{512})$, where we will consider rational primes with different decomposition types. As in Section 9, the challenge set $\tilde{\mathcal{C}}$ will be a Cartesian product of sets in the decomposition field K (Equation 16). These sets are of form

$$\tilde{\mathcal{C}}_K := \{\gamma \in \mathcal{O}_K : \|f(a)\|_1 \leq R\}.$$

Again the radius R of these sets will be chosen to be the minimal value for which $\tilde{\mathcal{C}}$ has cardinality at least 2^{237}. The cardinality of these sets is computed by enumerating all relevant lattice vectors and computing their ℓ_1-norm in the canonical embedding. This is a computationally intensive task and for this reason we only consider rational primes that split in at most 16 factors, i.e. the dimension of the decomposition field K is at most 16. The resulting prime sizes are shown in Table 3. For comparison, the ℓ_2-norm results of Section 9 are also displayed in this table.

Table 3 shows that, for primes that split in at least 8 factors in L, we can indeed achieve smaller prime sizes by considering the ℓ_1-norm directly in the canonical embedding. However, it must me noted that choosing the challenge sets in this manner does increase the ℓ_2-norm of the challenges. When we choose primes p that split in 16 prime factors the ℓ_2 approach bounds the ℓ_2-norms of challenges at 8, while the ℓ_1-approach results in challenges c with $\|c\| \leq 4\sqrt{7} \approx 10,58$. The increased ℓ_2-norm makes the underlying Ring-SIS problem easier to solve, hence decreasing the prime size comes at a costs. We have introduced here a new trade-off and showed the results for the most extreme cases, either only bounding the ℓ_2-norm or only bounding the ℓ_1-norm. However, depending on the application other trade-offs taking both norms into account might be optimal.

To summarize, defining challenge sets in the canonical eliminates the largest singular value term $s_1(B)$ in the invertibility results. Especially, when the matrix M_B is far from orthogonal this approach will lead to better parameters. In the case of cyclotomic number fields $L = \mathbb{Q}(\zeta_m)$ with power basis B these improvements are directly related to the number of distinct odd prime factors of the conductor m, i.e. the more distinct odd prime factors m has the more beneficial it will be to define challenge sets in the canonical embedding. Another benefit of this approach is that other norms can be considered to improve specific parameters of the resulting cryptographic protocols and to introduce new trade-offs between these parameters. A downside of this approach is that determining the cardinality of challenge sets becomes more complex.

Number of prime factors (g)	Inertia degree (f)	Chebotarev's Density	Prime size (ℓ_2) ($\log_2(p)$)	Prime size (ℓ_1) ($\log_2(p)$)
1	256	0	–	–
2	128	1/2	1	2
4	64	1/4	5, 16..	5, 53..
8	32	1/8	13, 28..	12, 07..
16	16	1/16	30, 45..	30, 01..

Table 3. Minimal prime size for challenge sets in $\mathcal{O}_L$ with $L = \mathbb{Q}(\zeta_{512})$ chosen via the canonical embedding.

11 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 10. This work was supported by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701)."

References

[ABD16] 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 Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 153–178. Springer, 2016.

[BBC+18] Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafaël del Pino, Jens Groth, and Vadim Lyubashevsky. Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 669–699. Springer, 2018.

[BCD+16] 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 Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 1006–1018. ACM, 2016.

[BCLvV17] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU prime: Reducing attack surface at low cost. In Carlisle Adams and Jan Camenisch, editors, *Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers*, volume 10719 of *Lecture Notes in Computer Science*, pages 235–260. Springer, 2017.

[BDL+18] Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. More efficient commitments from structured lattice assumptions. In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, volume 11035 of *Lecture Notes in Computer Science*, pages 368–385. Springer, 2018.

[BDLN16] Carsten Baum, Ivan Damgård, Kasper Green Larsen, and Michael Nielsen. How to prove knowledge of small secrets. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 478–498. Springer, 2016.

[Ber01] Daniel J Bernstein. Multidigit multiplication for mathematicians. *Advances in Applied Mathematics*, pages 1–19, 2001.

[Ber14] Daniel J. Bernstein. A subfield-logarithm attack against ideal lattices. http://blog.cr.yp.to/20140213-ideal.html, 2014.

[BGL+18] Sauvik Bhattacharya, 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. *IACR Cryptology ePrint Archive*, 2018:725, 2018.

[BKLP15] Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. Efficient zero-knowledge proofs for commitments from learning with errors over rings. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*, volume 9326 of *Lecture Notes in Computer Science*, pages 305–325. Springer, 2015.

[BLS19] Jonathan Bootle, Vadim Lyubashevsky, and Gregor Seiler. Algebraic techniques for short(er) exact lattice-based zero-knowledge proofs. *IACR Cryptology ePrint Archive*, 2019:642, 2019.

[Boh08] P Bohl. Zur theorie der trinomischen gleichungen. *Mathematische Annalen*, 65(4):556–566, 1908.

[Bos90] Wieb Bosma. Canonical bases for cyclotomic fields. *Appl. Algebra Eng. Commun. Comput.*, 1:125–134, 1990.

[BS16] 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 Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 893–902. SIAM, 2016.

[CD09] Ronald Cramer and Ivan Damgård. On the amortized complexity of zero-knowledge protocols. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 177–191. Springer, 2009.

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 559–585. Springer, 2016.

[CDW17] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 324–348, 2017.

[CDXY17] Ronald Cramer, Ivan Damgård, Chaoping Xing, and Chen Yuan. Amortized complexity of zero-knowledge proofs revisited: Achieving linear soundness slack. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part I*, volume 10210 of *Lecture Notes in Computer Science*, pages 479–500, 2017.

[CF02] Ronald Cramer and Serge Fehr. Optimal black-box secret sharing over arbitrary abelian groups. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 272–287. Springer, 2002.

[CFS05] Ronald Cramer, Serge Fehr, and Martijn Stam. Black-box secret sharing from primitive sets in algebraic number fields. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 344–360. Springer, 2005.

[CGS14] Peter Campbell, Michael Groves, and Dan Shepherd. Soliloquy: A cautionary tale. In *ETSI 2nd Quantum-Safe Crypto Workshop*, pages 1–9, 2014.

[CLS16] Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Vulnerable galois RLWE families and improved attacks. *IACR Cryptology ePrint Archive*, 2016:193, 2016.

[DF94] Yvo Desmedt and Yair Frankel. Perfect homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM J. Discrete Math.*, 7(4):667–679, 1994.

[DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the fiat-shamir transformation in the quantum random-oracle model. *CoRR*, abs/1902.07556, 2019.

[DKL+13] 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 Jason Crampton, Sushil Jajodia, and Keith Mayes, editors, *Computer Security - ESORICS 2013 - 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings*, volume 8134 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2013.

[dPLS18] Rafaël del Pino, Vadim Lyubashevsky, and Gregor Seiler. Lattice-based group signatures and zero-knowledge proofs of automorphism stability. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 574–591. ACM, 2018.

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986.

[GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate multilinear maps from ideal lattices. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2013.

[GS02] Craig Gentry and Michael Szydlo. Cryptanalysis of the revised NTRU signature scheme. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 299–320. Springer, 2002.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2002. Originally published by Addison-Wesley, 1993.

[Len76] Hendrik W Lenstra. Euclidean number fields of large degree. *Inventiones mathematicae*, 38(3):237–254, 1976.

[LN17] Vadim Lyubashevsky and Gregory Neven. One-shot verifiable encryption from lattices. *IACR Cryptology ePrint Archive*, 2017:122, 2017.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 35–54. Springer, 2013.

[LS18] Vadim Lyubashevsky and Gregor Seiler. Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 204–224. Springer, 2018.

[LSS14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld. Gghlite: More efficient multilinear maps from ideal lattices. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 239–256. Springer, 2014.

[Lyu09] Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *Lecture Notes in Computer Science*, pages 598–616. Springer, 2009.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 738–755. Springer, 2012.

[LZ19] Qipeng Liu and Mark Zhandry. Revisiting post-quantum fiat-shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 326–355. Springer, 2019.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag Berlin Heidelberg, 1 edition, 1999.

[Osa87] Hiroyuki Osada. The galois groups of the polynomials $X^n + aX^l + b$. *Journal of Number Theory*, 25:230–238, 1987.

[PP19] Chris Peikert and Zachary Pepin. Algebraically structured lwe, revisited. *IACR Cryptology ePrint Archive*, 2019:878, 2019.

[Sch89] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer, 1989.

[Sel57] Ernst S Selmer. On the irreducibility of certain trinomials. *Mathematica Scandinavica*, pages 287–302, 1957.

[SSZ17] Ron Steinfeld, Amin Sakzad, and Raymond Kuo Zhao. Titanium: Proposal for a nist post-quantum public-key encryption and kem standard. 2017.

[Sti93] Henning Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer, 1993.

[SV10] Nigel P. Smart and Frederik Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*, volume 6056 of *Lecture Notes in Computer Science*, pages 420–443. Springer, 2010.

[TdW16] Thorsten Theobald and Timo de Wolff. Norms of roots of trinomials. *Mathematische Annalen*, 366(1):219–247, Oct 2016.

[Tsc26] N. Tschebotareff. Die bestimmung der dichtigkeit einer menge von primzahlen, welche zu einer gegebenen substitutionsklasse gehören. *Mathematische Annalen*, 95(1):191–228, Dec 1926.

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2 edition, 1997.

[YAZ+19] 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 Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, volume 11692 of *Lecture Notes in Computer Science*, pages 147–175. Springer, 2019.