Subtractive Sets over Cyclotomic Rings
Limits of Schnorr-like Arguments over Lattices

Martin R. Albrecht[1⋆] and Russell W. F. Lai[2⋆⋆]

[1] Information Security Group, Royal Holloway, University of London
martin.albrecht@royalholloway.ac.uk
[2] Chair of Applied Cryptography, Friedrich-Alexander-Universität Erlangen-Nürnberg
russell.lai@cs.fau.de

Abstract. We study when (dual) Vandermonde systems of the form $\mathbf{V}_T^{(\intercal)} \cdot \mathbf{z} = s \cdot \mathbf{w}$ admit a solution $\mathbf{z}$ over a ring $\mathcal{R}$, where $\mathbf{V}_T$ is the Vandermonde matrix defined by a set T and where the "slack" s is a measure of the quality of solutions. To this end, we propose the notion of (s,t)-subtractive sets over a ring $\mathcal{R}$, with the property that if S is (s,t)-subtractive then the above (dual) Vandermonde systems defined by any t-subset $T \subseteq S$ are solvable over $\mathcal{R}$. The challenge is then to find large sets S while minimising (the norm of) s when given a ring $\mathcal{R}$.
By constructing families of (s,t)-subtractive sets S of size $n = \mathsf{poly}(\lambda)$ over cyclotomic rings $\mathcal{R} = \mathbb{Z}[\zeta_{p^\ell}]$ for prime p, we construct Schnorr-like lattice-based proofs of knowledge for the SIS relation $\mathbf{A} \cdot \mathbf{x} = s \cdot \mathbf{y} \bmod q$ with $O(1/n)$ knowledge error, and $s = 1$ in case $p = \mathsf{poly}(\lambda)$. Our technique slots naturally into the lattice Bulletproof framework from Crypto'20, producing lattice-based succinct arguments for NP with better parameters.
We then give matching impossibility results constraining n relative to s, which suggest that our Bulletproof-compatible protocols are optimal unless fundamentally new techniques are discovered. Noting that the knowledge error of lattice Bulletproofs is $\Omega(\log k/n)$ for witnesses in $\mathcal{R}^k$ and subtractive set size n, our result represents a barrier to practically efficient lattice-based succinct arguments in the Bulletproof framework.
Beyond these main results, the concept of (s,t)-subtractive sets bridges group-based threshold cryptography to lattice settings, which we demonstrate by relating it to distributed pseudorandom functions.

1 Introduction

Proving knowledge of a short integral vector $\mathbf{x}$ satisfying a system of linear equations of the form $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$ defined over some ring $\mathcal{R}$, i.e. an answer

⋆ The research of MA was supported by EPSRC grants EP/S020330/1, EP/S02087X/1, by the European Union Horizon 2020 Research and Innovation Program Grant 780701 and Innovate UK grant AQuaSec.

⋆⋆ Russell W. F. Lai is supported by the State of Bavaria at the Nuremberg Campus of Technology (NCT). NCT is a research cooperation between the Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) and the Technische Hochschule Nürnberg Georg Simon Ohm (THN).

to a short integer solution (SIS) problem and its generalisations, is a central task in lattice-based cryptography. Indeed, zero-knowledge variants of such proofs catalyse constructions of lattice-based privacy-preserving protocols such as group and ring signatures (e.g. [28,18,38]). These proofs are often also required for proving the well-formedness of the inputs of basic lattice building blocks. This is because random elements in $\mathcal{R}$ are easily trapdoored [23] such that using them in computations touching secret values risks their exposure. Furthermore, when $\mathbf{y}$ is a commitment of $\mathbf{x}$ encoding the witness to an NP statement, such a proof of knowledge can be compiled into a (succinct) argument of knowledge for NP [3,11]. The practical performance of such proofs has thus far-reaching consequences.

Prior to 2019 plausibly post-quantum secure proof systems for the SIS problem could be categorised into three classes: probabilistically-checkable proofs (PCP), "Stern-like" or "Schnorr-like".[3]

PCP-based systems [27] offer succinct proofs for arithmetic circuits from symmetric primitives only (e.g. [5]).

Stern-like systems [36,26,29] rely on the combinatorial cut-and-choose technique, and come with a knowledge extractor which is able to extract a solution $\tilde{\mathbf{x}}$ with $\|\mathbf{x}\| = \|\tilde{\mathbf{x}}\|$ satisfying $\mathbf{A} \cdot \tilde{\mathbf{x}} = \mathbf{y} \bmod q$. Due to their combinatorial nature, however, Stern-like systems only achieve constant knowledge error and have to be repeated $O(\lambda)$ times to make that negligible.

Schnorr-like systems (e.g. [30]) are algebraic and can achieve inverse polynomial or even negligible error, hence only $O(\lambda/\log\lambda)$ repetitions are needed in the former case and none in the latter. However, the knowledge extractors for Schnorr-like proofs are only able to extract a solution $\tilde{\mathbf{x}}$ to a relaxed statement $\mathbf{A} \cdot \tilde{\mathbf{x}} = s \cdot \mathbf{y} \bmod q$ with a "slack" $s \neq 1$ and "stretch" $\|\tilde{\mathbf{x}}\|/\|\mathbf{x}\| > 1$, which ultimately force the systems to be instantiated with larger moduli q. These relaxations may be acceptable in some applications, such as digital signatures, but can be prohibitive for others, e.g. when the system is recursively composed.

In the discrete logarithm setting, Bünz *et al.* [13] discovered that the linearity of Schnorr-like proofs can be exploited for recursive composition. This "Bulletproof" template was adapted to the lattice setting by Bootle *et al.* [11], where the task of proving $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$, with $\mathbf{A} = (\mathbf{A}_0, \mathbf{A}_1)$, is reduced to that of proving $\tilde{\mathbf{A}} \cdot \tilde{\mathbf{x}} = \tilde{\mathbf{y}} \bmod q$ with $\tilde{\mathbf{A}} = c\mathbf{A}_0 + \mathbf{A}_1$ and $\tilde{\mathbf{y}}$ dependent on some random challenge c, and the dimension of $\tilde{\mathbf{x}}$ halved compared to $\mathbf{x}$. By recursively composing the above protocol $\log k$ times, where k is the dimension of $\mathbf{x}$, Bootle *et al.* [11] obtained a protocol with poly-logarithmic communication for proving $\mathbf{A}\mathbf{x} = \mathbf{y} \bmod q$, which implies [3] the first lattice-based zero-knowledge arguments for NP with poly-logarithmic communication that deviates from the PCP-based framework.

Since 2019 several works [38,12,7,20] managed to give (almost) the best of both the Stern and Schnorr worlds: neither slack nor stretch as in Stern-like protocols and inverse-polynomial (but not negligible) soundness error as in Schnorr-like

[3] Without counting highly generic constructions requiring Karp reductions.

protocols. All these works prove $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$ exactly, i.e. $\mathbf{A} \cdot \tilde{\mathbf{x}} = s \cdot \mathbf{y} \bmod q$ with $s = 1$ and $\|\tilde{\mathbf{x}}\| = \|\mathbf{x}\|$. The work of Beullens [7] generalises the "MPC in the head with preprocessing" idea of [25] to give a variant of Stern's protocol with inverse-polynomial soundness error.[4] The works [38,12,20] augment a Schnorr-like protocol with non-linear constraints fixing $\mathbf{x}$ to be, say, ternary.

While these works resolve the question of proving $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$ without slack or stretch, they all share the properties of introducing non-linear constraints and producing linear-size proofs.[5] Indeed, unless new techniques are developed, it is unclear how the non-linear constraints used in these systems can be integrated into the Bulletproof framework of "folding down" the problem to polylogarithmic size, exploiting linearity. Thus, it is natural to ask if the approaches taken in these prior works are necessary, or whether Schnorr-like constructions that reduce or eliminate stretch and slack while achieving inverse-(super-)polynomial soundness error have yet to be found.

Knowledge extraction in Schnorr-like proofs for the SIS problem classically proceeds roughly as follows. Let $S = \{c_0, \ldots, c_{n-1}\}$ be a set of challenges. Given a convincing prover, the extractor $\mathcal{E}$ runs the prover multiple times to extract t solutions $\tilde{\mathbf{x}}_i$ satisfying $\mathbf{A} \cdot \tilde{\mathbf{x}}_i = \tilde{\mathbf{y}}_0 + c_i\, \mathbf{y} + c_i^2\, \tilde{\mathbf{y}}_2 + \cdots + c_i^{t-1}\, \tilde{\mathbf{y}}_{t-1} \bmod q$ for distinct $c_i \in S$. In the simple $t = 2$ case which captures linear-size proofs, $\mathcal{E}$ subtracts the two relations and obtains $\mathbf{A} \cdot (\tilde{\mathbf{x}}_{i_0} - \tilde{\mathbf{x}}_{i_1}) = (c_{i_0} - c_{i_1}) \cdot \mathbf{y} \bmod q$. If $c_{i_0} - c_{i_1}$ is invertible, e.g. when the c_i's are field elements, and we do not care about the length of the extracted solution, then $\mathcal{E}$ could simply divide both sides by $c_{i_0} - c_{i_1}$ and obtain an exact solution. The issue in the lattice settings is that the relation $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$ is defined over e.g. a cyclotomic ring $\mathcal{R} = \mathbb{Z}[\zeta]$, where not all elements are invertible. Even if $c_{i_0} - c_{i_1}$ is invertible (mod q), its inverse and hence the extracted solution might not be short (relative to q).

A workaround is to accept a slack of s which is divisible by $c_i - c_j$ over $\mathcal{R}$ for all possible $c_i, c_j \in S$. Then by choosing a large enough modulus $q \in \mathbb{N}$, $\mathcal{E}$ can extract a short (relative to q) solution $\tilde{\mathbf{x}}$ to $\mathbf{A} \cdot \tilde{\mathbf{x}} = s \cdot \mathbf{y} \bmod q$. In matrix form, it means that the extractor $\mathcal{E}$ solves a linear system of the form $\mathbf{V}_T^\intercal \cdot \mathbf{z} = s \cdot \mathbf{w}$ where $\mathbf{V}_T$ is the Vandermonde matrix (Equation (3)) defined by $T = \{c_{i_0}, c_{i_1}\}$ and $\mathbf{w} = (0, 1)^\intercal$. In the $t = 3$ case which captures one level of the lattice Bulletproof protocol [11], $\mathcal{E}$ solves a linear system of the same form except that $T = \{c_{i_0}, c_{i_1}, c_{i_2}\}$ and $\mathbf{w} = (0, 1, 0)^\intercal$. In both cases $\mathcal{E}$ extracts $\tilde{\mathbf{x}} = \sum_{i \in \mathbb{Z}_t} z_i \cdot \tilde{\mathbf{x}}_i$ as a solution to $\mathbf{A} \cdot \tilde{\mathbf{x}} = s \cdot \mathbf{y} \bmod q$ with stretch dependent on $\|\mathbf{z}\|$.

From this discussion we can reduce the task of finding Schnorr-like protocols (especially Bulletproof-compatible ones) with small soundness error to the task of finding a large set S and a small slack s, so that for any t-subset $T \subseteq S$ for some desired threshold t, the dual Vandermonde systems of linear equations of the form $V_T^\intercal \cdot \mathbf{z} = s \cdot \mathbf{w}$ have a short solution $\mathbf{z}$ over $\mathcal{R}$.

[4] A similar approach is taken in [4] but for proofs from symmetric primitives.

[5] Proof effort can be amortised, though [10].

Contribution. In this work, we give both positive and negative resolutions to the above problem. Our main results are summarised below.

(s,t)-subtractive sets. In Section 3 we define the notion of (s,t)-subtractive sets of size n over a ring $\mathcal{R}$. If $S \subseteq \mathcal{R}$ is (s,t)-subtractive, then for any t-subset $T \subseteq S$, (dual) Vandermonde systems defined by T are solvable over $\mathcal{R}$. If S is $(1,t)$-subtractive (without slack) then we simply call S subtractive.

(s,t)-subtractive sets over power-of-2 rings. In Section 3.1 we construct a family of (s,t)-subtractive sets, with different tradeoffs between the set size n, slack s, and threshold t, over any power-of-2 cyclotomic ring $\mathcal{R} = \mathbb{Z}[\zeta_m]$ where $m = 2^\ell$. This can be seen as a generalisation of [6] who essentially constructed a $(2,2)$-subtractive set of size m. Our family includes a $(2,3)$-subtractive set of size $n = m/2+1$, which implies a lattice Bulletproof protocol with slack k and stretch $\tilde{O}(k^{2\log m+0.58})$. In comparison, the protocol of Bootle *et al.* [11] had slack k^3 and stretch $\tilde{O}(k^{3\log m+4.5})$.[6]

Subtractive sets over prime-power rings. In Section 3.2 we construct a subtractive set S of prime size p over any prime-power cyclotomic ring $\mathcal{R} = \mathbb{Z}[\zeta_{p^\ell}]$. For $p = \mathsf{poly}(\lambda)$ it implies a Schnorr-like proof of knowledge for lattice statements over $\mathcal{R}$ without slack with knowledge error $O(1/\mathsf{poly}(\lambda))$, which in turn implies a lattice Bulletproof protocol with no slack and stretch $\tilde{O}(k^{3\log m+4.58})$.

No large (s,t)-subtractive sets. In Section 3.3 we prove that if $\mathcal{R}$ has an ideal $\mathfrak{q}$ of algebraic norm q, then for any (s,t)-subtractive set S over $\mathcal{R}$ of size $n > q$, we necessarily have $s \in \mathfrak{q}$. Consequently, there is no family of $(2,t)$-subtractive sets of size $n > m+1$ over power-of-2 cyclotomic rings, meaning that our $(2,3)$-subtractive set of size $n = m/2+1$ is within a factor of 2 of being optimal. There is also no subtractive set of size $n > p$ over prime-power cyclotomic rings, meaning that our subtractive sets of size $n = p$ are optimal.

Soundness of lattice Bulletproofs. In Section 4 we construct a slight generalisation of the Bulletproof protocol from [11] and instantiate it with our subtractive sets. We prove both completeness and soundness for each level. For the recursive composition, we note that unfortunately the knowledge error of $O(1/n)$ given in [11] turns out to be too optimistic: it does not account for the freedom of the prover to choose for which level(s) to cheat. As we discuss in Section 4.2, we can hope for $O(\log k/n)$ by applying a union bound. Indeed, applying [19, Lemma 3.2], we obtain a knowledge error of $8.16 \log k/n$. We consider our more careful analysis of the knowledge error in [11] an independent contribution.

Small slack and negligible knowledge error is unlikely. Based on the technique for proving the impossibility of large (s,t)-subtractive sets we prove that, for a natural class of "algebraic" knowledge extractors for Schnorr-like protocols, it is impossible to achieve knowledge error $\kappa < q^{-1}$ if $\mathcal{R}$ has an ideal $\mathfrak{q}$ of algebraic norm q unless we accept a slack $s \in \mathfrak{q}$. For a natural generalisation of Schnorr-like protocols, where the verifier sends two challenges chosen from sets S_0 and S_1 instead of one, it is still impossible[7] for algebraic knowledge extractors

[6] Their stretch analysis appears to be generous, though. We discuss the tightness of our analysis in Section 4.3.

[7] Under mild additional assumptions.

to achieve knowledge error $\kappa < q^{-2}$ unless $s \in \mathfrak{q}$. For concreteness, we note that a prime-power cyclotomic ring $\mathcal{R} = \mathbb{Z}[\zeta_{p^\ell}]$ always has an ideal $\left\langle 1 - \zeta_{p^\ell} \right\rangle$ of norm p. Therefore our instantiations over prime-power rings are optimal assuming algebraic extractors. We interpret this as a limit to achieving negligible knowledge error in Schnorr-like (Bulletproof-compatible) proofs for the SIS problem with small slack without introducing non-linear relations.

Application to homomorphic secret sharing over rings. Apart from its applications in constructing Schnorr-like protocols, in the full version of this work we demonstrate how (s,t)-subtractive sets can be used as a tool to bridge group-based threshold cryptography techniques to the lattice setting by relating them to the construction of homomorphic secret sharing schemes over rings. Roughly, in matrix form, the recovery procedure in such a scheme is equivalent to finding the first term z_0 of the solution $\mathbf{z}$ to a linear system of the form $\mathbf{V}_T \cdot \mathbf{z} = s \cdot \mathbf{w}$ where $\mathbf{V}_T$ is the Vandermonde matrix defined by T (as above). As a concrete example, we generalise the construction of distributed pseudorandom functions from (almost) key-homomorphic pseudorandom functions and Shamir secret sharing by Boneh *et al.* [8] using (s,t)-subtractive sets.

2 Preliminaries

Let $\lambda \in \mathbb{N}$ be the security parameter. For $n \in \mathbb{N}$, write $[n] \coloneqq \{1, 2, \ldots, n\}$, $\mathbb{Z}_n \coloneqq \{0, 1, \ldots, n-1\}$ denotes the ring of integers modulo n, $\mathbb{Z}_n^*$ denotes the multiplicative group of integers modulo n, and the Euler totient function $\varphi(n)$ denotes the number of positive integers at most and coprime with n. If $T \subseteq S$ are sets and T has t elements, we write $T \subseteq_t S$. If S is a finite set then $\leftarrow\!\$\, S$ denotes the sampling of a uniformly random element from S.

2.1 Cyclotomic Rings

For $m \in \mathbb{N}$, let $\zeta_m \in \mathbb{C}$ be any fixed primitive m-th root of unity. Denote by $K = \mathbb{Q}(\zeta_m)$ the cyclotomic field of order $m \geq 2$ and degree $\varphi(m)$, and by $\mathcal{R} = \mathbb{Z}[\zeta_m]$ its ring of integers, called a cyclotomic ring for short. We have $\mathcal{R} \cong \mathbb{Z}[x]/\langle \Phi_m(x) \rangle$, where $\Phi_m(x)$ is the m-th cyclotomic polynomial. We write $\sigma_i(x)$ for $0 \leq i < \varphi(m)$ be the $\varphi(m)$ different embeddings of $x \in \mathbb{Q}[\zeta_m]$ into $\mathbb{C}$. Cyclotomic fields $\mathbb{Q}[\zeta_m]$ are Galois extensions of $\mathbb{Q}$ [37, Thm 2.5], i.e. for all embeddings $\sigma_i(\cdot)$ of the field to $\mathbb{C}$ we have $\sigma_i(\mathbb{Q}[\zeta_m]) = \mathbb{Q}[\zeta_m]$. If $f_1, \ldots, f_k \in \mathcal{R}$, we write $\langle f_1, \ldots, f_k \rangle \subseteq \mathcal{R}$ for the ideal generated by $f_1, \ldots, f_k$. If $T \subseteq \mathcal{R}$, we also write $\langle T \rangle$ for the ideal generated by the elements in T. For $T_0, T_1 \subseteq \mathcal{R}$, we write $T_0 - T_1 \coloneqq \{t_0 - t_1 : t_i \in T_i\}$. Similarly, we write $T_0 \cdot T_1 - T_2 \cdot T_3 \coloneqq \{t_0 \cdot t_1 - t_2 \cdot t_3 : t_i \in T_i\}$ and so on. When m is clear from the context, we omit the subscript m and write $\zeta = \zeta_m$. We will focus primarily on $m \geq 2$ which is a prime-power. Using the "powerful" basis $\left\{\zeta^i\right\}_{i \in \mathbb{Z}_{\varphi(m)}}$, we can view $\mathcal{R}$ as a $\mathbb{Z}$-module of dimension $\varphi(m)$.

2.2 Norms and Ring Expansion Factors

For elements $x \in \mathcal{R}$ we denote the infinity norm of its coefficient vector (with the powerful basis) as $\|x\|$. If $\mathbf{x} \in \mathcal{R}^k$ we write $\|\mathbf{x}\|$ for the infinity norm of $\mathbf{x}$. We denote the algebraic norm of elements $x \in \mathcal{R}$ by $N(x) \coloneqq \prod_{0 \le i < n} \sigma_i(x)$. It holds that $N(x) = |\mathcal{R}/\langle x \rangle|$. We define the degree-$d$ expansion factor of a ring $\mathcal{R}$.

Definition 1. *Let $\mathcal{R}$ be a ring. The degree-d expansion factor of $\mathcal{R}$, denoted by $\gamma_{\mathcal{R},d}$, is defined as $\gamma_{\mathcal{R},d} \coloneqq \max_{S \subseteq_d \mathcal{R}} \left\|\prod_{a \in S} a\right\| / \prod_{a \in S} \|a\|$. If $d = 2$ we simply write $\gamma_{\mathcal{R}} = \gamma_{\mathcal{R},2}$.*

To upper bound $\gamma_{\mathcal{R},d}$ for a cyclotomic ring $\mathcal{R}$, we prove the following technical lemma which can be seen as a generalisation of [31, Theorem 3.3] to prime-power cyclotomic rings together with Proposition 1 given below.

Lemma 1. *Let $\zeta = \zeta_m$ where $m = p^\ell$ for some prime p. Let $d \in \mathbb{N}$. Then the expression $a = \sum_{i \in \mathbb{Z}_{dm}} a_i \cdot \zeta^i$ where $\max_{i \in \mathbb{Z}_{dm}} \|a_i\| \le \alpha$ can be reduced to $a = \sum_{i \in \mathbb{Z}_{\varphi(m)}} a'_i \cdot \zeta^i$ with $\max_{i \in \mathbb{Z}_{\varphi(m)}} \|a'_i\| \le 2\, d \cdot \alpha$. Assume further that $a_i \ge 0$ for all $i \in \mathbb{Z}_{dm}$, then we have $\max_{i \in \mathbb{Z}_{\varphi(m)}} \|a'_i\| \le d \cdot \alpha$.*

Proof. Recall that ζ is a root of $\Phi_m(x) = \sum_{i=0}^{p-1} x^{ip^{\ell-1}}$. We thus have the identities $\zeta^{m-k} = -\sum_{i=1}^{p-1} \zeta^{ip^{\ell-1}-k}$ for $k \in [p^{\ell-1}]$. Suppose that the monomials $\left\{\zeta^{ip^{\ell-1}-k} : i \in [p-1]\right\}$ of ζ^{m-k} overlap with those of $\zeta^{m-k'}$, we then have $ip^{\ell-1} - k = i'p^{\ell-1} - k'$ for some $i, i' \in [p-1]$ and $k, k' \in [p^{\ell-1}]$. We have $|i' - i|p^{\ell-1} = |k' - k| < p^{\ell-1}$ which forces $i = i'$ and hence $k = k'$. In other words, the sets of monomials of ζ^{m-k} are non-overlapping for distinct $k \in [p^{\ell-1}]$. For $i \in \mathbb{Z}_{dm}$, write $i = jm + k$ for $j \in \mathbb{Z}_d$ and $k \in \mathbb{Z}_m$, and rename a_i to $a_{j,k}$. Then $a = \sum_{i \in \mathbb{Z}_{dm}} a_i \cdot \zeta^i = \sum_{j \in \mathbb{Z}_d} \zeta^{jm} \cdot \sum_{k \in \mathbb{Z}_m} a_{j,k} \cdot \zeta^k = \sum_{j \in \mathbb{Z}_d} \sum_{k \in \mathbb{Z}_m} a_{j,k} \cdot \zeta^k \coloneqq \sum_{j \in \mathbb{Z}_d} \bar{a}_j$. We observe that each term $\bar{a}_j = \sum_{k \in \mathbb{Z}_m} a_{j,k} \cdot \zeta^k$ where $\max_{i \in \mathbb{Z}_{dm}} \|a_i\| \le \alpha$ can be reduced using the above identities to $\bar{a}_j = \sum_{k \in \mathbb{Z}_{\varphi(m)}} a'_{j,k} \cdot \zeta^k$ with $\max_{k \in \mathbb{Z}_{\varphi(m)}} \left\|a'_{j,k}\right\| \le 2\alpha$. If $a_i \ge 0$ for all $i \in \mathbb{Z}_{dm}$, then we have $\max_{k \in \mathbb{Z}_{\varphi(m)}} \left\|a'_{j,k}\right\| \le \alpha$. The claim then follows. □

Proposition 1. *Let $i \in \mathbb{N}$, $m = p^\ell$ for some prime p, $\zeta = \zeta_m$ and $a \in \mathcal{R}$, then $\|\zeta_m^i \cdot a\| \le 2\|a\|$. When $p = 2$ then $\|\zeta_m^i \cdot a\| = \|a\|$.*

Proof. Since the power-of-two case is well known to just be a rotation, we treat the general case. Let $j = i \bmod m$ then $\zeta^i \cdot a = \zeta^j \cdot a$. Write $a = \sum_{k \in \mathbb{Z}_m} a_k \zeta^k$ ($a_k = 0$ for $k \ge \varphi(m)$), then

$$\begin{aligned}
\zeta^j \cdot a &= \sum_{k \in \mathbb{Z}_m} a_k \cdot \zeta^{j+k} \\
&= \sum_{k:\ j+k<m} a_k \cdot \zeta^{j+k} + \zeta^m \cdot \sum_{k:\ m \le j+k < 2m-1} a_k \cdot \zeta^{j+k-m} \\
&= \sum_{k' \in \mathbb{Z}_m} a_{k'-j} \cdot \zeta^{k'} + \sum_{k'' \in \mathbb{Z}_m} a_{k''+m-j} \cdot \zeta^{k''} = b + c.
\end{aligned}$$

By Lemma 1, b and c can each be expressed in the powerful basis with ternary coefficients. Therefore $\left\|\zeta^i \cdot a\right\| = \|b + c\| \leq \|b\| + \|c\| \leq 2 \cdot \|a\|$. ☐

Combining the above we arrive at bounds for $\gamma_{\mathcal{R},d}$.

Proposition 2. *If $\mathcal{R}$ is a prime-power cyclotomic ring, then $\gamma_{\mathcal{R},d} \leq \min(2d, 2^{d-1}) \cdot \varphi(m)^{d-1}$. If $\mathcal{R}$ is a power-of-2 cyclotomic ring, then $\gamma_{\mathcal{R},d} \leq \varphi(m)^{d-1}$.*

Proof. For the power-of-2 case and $a, b \in \mathcal{R}$, write $a \cdot b$ as $\varphi(m)$ multiplications of the form $a_i \zeta^i \cdot b$, where the a_i are the coefficients of a. By Proposition 1, we obtain $\gamma_{\mathcal{R}} \leq \varphi(m)$. Recursively composing gives the claimed bound.

For the general prime-power case, the same argument gives $\gamma_{\mathcal{R},d} \leq 2^{d-1} \cdot \varphi(m)^{d-1}$. For the other bound, consider the product $r = a_{(0)} \cdots a_{(d-1)}$ for $a_{(i)} \in \mathcal{R}$. Write $r = a_{(0)} \cdots a_{(d-1)} = \sum_{i \in \mathbb{Z}_{dm}} r_i \cdot \zeta^i$ without modular reduction. Then for each coefficient r_i of r we have $\|r_i\| \leq \varphi(m)^{d-1} \cdot \prod_{j \in \mathbb{Z}_d} \left\|a_{(j)}\right\|$. By Lemma 1, after reduction we have $\|r\| \leq 2d \cdot \varphi(m)^{d-1} \cdot \prod_{j \in \mathbb{Z}_d} \left\|a_{(j)}\right\|$. ☐

We finish this subsection by giving some propositions that will be useful when we construct (s, t)-subtractive sets in Sections 3.1 and 3.2.

Proposition 3. *For any $m \geq 2$, $\sum_{i \in \mathbb{Z}_m} \zeta_m^i = 0$.*

Proof. We realise $\zeta_m^m - 1 = (\zeta_m - 1) \cdot \left(\sum_{i \in \mathbb{Z}_m} \zeta_m^i\right) = 0$ but $\zeta_m \neq 1$. ☐

Proposition 4. *Let $m = p^\ell \in \mathbb{N}$ for some prime p, then $\left\|(1 - \zeta^n)/(1 - \zeta^f)\right\| \leq 1$ for $n, f \in \mathbb{Z}_m^*$.*

Proof. Let $g = f^{-1} \mod m$ and $k = g \cdot n \bmod m$. Then

$$(1 - \zeta^n)/(1 - \zeta^f) = (1 - \zeta^{fgn})/(1 - \zeta^f) = \sum_{i \in \mathbb{Z}_k} \zeta^{f \cdot i}.$$

Note that for any $i \in \mathbb{Z}_k \setminus \{0\}$, we have $i \in \mathbb{Z}_m^*$. Therefore, observing that $f\mathbb{Z}_m = \mathbb{Z}_m$ since $f \in \mathbb{Z}_m^*$, we note that the sum $1 + \sum_{i \in \mathbb{Z}_k \setminus \{0\}} \zeta^{f \cdot i}$ can be expressed as $a = \sum_{i \in \mathbb{Z}_m} a_i \zeta^i$ with binary coefficients a_i. Then by Lemma 1 we conclude that a can be expressed in the powerful basis as a ternary vector. ☐

2.3 Ideals in Cyclotomic Rings

Our results critically rely on the presence and absence of ideals in $\mathcal{R}$. We recall some basic facts. In the ring of integers $\mathcal{R}$ of any number field, any ideal $\mathcal{I} \in \mathcal{R}$ can written in a unique way as $\mathcal{I} = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\mathcal{I})}$, the product being over a finite set of prime ideals, and the exponent $v_{\mathfrak{P}}(\mathcal{I})$ being in $\mathbb{Z}$. When $\mathcal{I}$ is an integral ideal then all $v_{\mathfrak{P}}(\mathcal{I}) \geq 0$ [15, Thm 4.6.14]. Otherwise it is fractional. We mostly deal with integral ideals in this work. The norm $N(\mathcal{I})$ of the ideal $\mathcal{I}$, i.e. $|\mathcal{R}/\mathcal{I}|$, is $N(\mathcal{I}) = \prod_{\mathfrak{P}} N(\mathfrak{P}^{v_{\mathfrak{P}}(\mathcal{I})}) = \prod_{\mathfrak{P}} N(\mathfrak{P})^{v_{\mathfrak{P}}(\mathcal{I})}$ [15, p.187]. For any prime ideal $\mathfrak{P} \subset \mathcal{R}$ we have $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime $p \in \mathbb{Z}$ and we write that $\mathfrak{P}$ "is above" p [15, Prop. 4.8.1]. Moreover, for any prime $p \in \mathbb{Z}$ there exist positive integers e_i such that $p\mathcal{R} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ [15, Thm. 4.8.3], the integer e_i is called the "ramification index" of p at $\mathfrak{P}_i$. The degree f_i of the field extension defined by $f_i = [\mathcal{R}/\mathfrak{P}_i : \mathbb{Z}_p]$ is the "residual degree" of p. We have $N(\mathfrak{P}_i) = p^{f_i}$ and $\sum_{i=1}^{g} e_i f_i = \varphi(m)$ [15, Thm. 4.8.5]. Since $\mathbb{Q}[\zeta_m]$ is a Galois extension, all $e_i = e$ for some fixed e and $f_i = f$ for some fixed f and $\varphi(m) = efg$ [15, Thm. 4.8.6]. A prime $p \in \mathbb{Z}$ ramifies, i.e. has some $e_i > 1$, if and only if it divides the discriminant of $\mathbb{Q}[\zeta_m]$ [15, Thm. 4.8.8]. The discriminant of a prime-power cyclotomic field of order q^k is given by $\pm q^{q^{n-1}((q-1)\cdot n-1)}$, i.e. a power of q [37, Prop. 2.1]. Thus, on the one hand, q ramifies completely in $\mathbb{Z}[\zeta_{q^k}]$ and $\langle q \rangle = \left\langle 1 - \zeta_{q^k} \right\rangle^{\varphi(m)}$ [37, Lem. 1.4, Prop. 2.3, p.15]. On the other hand, for all $p \neq q$ we have $e = 1$ and obtain $\varphi(m) = fg$. For any prime $p \in \mathbb{Z}$ that does not divide m, let f be the smallest positive integer s.t. $p^f \equiv 1 \bmod m$. Then p splits into $g = \varphi(m)/f$ distinct prime ideals in $\mathcal{R}$ [37, Thm. 2.13]. Note that this implies $p^f > m$. Combining these results, we obtain:

Proposition 5. *Let $\mathcal{R} = \mathbb{Z}[\zeta_m]$ with $m = p^k$ a prime power. Then there exists no ideal of norm $\leq m$ in $\mathcal{R}$ except for the ideals above p, i.e. powers of $\langle 1 - \zeta_m \rangle$. The proper ideal of smallest norm is $\langle 1 - \zeta_m \rangle$ of norm $N(\langle 1 - \zeta_m \rangle) = p$.*

Remark 1. The bound in Proposition 5 is tight. For example, in $\mathbb{Z}[\zeta_{256}]$, the ideal $\langle 257, \zeta_{256} + 3 \rangle$ is of norm $m + 1$ not above 2. There are, however, $\mathbb{Z}[\zeta_m]$ where no ideal of norm $m + 1$ exists. For example, no such ideal exists in $\mathbb{Z}[\zeta_{1024}]$: the ideal with smallest norm not above 2 has norm 12289 (found by brute force search).

2.4 Proof of Knowledge

Let $R(\mathsf{stmt}, \mathsf{wit})$ be a binary relation. The language L associated to the relation R is a set $L := \{\mathsf{stmt} : \exists\ \mathsf{wit}\ s.t.\ R(\mathsf{stmt}, \mathsf{wit}) = 1\}$.

Definition 2 (Proof Systems). *A proof system Π is an interactive protocol $\langle \mathcal{P}(\mathsf{stmt}, \mathsf{wit}), \mathcal{V}(\mathsf{stmt}) \rangle$ between a* PPT *prover $\mathcal{P}$ and a* PPT *verifier $\mathcal{V}$, both input a statement* stmt*. The prover $\mathcal{P}$ additionally inputs a witness* wit*. Upon termination the verifier $\mathcal{V}$ should decide to accept or reject* stmt *by outputing a bit b, while the prover $\mathcal{P}$ outputs nothing. For convenience we write $b \leftarrow \langle \mathcal{P}(\mathsf{stmt}, \mathsf{wit}), \mathcal{V}(\mathsf{stmt}) \rangle$.*

A wide class of proof systems, including the so-called sigma protocols, conform to the following pattern.

Definition 3 (Challenges, Moves, Public Coin). *A proof system Π is said to be f-challenge, $(2g + 1)$-move, and public-coin with challenge sets $S_{i,j}$ for $i \in [f]$ and $j \in [g]$, if the protocol $\langle \mathcal{P}, \mathcal{V} \rangle$ conforms to the following pattern:*

- $2g + 1$-*Move: There are in total $2g + 1$ messages being communicated, where $\mathcal{P}$ sends the first, $\mathcal{V}$ sends the second, $\mathcal{P}$ sends the third, and so on. The prover $\mathcal{P}$ sends the last, i.e. $(2g + 1)$-th message and after which the verifier $\mathcal{V}$ outputs a bit b.*

– *f-Challenge and Public-Coin: For $j \in [g]$, the j-th message sent by $\mathcal{V}$ is a tuple $(c_{i,j})_{i\in[f]}$ where $c_{i,j} \leftarrow\$ S_{i,j}$ for all $i \in [f]$.*

A proof system Π should satisfy completeness and knowledge soundness. We omit the zero-knowledge property as it is not needed for our purpose.

Definition 4 (ϵ-Completeness). *Π is ϵ-complete relative to L if*

$$\mathsf{Pr}\left[\langle \mathcal{P}(\mathsf{stmt}, \mathsf{wit}), \mathcal{V}(\mathsf{stmt})\rangle\right] \geq \epsilon$$

whenever $\mathsf{stmt} \in L$ and $R(\mathsf{stmt}, \mathsf{wit}) = 1$. If $\epsilon = 1$, Π is perfectly complete.

Definition 5 (κ-Knowledge Soundness). *Let $\mathcal{E}$ be a PPT knowledge extractor. Π is said to have κ-knowledge soundness relative to $(\mathcal{E}, L')$, if for any stmt and for any (unbounded) adversary $\mathcal{A}$ such that $\langle \mathcal{A}, \mathcal{V}(\mathsf{stmt})\rangle = 1$ with probability $\rho > \kappa$ (over the randomness of $\mathcal{A}$ and $\mathcal{V}$), $\mathcal{E}^{\mathcal{A}}$ outputs wit such that $R'(\mathsf{stmt}, \mathsf{wit}) = 1$ with probability at least $\rho - \kappa$, where R' is the relation associated to L'.*

If the above holds, we call Π a proof of knowledge, κ the knowledge error of Π, $\mathcal{E}$ an extractor for L'. If $\kappa = 0$ we say Π has perfect knowledge soundness. If the above only holds for PPT adversaries $\mathcal{A}$, we say that Π has computational κ-knowledge soundness. Π is then called an argument of knowledge by convention.

We remark that a proof system Π could be complete relative to L while having knowledge soundness relative to L', where $L \subset L'$ are not necessarily equal. In this case we say that Π is a proof system for the languages (L, L'). This is common in lattice-based proof systems where the knowledge extractor is only able to extract a relaxed witness of the statement being proven.

3 Subtractive Sets over Cyclotomic Rings

As the central tool for our results, we construct (generalised) substractive sets over cyclotomic rings. Let $S := \{c_0, \ldots, c_{n-1}\} \subseteq_n \mathcal{R}$. Borrowing the terminology from [32,34], we say that S is *subtractive* if $c_i - c_j$ is invertible over $\mathcal{R}$ for any distinct i and j. Since (the products of) $c_i - c_j$ might be not quite invertible, but divide some element $s \in \mathcal{R}$, we generalise the notion of subtractiveness as follows.

Definition 6 ((s,t)-Subtractive Sets[8]). *For $s \in \mathcal{R}$ and $1 < t \leq n \in \mathbb{N}$, we say that $S \subseteq_n \mathcal{R}$ is (s,t)-subtractive if for any $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t S$, and for all $i \in \mathbb{Z}_t$, it holds that $s \in \left\langle \prod_{j\in\mathbb{Z}_t\setminus\{i\}} (c_i - c_j)\right\rangle$. The element s is called the slack of S. If S is $(1,n)$-subtractive, meaning that $c_i - c_j$ is invertible in $\mathcal{R}$ for any distinct $i, j \in \mathbb{Z}_n$, we simply say that S is subtractive.*

The expansion factor $\gamma_S^{(s,t)}$ of S (as an (s,t)-subtractive set) is defined as $\gamma_S^{(s,t)} := \max_{T\subseteq_t S, i\in\mathbb{Z}_t} \left\| s / \prod_{j\in\mathbb{Z}_t\setminus\{i\}} (c_i - c_j)\right\|$ where the maximum is over all t-subsets $T \subseteq_t S$ and all $i \in \mathbb{Z}_t$.

[8] Special cases of (s,t)-substractive sets are studied in the literature under different names. For example, $(1,2)$-subtractive sets are called exceptional sets [16,21] and sequences [1], while $(s,2)$-subtractive sets are called s-exceptional sets [2]. We choose the name "subtractive" since it appears to be the earliest [32] and the most informative.

The above definition of (s,t)-subtractive sets is motivated by the problem of solving (dual) Vandermonde systems of linear equations of the form

$$\mathbf{V}_T \cdot \mathbf{z} = s \cdot \mathbf{w} \quad (1) \qquad \text{and} \qquad \mathbf{V}_T^{\intercal} \cdot \mathbf{z} = s \cdot \mathbf{w} \quad (2)$$

respectively in the variable $\mathbf{z}$ where $\mathbf{V}_T$ is the Vandermonde matrix

$$\mathbf{V}_T = \begin{pmatrix} 1 & c_0 & \cdots & c_0^{t-1} \\ 1 & c_1 & \cdots & c_1^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & c_{t-1} & \cdots & c_{t-1}^{t-1} \end{pmatrix} \tag{3}$$

defined by the elements in $T = \{c_0, \ldots, c_{t-1}\}$ and $\mathbf{t} \in \mathcal{R}^t$ is some vector over $\mathcal{R}$. If S is (s,t)-subtractive, then for any $T \subseteq_t S$, Equations (1) and (2) each admits a solution $\mathbf{z}$ over $\mathcal{R}$.

Since fully expanded formulae for the solutions to Equations (1) and (2) (instead of, e.g. those in terms of determinants or matrix inverses) do not seem to be widely available in the literature, we give them explicitly.

Proposition 6. *Fix $T = \{c_0, \ldots, c_{t-1}\}$. Let $\mathbf{V}_T$ be the Vandermonde matrix for T, i.e. $(\mathbf{V}_T)_{i,j} = c_i^j$ for $i, j \in \mathbb{Z}_t$. For $i \in \mathbb{Z}_t$, let $T_i \coloneqq T \setminus \{c_i\}$ and $\binom{T_i}{j} \coloneqq \sum_{J \subseteq_j T_i} \prod_{c \in J} c \in \mathcal{R}$, the latter denoting the sum of products of j elements in T_i where the sum is over all possible j-subsets of T_i. Further, let $d_i \coloneqq \prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \in \mathcal{R}$ and $\mathbf{w} = (w_0, \ldots, w_{t-1})$.*

Then, the solution to $\mathbf{V}_T \cdot \mathbf{z} = s \cdot \mathbf{w}$ is given by $\mathbf{z} = (z_0, \ldots, z_{t-1})$ where

$$z_i = \sum_{j \in \mathbb{Z}_t} (-1)^{t-i-1} \frac{s}{d_j} \binom{T_j}{t-i-1} w_j.$$

The solution to $\mathbf{V}_T^{\intercal} \cdot \mathbf{z} = s \cdot \mathbf{w}$ is given by $\mathbf{z} = (z_0, \ldots, z_{t-1})$ where

$$z_i = \sum_{j \in \mathbb{Z}_t} (-1)^{t-j-1} \frac{s}{d_i} \binom{T_i}{t-j-1} w_j.$$

Furthermore, if S is (s,t)-subtractive then for any $T \subseteq_t S$, we have s/d_i and $s/d_j \in \mathcal{R}$ for all $i, j \in \mathbb{Z}_t$, and therefore $z_i \in \mathcal{R}$ for all $i \in \mathbb{Z}_t$.

In the context of cryptography, problems in the form $\mathbf{V}_T \cdot \mathbf{z} = s \cdot \mathbf{w}$ arise naturally, e.g. when recovering secrets shared using Shamir secret sharing. On the other hand, problems in the form $\mathbf{V}_T^{\intercal} \cdot \mathbf{z} = s \cdot \mathbf{w}$ arise, e.g. when constructing knowledge extractors for Schnorr-like proof systems.

We first prove a simple property that, if S is (s,t)-subtractive, then it is also $(s, t-1)$-subtractive.

Proposition 7. *If S is (s,t)-subtractive, then S is (s,t')-subtractive for $t' \leq t$.*

Proof. Fix any $t' \in \{2, \ldots, t\}$ and any $T' = \{c_0, \ldots, c_{t'-1}\} \subseteq_{t'} S$. Let T be such that $T' \subseteq_{t'} T \subseteq_t S$. Write $T = \{c_0, \ldots, c_{t'-1}, \ldots, c_{t-1}\}$. Since S is (s,t)-subtractive, it holds that $s \in \left\langle \prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \right\rangle$ for all $j \in \mathbb{Z}_t$. However, for all $i \in \mathbb{Z}_{t'}$, it holds that $\left\langle \prod_{j \in \mathbb{Z}_t \setminus \{i\}} (c_i - c_j) \right\rangle \subseteq \left\langle \prod_{j \in \mathbb{Z}_{t'} \setminus \{i\}} (c_i - c_j) \right\rangle$. We therefore have $s \in \left\langle \prod_{j \in \mathbb{Z}_{t'} \setminus \{i\}} (c_i - c_j) \right\rangle$ which means S is (s,t')-subtractive. $\square$

To prepare for our impossibility results, we generalise the notion of subtractive sets to weak subtractive sets which permit arbitrary ring operations on differences.

Definition 7 (Weak (s,t)-Subtractive Sets). *For $s \in \mathcal{R}$ and $1 < t \leq n \in \mathbb{N}$, $S \subseteq_n \mathcal{R}$ is weakly (s,t)-subtractive if for any $T \subseteq_t S$, it holds that $s \in \langle T - T \rangle$.*

Since subtractive sets are defined by products of differences, they are weakly $(s,2)$-subtractive.

Proposition 8. *If S is (s,t)-subtractive, then S is weakly $(s,2)$-subtractive.*

Proof. Fix any $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t S$. Since S is (s,t)-subtractive,

$$s \in \left\langle (c_0 - c_1) \cdot \prod_{j \in \mathbb{Z}_t \setminus \{0,1\}} (c_0 - c_j) \right\rangle \in \langle c_0 - c_1 \rangle. \qquad \square$$

The following proposition is immediate by realising that for any $T' \supseteq T$ we have $\langle T' - T' \rangle \supseteq \langle T - T \rangle$.

Proposition 9. *If $S \subseteq_n \mathcal{R}$ is weakly (s,t) subtractive then S is weakly (s,t') subtractive for any $t < t' \leq n$.*

Remark 2. Note that t behaves differently between (s,t)-subtractive sets and weakly (s,t)-subtractive sets. On the one hand, S being (s,t)-subtractive implies S being (s,t')-subtractive for *smaller* t'. On the other hand, S being weakly (s,t)-subtractive implies S being weakly (s,t')-subtractive for *larger* t'.

3.1 Power-of-2 Cyclotomic Rings

Power-of-2 cyclotomic rings $\mathcal{R} = \mathbb{Z}[\zeta_m]$, where $m = 2^\ell$ for some $\ell \in \mathbb{N}$, are popular among lattice-based constructions due to implementation convenience such as fast multiplication via a number theoretic transform (NTT). We construct families of (s,t)-subtractive sets over $\mathcal{R}$ with different tradeoffs between n, t, and s.

Theorem 1. *Let $\mathcal{R} = \mathbb{Z}[\zeta_m]$ with $m = 2^\ell \geq 4$. Then for $i = 0, \ldots, \ell$, the set*

$$S_i \coloneqq \left\{0, 1, \zeta, \ldots, \zeta^{2^i - 1}\right\} \subseteq_{n_i} \mathcal{R}$$

is $(s_{i,t}, t)$-subtractive for any $s_{i,t} \in \langle 1 - \zeta \rangle^{\lceil \log t \rceil (n_i - 1)/2}$, where $n_i = 2^i + 1$.

Let j_t be the smallest such that $\lceil \log t \rceil \leq 2^{j_t}$. If $i + j_t \leq \ell$, then we can pick $s_{i,t} = 1 - \zeta^{2^{i+j_t-1}}$ such that $\gamma_{S_i}^{(s_{i,2},2)} = 1$ and $\gamma_{S_i}^{(s_{i,3},3)} \leq \varphi(m)$ for all $i = 0, \ldots, \ell$. Empirically, for $4 \leq m \leq 2048$, we have $\gamma_{S_{\ell-1}}^{(2,3)} = m/8$ and $\gamma_{S_{\ell-2}}^{(1-\zeta^{m/4},3)} = m/16$.

Proof. If $i = 0$, then $S_i = \{0, 1\}$ is subtractive. In the following we assume $i \in [\ell]$.

For $k \in \mathbb{Z}$, let $\mathrm{Ev}(k)$ be the even part of k, i.e. the largest power of 2 which divides k. It suffices to consider the case $0 \notin T \subseteq_t S_i$, since in the case where $0 \in T$, the difference between any other element in T and 0 is a unit. To handle both cases together, let $T' = T \setminus \{0\}$ so that $t' = |T'| = t$ if $0 \notin T$ and $t' = t - 1$ otherwise. In any case, we have $t' \leq 2^i$ and $t' \leq t$. Write $T' = \left\{\zeta^{j_0}, \ldots, \zeta^{j_{t'-1}}\right\}$. We consider the ideal

$$\begin{aligned}
\left\langle \prod_{k \in \mathbb{Z}_{t'} \setminus \{0\}} (\zeta^{j_0} - \zeta^{j_k}) \right\rangle &= \left\langle \prod_{k \in \mathbb{Z}_{t'} \setminus \{0\}} (1 - \zeta^{j_0 - j_k}) \right\rangle \\
&= \left\langle \prod_{k \in \mathbb{Z}_{t'} \setminus \{0\}} (1 - \zeta^{\mathrm{Ev}(j_0 - j_k)}) \right\rangle \qquad (4) \\
&= \prod_{k \in \mathbb{Z}_{t'} \setminus \{0\}} \langle 1 - \zeta \rangle^{\mathrm{Ev}(j_0 - j_k)} \qquad (5) \\
&= \langle 1 - \zeta \rangle^{\sum_{k \in \mathbb{Z}_{t'} \setminus \{0\}} \mathrm{Ev}(j_0 - j_k)}.
\end{aligned}$$

For Equality (4) we use that if $k = ef$ with e a power of 2 and f odd, then $1 - \zeta^{ef}$ and $1 - \zeta^e$ are divisible by each other in $\mathcal{R}$. First, note that $(1 - \zeta^{ef})/(1 - \zeta^e) = 1 + \zeta^e + \cdots + \zeta^{e(f-1)}$. Second, since $\gcd(f, m) = 1$, let $g = f^{-1} \bmod m$ and observe $(1 - \zeta^e)/(1 - \zeta^{ef}) = (1 - \zeta^{efg})/(1 - \zeta^{ef}) = 1 + \zeta^{ef} + \cdots + \zeta^{ef(g-1)}$. For Equality (5) we use $1 - \zeta^2 = -(1 - \zeta)^2 + 2(1 - \zeta)$, $2 \in \left\langle (1 - \zeta)^2 \right\rangle$, and $2 \in \langle 1 - \zeta^2 \rangle$.

Note that since $0 \leq j_0, j_k < 2^i$, we have $\mathrm{Ev}(j_0 - j_k) \leq 2^{i-1}$. Furthermore, for any fixed j_0, there is at most one j_k such that $\mathrm{Ev}(j_0 - j_k) = 2^{i-1}$. Beside such k, there are then at most $2 = 2^1$ other j_k's such that $\mathrm{Ev}(j_0 - j_k) = 2^{i-2}$. Beside these k's, there are at most $4 = 2^2$ other j_k's such that $\mathrm{Ev}(j_0 - j_k) = 2^{i-3}$. Continue this way, we have

$$\begin{aligned}
\sum_{k \in \mathbb{Z}_{t'} \setminus \{0\}} \mathrm{Ev}(j_0 - j_k) &\leq 1 \cdot 2^{i-1} + 2 \cdot 2^{i-2} + \cdots + 2^{\tau-1} \cdot 2^{i-\tau-2} + (t' - 2^\tau) \cdot 2^{i-\tau-1} \\
&< 1 \cdot 2^{i-1} + 2 \cdot 2^{i-2} + \cdots + 2^{\tau-1} \cdot 2^{i-\tau-2} + 2^\tau \cdot 2^{i-\tau-1} \\
&= (\tau + 1) \cdot 2^{i-1} \leq \lceil \log t' \rceil 2^{i-1} \leq \lceil \log t \rceil 2^{i-1}
\end{aligned}$$

where τ is the maximum non-negative integer such that $1 + 2 + 4 + \cdots + 2^{\tau-1} \leq t' - 2$ or equivalently $2^\tau < t' \leq 2^{\tau+1}$. Note that $2^\tau < t' \leq 2^i$ and hence $\tau < i$. Therefore $i - \tau - 1 \geq 0$ and hence $2^{i-\tau-1} \geq 1$.

Since $\sum_{k \in \mathbb{Z}_{t'} \setminus \{0\}} \mathrm{Ev}(j_0 - j_k) \leq \lceil \log t \rceil 2^{i-1}$, we have

$$\langle 1 - \zeta \rangle^{\lceil \log t \rceil 2^{i-1}} \subseteq \langle 1 - \zeta \rangle^{\sum_{k \in \mathbb{Z}_{t'} \setminus \{0\}} \mathrm{Ev}(j_0 - j_k)} = \left\langle \prod_{k \in \mathbb{Z}_{t'} \setminus \{0\}} (\zeta^{j_0} - \zeta^{j_k}) \right\rangle$$

for all $k \in \mathbb{Z}_{t'}$. Therefore, for any $s_{i,t} \in \langle 1-\zeta \rangle^{\lceil \log t \rceil 2^{i-1}}$, we have

$$s_{i,t} \in \left\langle \prod_{k \in \mathbb{Z}_{t'} \setminus \{0\}} (\zeta^{j_0} - \zeta^{j_k}) \right\rangle$$

for all $k \in \mathbb{Z}_{t'}$. Thus S_i is $(s_{i,t}, t)$-subtractive.

Let j_t be the smallest such that $\lceil \log t \rceil \leq 2^{j_t}$. Let $s_{i,t} = 1 - \zeta^{2^{e_{i,t}}}$ where $e_{i,t} \coloneqq i + j_t - 1$. Suppose $i + j_t \leq \ell$, then $\lceil \log t \rceil 2^{i-1} \leq 2^{i+j_t-1} \leq 2^{\ell-1} = m/2$. Therefore $\langle s_{i,t} \rangle = \langle 1-\zeta \rangle^{2^{e_{i,t}}} \subseteq \langle 1-\zeta \rangle^{\lceil \log t \rceil 2^{i-1}}$ and hence $s_{i,t} \in \langle 1-\zeta \rangle^{\lceil \log t \rceil 2^{i-1}}$.

We now establish $\gamma_{S_i}^{(s,t)}$ as claimed above, starting with $t = 2$. Hence, we have $j_t = \lceil \log \lceil \log t \rceil \rceil = 0$, $s_{i,2} = 1 - \zeta^{2^{i-1}}$ and

$$\gamma_{S_i}^{(s_{i,2},2)} = \max_{\alpha,\beta \in \mathbb{Z}_{2^i}} \left\| \frac{s_{i,2}}{\zeta^\alpha - \zeta^\beta} \right\| = \max_{\alpha,\beta \in \mathbb{Z}_{2^i}} \left\| \frac{1 - \zeta^{2^{i-1}}}{\zeta^\alpha (1 - \zeta^{\beta-\alpha})} \right\| = \max_{\alpha,\beta \in \mathbb{Z}_{2^i}} \left\| \frac{1 - \zeta^{2^{i-1}}}{1 - \zeta^{2^\eta \mu}} \right\| \leq 1$$

where $2^\eta = \mathrm{Ev}(\beta - \alpha)$ with $\eta \in \mathbb{Z}_i$, μ is the odd part of $\beta - \alpha$ satisfying $\beta - \alpha = 2^\eta \mu$, and the last equality can be derived through a routine calculation.

For $t = 3$, hence $j_t = \lceil \log \lceil \log t \rceil \rceil = 1$ and $s_{i,2} = 1 - \zeta^{2^i}$, we have

$$\begin{aligned}
\gamma_{S_i}^{(s_{i,3},3)} &= \max_{\alpha,\beta,\gamma \in \mathbb{Z}_i} \left\| \frac{s_{i,3}}{(\zeta^\alpha - \zeta^\beta)(\zeta^\alpha - \zeta^\gamma)} \right\| \\
&= \max_{\alpha,\beta,\gamma \in \mathbb{Z}_i} \left\| \frac{1 - \zeta^{2^i}}{(1 - \zeta^{\beta-\alpha})(1 - \zeta^{\gamma-\alpha})} \right\| = \max_{\alpha,\beta,\gamma \in \mathbb{Z}_i} \left\| \frac{1 - \zeta^{2^{i-1}}}{1 - \zeta^{\beta-\alpha}} \cdot \frac{1 + \zeta^{2^{i-1}}}{1 - \zeta^{\gamma-\alpha}} \right\| \\
&\leq \gamma_{\mathcal{R}} \cdot \left(\gamma_{S_i}^{(s_{i,2},2)} \right)^2 = \gamma_{\mathcal{R}} = \varphi(m).
\end{aligned}$$

The empirical results are verified by direct computation. □

We highlight some notable settings of (s, t) in Theorem 1. The case $t = 2$ is useful for constructing knowledge extractors of Schnorr-like proof systems. In this setting, $S_\ell \subseteq_{m+1} \mathcal{R}$ chosen in prior works [6] is $(2, 2)$-subtractive, while $S_{\ell-1} \subseteq_{m/2+1}$ is $(1 - \zeta^{m/4}, 2)$-subtractive. Note that although $\left\|1 - \zeta^{m/4}\right\| = 1$, multiplying $(1 - \zeta^{m/4})$ to an element $f \in \mathcal{R}$ results in an element of length $\left\|(1 - \zeta^{m/4}) f\right\| \leq 2\|f\|$ if we consider the infinity norm as prior works did [11], and hence $S_{\ell-1}$ appears to be not better than S_ℓ in terms of slack. However, for the Euclidean norm $\|\cdot\|_2$, we have $\left\|(1 - \zeta^{m/4}) f\right\|_2 < \sqrt{2}\|f\|_2 \leq 2\|f\|_2 = \|2f\|_2$.

The case $t = 3$ is useful for lattice Bulletproofs, as we will see in Section 4.1. Bootle *et al.* [11] chose $S_\ell \setminus \{0\} \subseteq_m \mathcal{R}$ as the challenge set for their instantiation of lattice Bulletproof, and essentially proved that $S_\ell \setminus \{0\}$ is $(8, 3)$-subtractive. The above tighter analysis shows that S_ℓ is in fact $(4, 3)$-subtractive. Similar to the $t = 2$ case, we notice that $S_{\ell-1} \subseteq_{m/2+1} \mathcal{R}$ is $(2, 3)$-subtractive and $S_{\ell-2} \subseteq_{m/4+1} \mathcal{R}$ is $(1 - \zeta^{m/4}, 3)$-subtractive. As discussed in the $t = 2$ case, the slack $1 - \zeta^{m/4}$ is better than 2 if we consider the Euclidean norm.

For general n_i and t useful in t-out-of-n_i secret sharing, assuming $m = 2^\ell$ is (polynomially) large enough so that $\ell > i + t_j$, then $\|s_{i,t}\| = 1$, which is more manageable than the $(n!, t)$-subtractive set $\mathbb{Z}_n$ chosen by Boneh *et al.* [8].

We observe that among all sets S_i constructed in Theorem 1, only $S_0 \subseteq_2 \mathcal{R}$ is subtractive, while the others are $(s_{i,t}, t)$-subtractive for some $s_{i,t} \neq 1$. As we will see in Section 3.3, this is not a shortcoming of the construction but rather a fundamental limit in power-of-2 cyclotomic rings. Indeed, in Proposition 12 and Lemma 2 we show that over power-of-2 cyclotomic rings no subtractive set of size greater than 2 exists.

We finish this section with a technical proposition, giving a bound for $\|c_i z_i\|$ that is tighter than the generic bound $2 \cdot \gamma_R \cdot \gamma_S^{(2,3)}$.

Proposition 10. *Let $S = S_{\ell-1}$, $(s, t) = (2, 3)$, $\{c_0, c_1, c_2\} \subset_t S$ and z_i as defined in Proposition 6, then $\|c_i \cdot z_i\| \leq \varphi(m)$. Empirically, for all $8 \leq m = 2^\ell \leq 512$ we have $\max(\|c_i \cdot z_i\|) = \varphi(m) - 2$.*

Proof. We write $c_0 = \zeta^i, c_1 = \zeta^j, c_2 = \zeta^k$. Wlog, we consider

$$c_0 \cdot z_0 = \frac{-s \cdot c_0 \cdot (c_1 + c_2)}{(c_0 - c_1) \cdot (c_0 - c_2)} = \frac{2 \cdot \zeta^i(\zeta^j + \zeta^k)}{(\zeta^i - \zeta^j) \cdot (\zeta^j - \zeta^k)} = \frac{2 \cdot \zeta^{i-j} \cdot (\zeta^{j-k} + 1)}{(\zeta^{i-j} - 1) \cdot (\zeta^{i-k} - 1)}.$$

Multiplying by ζ^{i-j} does not change the norm so we can consider

$$\|g\| = \left\| \frac{2 \cdot (\zeta^{j-k} + 1)}{(\zeta^{i-j} - 1) \cdot (\zeta^{i-k} - 1)} \right\|$$
$$\|2\,g\| = \left\| (\zeta^{j-k} + 1) \cdot \frac{2}{\zeta^{i-j} - 1} \cdot \frac{2}{\zeta^{i-k} - 1} \right\| \leq 2 \cdot \gamma_R \cdot \left(\gamma_S^{(2,2)}\right)^2.$$

Since $\|c_0 \cdot z_0\| = \|g\| = \|2\,g\|/2$, we obtain $\|c_0 \cdot z_0\| \leq \varphi(m)$. The empirical results are verified by direct computation. $\square$

3.2 Prime-Power Cyclotomic Rings

We turn to prime-power cyclotomic rings $\mathcal{R} := \mathbb{Z}[\zeta_m]$ where m is a power of a prime p. Although we are interested mostly in the case $p > 2$, the following results also hold for $p = 2$. To construct subtractive sets over prime-power cyclotomic rings, we recall the well-known fact that $\mu_k := (\zeta^k - 1)/(\zeta - 1)$ is invertible over $\mathcal{R}$ when $\gcd(k, p) = \gcd(k, m) = 1$. Indeed its inverse is given by $\nu_k := \sum_{i \in \mathbb{Z}_h} \zeta^{ik \bmod m}$ where $h = k^{-1} \bmod m$. Our subtractive set of size over prime-power cyclotomic rings of order consist precisely of these invertible elements with an additional zero.

Theorem 2 (Prime-Power). *Let $\mathcal{R} = \mathbb{Z}[\zeta_m]$ with $m = p^\ell$ for some prime p. Then the set*

$$S := \{\mu_0, \ldots, \mu_{p-1}\} \subseteq_p \mathcal{R}$$

is subtractive, where $\mu_i = (\zeta^i - 1)/(\zeta - 1)$ for $i \in \mathbb{Z}_p$. Furthermore, $\gamma_S^{(1,2)} = 1$, $\gamma_S^{(1,3)} \leq 4\varphi(m)$ and $4\,(t-1) \cdot \varphi(m)^{t-2}$ for $3 < t \leq p$. Empirically, $\gamma_S^{(1,3)} = \varphi(m)/2$ for all primes $3 \leq m \leq 277$.

Proof. For any $0 \le i < j < p$, it holds that[9]

$$\begin{aligned} \mu_j - \mu_i &= \frac{\zeta^j - 1}{\zeta - 1} - \frac{\zeta^i - 1}{\zeta - 1} = \sum_{k=0}^{j-1} \zeta^k - \sum_{k=0}^{i-1} \zeta^k = \zeta^i + \zeta^{i+1} + \cdots + \zeta^{j-1} \\ &= \zeta^i \cdot (1 + \zeta + \cdots + \zeta^{j-i+1}) = \zeta^i \cdot \mu_{j-i} \end{aligned}$$

which is a unit in $\mathcal{R}$ since $j - i \in \mathbb{Z}_p^*$. Consequently $\mu_i - \mu_j = (-1) \cdot (\mu_j - \mu_i)$ is also a unit in $\mathcal{R}$. Therefore S is subtractive.

We next upper bound $\gamma_S^{(1,t)}$. In the case $t = 2$, we have

$$\gamma_S^{(1,2)} = \max_{i,j \in \mathbb{Z}_p} \left\| \frac{1}{\mu_j - \mu_i} \right\| = \max_{i,j \in \mathbb{Z}_p} \left\| \frac{1}{\mu_{j-i}} \right\| \le 1$$

where the inequality is due to Proposition 4.

For $2 < t \le p$, let $T = \left\{ \mu_{i_0}, \ldots, \mu_{i_{t-1}} \right\} \subseteq_t S$. We examine the norm of r^{-1} where $r \coloneqq \prod_{j \in [t-1]} (\mu_{i_0} - \mu_{i_j})$. By the above analysis, we know that $\mu_{i_0} - \mu_{i_j}$ equals some power of ζ multiplied by $\mu_{i_0 - i_j}$. Therefore r can be written as $r = \zeta^{j_0} \mu_{j_1} \ldots \mu_{j_{t-1}}$ for some $j_0 \in \mathbb{Z}$ and $j_1, \ldots, j_{t-1} \in \mathbb{Z}_p^*$. Note that multiplication by ζ^{j_0} increases the norm at most by a factor of two. Let $\nu_j = \mu_j^{-1}$ for $j \in \{j_1, \ldots, j_{t-1}\}$. Then $\nu_j = \sum_{i=0}^{k-1} \zeta^{ij \bmod m}$ where $k = j^{-1} \bmod m$. By Lemma 1, we have $\|\nu_j\| \le 1$ for all $j \in \mathbb{Z}_p^*$. Summarising the above, we can upper bound $\gamma_S^{(1,t)}$ as

$$\gamma_S^{(1,t)} \le 2\, \gamma_{\mathcal{R},t-1} \|\nu_{j_1}\| \ldots \|\nu_{j_{t-1}}\| \le 4\,(t-1) \cdot \varphi(m)^{t-2}$$

where in the second inquality we used Proposition 2. When $t = 3$, we can use $\gamma_{\mathcal{R},2} \le 2\varphi(m)$. The empirical results are verified by direct computation. ☐

Remark 3. Theorem 2 can be generalised to give a size $\varphi(\mathrm{rad}(m)) + 1$ subtractive set over the cyclotomic ring of any order m with prime-power factorisation $m = \prod_i p_i^{\ell_i}$, where the radical $\mathrm{rad}(m) = \prod_i p_i$ of m is the product of distinct prime divisors of m, by viewing the m-th cyclotomic ring as a tensor product of the $p_i^{\ell_i}$-th cyclotomic rings.

Proposition 11. *Let S be as defined in Theorem 2, $(s,t) = (1,3)$, $\{c_0, c_1, c_2\} \subset_t S$ and z_i as defined in Proposition 6, $c_i \cdot z_i = \zeta^j \cdot a$ for some a with $\|a\| \le 4\,\varphi(m)$ and thus $\|c_i \cdot z_i\| \le 8\,\varphi(m)$. Empirically, for all prime $3 \le m \le 229$ we have $\max(\|c_i \cdot z_i\|) = \varphi(m) - 1$.*

Proof. We write $c_0 = (\zeta^i - 1)/(\zeta - 1), c_1 = (\zeta^j - 1)/(\zeta - 1), c_2 = (\zeta^k - 1)/(\zeta - 1)$. Wlog, we consider

$$\begin{aligned} c_0 \cdot z_0 &= \frac{-s \cdot c_0 \cdot (c_1 + c_2)}{(c_0 - c_1) \cdot (c_0 - c_2)} = \frac{-(\zeta^i - 1) \cdot (\zeta^j + \zeta^k - 2)}{((\zeta^i - \zeta^j) \cdot (\zeta^i - \zeta^k))} \\ &= -\zeta^{-j-k} \cdot \left[\frac{\zeta^i - 1}{\zeta^{i-j} - 1} \cdot \frac{\zeta^j - 1}{\zeta^{i-k} - 1} + \frac{\zeta^i - 1}{\zeta^{i-j} - 1} \cdot \frac{\zeta^k - 1}{\zeta^{i-k} - 1} \right] \end{aligned}$$

[9] We adopt the convention that the empty sum is 0.

Multiplication by $-\zeta^{-j-k}$ at most doubles the norm (Proposition 1) and we have $\left\|(\zeta^i-1)/(\zeta^j-1)\right\| = 1$ for $j \neq 0$ (Proposition 4). Thus, $\|c_0 \cdot z_0\| \leq 4 \cdot \gamma_R \leq 8\varphi(m)$. The empirical results are verified by direct computation. □

3.3 Impossibility of Large Subtractive Sets

In this section we prove two flavours of impossibility results concerning subtractive sets. The first kind of results state that if S is an (s,t)-subtractive set of sufficient size, then s belongs to the ideal $\langle 1-\zeta \rangle^e$ for some e lower bounded from 0. The second kind of results state that if $\mathcal{R}$ contains an ideal of small algebraic norm, then either S cannot be too large, or S is weakly (s,t)-subtractive with s belonging to that ideal. The key observation in all our proofs is that if we consider $N(\mathcal{I})+1$ elements $c_i \in \mathcal{R}$ then there must be two elements, say, c_i, c_j s.t. $c_i \equiv c_j \bmod \mathcal{I}$ and thus $c_i - c_j \in \mathcal{I}$.

We first prove that $S \subseteq_n \mathcal{R}$ cannot be (s,t)-subtractive unless

$$s \in \mathcal{I} = \langle 1-\zeta \rangle^{\min\{\lceil n/p \rceil, t\}-1}.$$

The size of $\mathcal{I}$ in a sense shrinks when t and n grow, since $|\mathcal{R}/\mathcal{I}| = p^{\min\{\lceil n/p \rceil, t\}-1}$. The result thus rules out all S that are too "large" relative to s, in the sense that $\mathcal{I}$ becomes so "small" that the choice of $s \in \mathcal{I}$ is highly restrictive.

Proposition 12. *Let $\mathcal{R}$ be a prime-power cyclotomic ring of order m a power of p, and $n > p$. If $S \subseteq_n \mathcal{R}$ is (s,t)-subtractive, then $s \in \langle 1-\zeta \rangle^e$ where*

$$e \geq \min\{\lceil n/p \rceil, t\} - 1 > 0.$$

Proof. Proposition 5 shows that $N(\langle 1-\zeta \rangle) = |\mathcal{R}/\langle 1-\zeta \rangle| = p$. The ideal $\langle 1-\zeta \rangle$ therefore partitions $\mathcal{R}$ into p cosets. Let $n = \sum_{k \in \mathbb{Z}_p} n_k$ such that n_k elements in S belong to the k-th coset. Let $\bar{n} := \max_{k \in \mathbb{Z}_p} n_k \geq \lceil n/p \rceil$ be attained when $k = \bar{k}$. Let $T = \{c_0, \ldots, c_{t-1}\} \subseteq_t S$ be such that T contains $\min\{\bar{n}, t\} \geq \min\{\lceil n/p \rceil, t\} > 0$ elements in the $\bar{k}$-th coset. Let j be such that v_j belongs to the $\bar{k}$-th coset. The product $r = \prod_{i \in \mathbb{Z}_t \setminus \{\bar{j}\}} (c_i - c_j)$ has a factor $1-\zeta$ with multiplicity at least $\min\{\lceil n/p \rceil, t\} - 1$. Since S is (s,t)-subtractive, s has a factor $1-\zeta$ with multiplicity at least $\min\{\lceil n/p \rceil, t\} - 1$. In other words, $s \in \langle 1-\zeta \rangle^{\min\{\lceil n/p \rceil, t\}-1}$. □

Remark 4. An interesting observation is that, when $m = 2$ hence $\zeta = -1$ and $\mathcal{R} = \mathbb{Z}$, the above lower bound implies that an (s,t)-subtractive set $S \subseteq_n \mathbb{Z}$ for $t \geq \lceil n/2 \rceil$ must have $|s| \geq 2^{\lceil n/2 \rceil - 1} = 2^{\Omega(n)}$. On the other hand, the trivial choice of $S = \mathbb{Z}_n$ (chosen by, e.g. Boneh *et al.* [8] for higher m) has a slack of $n! = 2^{O(n \lg n)}$ which almost reaches the lower bound. When m is a higher power of 2, there are however much better choices of S, such as the ones constructed in Theorem 1 rather than $S = \mathbb{Z}_n$.

Through a more careful analysis, we can prove a strengthened lower bound.

Lemma 2. *Let $\mathcal{R}$ be a prime-power cyclotomic ring of order m a power of p. Let $n > p^\ell$ for some $\ell \in \mathbb{N}$. If $S \subseteq_n \mathcal{R}$ is (s,t)-subtractive, then $s \in \langle 1-\zeta \rangle^e$ where*

$$e \geq \sum_{i=1}^{\ell} \min\left\{ \lceil n/p^i \rceil - 1, t-1 \right\} > 0.$$

Proof. Let $\mathfrak{P} = \langle 1-\zeta \rangle$. Recall from Proposition 5 that $N(\mathfrak{P}) = |\mathcal{R}/\mathfrak{P}| = p$. Since $|S| = n > p^\ell$, by the pigeonhole principle there exists $S_1 \subseteq_{\lceil n/p \rceil} S$ such that all elements of S_1 belong to the same equivalence class $\mathfrak{C}_1$ modulo $\mathfrak{P}$. Similarly, there exists $S_2 \subseteq_{\lceil n/p^2 \rceil} S_1$ such that all elements of S_1 belong to the same equivalence class $\mathfrak{C}_2$ modulo $\mathfrak{P}^2$. Continue analogously, for $j \in [\ell]$, there exists $S_j \subseteq_{\lceil n/p^j \rceil} S_{j-1}$ such that all elements of S_j belong to the same equivalence class $\mathfrak{C}_j$ modulo $\mathfrak{P}^j$.

Consider a binary matrix H of ℓ rows and n columns, where the first $\lceil n/p^j \rceil$ columns are labeled by the elements of S_j for $j \in [\ell]$. The remaining columns are labeled by the elements of $S \setminus S_1$. The (i,v)-th entry is 1 if v belongs to the equivalence class $\mathfrak{C}_i$ modulo $\mathfrak{P}^i$, i.e. the first $\lceil n/p^i \rceil$ entries of row i are 1.

Pick $T \subseteq_t S$ such that $S_\ell \subseteq \ldots \subseteq S_k \subseteq T \subseteq S_{k-1} \subseteq S$ for some $k \in [\ell]$, where $S_0 := S$. Note that T labels the first t columns of H.

Let $v^* \in S_\ell \subseteq T$ be the element that labels the first column of H, and $\bar{T} = T \setminus \{v^*\}$ labels the second to the t-th column. Consider the product $r = \prod_{v \in \bar{T}} (v - v^*)$. Note that for $v \in \bar{T}$, if v belongs to the equivalence class $\mathfrak{C}_i$ modulo $\mathfrak{P}^i$, then $(v - v^*)$ contributes a factor $(1-\zeta)^i$ of r. The multiplicity of the factor $(1-\zeta)$ of r is at least the number of 1's in the first t columns of H minus that of the first column. By collecting the columns of interest, let H_t be the submatrix of H formed by the second to the t-th column. Observe that the i-th row of H_t contains $\min\left\{ \lceil n/p^i \rceil, t \right\} - 1$ many 1's. Therefore the number of 1's in H_t is given by $\sum_{i=1}^{\ell} \min\left\{ \lceil n/p^i \rceil - 1, t-1 \right\}$. □

Concretely, for power-of-2 cyclotomic rings we obtain:

Corollary 1. *Let $\mathcal{R}$ be a power-of-2 cyclotomic ring of order $m \geq 8$ and $n \geq \varphi(m)$. If $S \subseteq_n \mathcal{R}$ is $(s,3)$-subtractive, then $s \in \langle 1-\zeta \rangle^e$ where $e \geq 2\log_2 m - 3$.*

Proof. Let $m = 2^{\ell+2}$ for some $\ell \in \mathbb{N}$. Then $n \geq \varphi(m) = 2^{\ell+1}$. By Lemma 2 we have $e + \ell \geq \sum_{i=1}^{\ell} \min\left\{ \lceil n/2^i \rceil, 3 \right\}$. Note that since $n \geq 2^{\ell+1}$ we have $n/2^{\ell-1} \geq 4$ and hence $n/2^i \geq 3$ for $i = 1, \ldots, \ell-1$. When $i = \ell$, we have $n/2^\ell \geq 2$ and therefore $\min\left\{ \lceil n/2^\ell \rceil, 3 \right\} \geq 2$. Therefore $e + \ell \geq 3(\ell-1) + 2 = 3\ell - 1$, or in other words $e \geq 2\ell - 1 = 2\log_2 m - 3$. □

Next, we upper bound the size n of weakly (s,t)-subtractive sets.

Lemma 3. *Let $\mathcal{I} \subset \mathcal{R}$ be an ideal of norm $N(\mathcal{I})$. There exists no weakly (s,t)-subtractive set of size $(t-1) \cdot N(\mathcal{I}) + 1$ for $s \notin \mathcal{I}$.*

Proof. Assume S is such a weakly (s,t) subtractive set of size $(t-1) \cdot N(\mathcal{I}) + 1$. There are $N(\mathcal{I})$ cosets of $\mathcal{I}$. Sort the elements of S into buckets depending on which coset of mod $\mathcal{I}$ they land in. By the pigeonhole principle, there must exist at least one bucket containing t elements. Let $T = \{c_i\}_{i\in\mathbb{Z}_t}$ be a such a set of challenges of size t s.t. all $c_i \equiv c_j \bmod \mathcal{I}$ for $i, j \in \mathbb{Z}_t \Leftrightarrow c_i - c_j \in \mathcal{I}$. Thus, $\langle T - T\rangle \subset \mathcal{I}$ and $s \in \mathcal{I}$. □

Finally, deploying Proposition 12 and Lemmas 2 and 3 we arrive at our central impossibility results for power-of-two cyclotomic rings and prime cyclotomic rings.

First, since $(2, t)$-subtractive sets are weakly $(2, 2)$-subtractive and there are power-of-two cyclotomic rings that contain an ideal of norm $m + 1$, we arrive at the theorem below. We state the result for $s = 2$ as opposed to, say, $s = 1 - \zeta$ as the former is more general than the latter: the existence $(1 - \zeta, t)$-subtractive sets implies the existence of $(2, t)$-subtractive sets.

Theorem 3. *There is no family of $(2, t)$-subtractive sets of size $n > m + 1$ in the power of two cyclotomic ring $\mathbb{Z}[\zeta_m]$ where $m = 2^\ell$ for some $\ell \in \mathbb{N}$.*

Putting Theorems 1 and 3 together, we see that our $(2, 3)$-subtractive set construction achieves size $m/2+1$ compared to the limit of $m+1$. This construction is thus within a factor of 2 of being optimal. However, we note that Theorem 3 does not rule out the existence of $(2, t)$-subtractive sets of size $n > m + 1$ for specific choices of m, e.g. $m = 2^{10} = 1024$ is a good candidate, cf. Remark 1.

Second, since $(1, t)$-subtractive sets are weakly $(1, 2)$-subtractive and prime-power cyclotomic rings contain an ideal of norm p, Lemma 3 rules out larger subtractive sets. An alternative route to the same statement is by noting that $e \geq 1$ in Proposition 12 and that $1 \notin \langle 1 - \zeta\rangle$. Therefore the subtractive sets for prime-power cyclotomic rings in Theorem 2 are in a sense optimal. On the flip side it means that over a power-of-2 cyclotomic ring the only subtractive sets are of size 2, such as $S = \{0, 1\}$.

Theorem 4. *There is no subtractive set of size $n > p$ in any prime-power cyclotomic ring $\mathbb{Z}[\zeta_{p^\ell}]$ for any prime $p \in \mathbb{N}$ and any $\ell \in \mathbb{N}$.*

Finally, Lemma 3 rules out many natural algebraic strategies of constructing knowledge extractors for Schnorr-like proof systems that go beyond some generalised form of matrix inversion. For example, an algebraic extractor could attempt to compute s by running an extended Euclidean algorithm on pairs $c_0 - c_1, c_2 - c_3$, i.e. attempt to find (small) r_0, r_1 s.t. $s = r_0 \cdot (c_0 - c_1) + r_1 \cdot (c_2 - c_3)$, cf. [22,35,33] for the application of the Euclidean algorithm for finding small elements of this form in number rings. By Lemma 3 such extensions do not significantly improve the bounds. We will make use of this implicitly in Section 4 below.

4 Proof of Knowledge of Lattice Statements

In this section we give positive and negative results on using subtractive sets over cyclotomic rings to construct proof systems for lattice statements of the form

$$L_{s,\beta} := \left\{(\mathbf{A}, \mathbf{y}) \in \mathcal{R}_q^{h\times k} \times \mathcal{R}_q^h : \exists \mathbf{x} \in \mathcal{R}^k \ s.t.\ \mathbf{A}\mathbf{x} = s\mathbf{y} \wedge \|\mathbf{x}\| \leq \beta\right\}.$$

$$
\begin{array}{lcl}
\multicolumn{3}{l}{\mathit{\Pi}_r.\langle \mathcal{P}((\mathbf{A},\mathbf{y}),\mathbf{x}) | \mathcal{V}(\mathbf{A},\mathbf{y})\rangle \text{ where } (\mathbf{A},\mathbf{y}) \in \mathcal{R}_q^{h\times k_r} \times \mathcal{R}_q^h,\ \mathbf{x} \in \mathcal{R}^{k_r},\ r \in \mathbb{Z}_{\log k}} \\
\hline
\mathbf{l} := \mathbf{A}_1\mathbf{x}_0,\ \mathbf{r} := \mathbf{A}_0\mathbf{x}_1 & \xrightarrow{\mathbf{l},\mathbf{r} \in \mathcal{R}^h} & c \leftarrow\$\, S_0, d \leftarrow\$\, S_1 \\
 & \xleftarrow{c \in \mathcal{R}, d \in \mathcal{R}} & \tilde{\mathbf{A}} := (c\mathbf{A}_0 + d\mathbf{A}_1) \\
 & & \tilde{\mathbf{y}} := d^2\mathbf{l} + cd\mathbf{y} + c^2\mathbf{r} \\
\tilde{\mathbf{x}} := d\mathbf{x}_0 + c\mathbf{x}_1 & \xrightarrow{\tilde{\mathbf{x}} \in \mathcal{R}^{k_{r+1}}} & \tilde{\mathbf{A}} \cdot \tilde{\mathbf{x}} \stackrel{?}{=} \tilde{\mathbf{y}} \\
 & & \|\tilde{\mathbf{x}}\| \stackrel{?}{\leq} \gamma_r
\end{array}
$$

$$
\begin{array}{cl}
\multicolumn{2}{l}{\mathit{\Pi}_{\log k}.\langle \mathcal{P}((\mathbf{A},\mathbf{y}),\mathbf{x}) | \mathcal{V}(\mathbf{A},\mathbf{y})\rangle \text{ where } (\mathbf{A},\mathbf{y}) \in \mathcal{R}_q^{h\times 1} \times \mathcal{R}_q^h,\ \mathbf{x} \in \mathcal{R},\ r = \log k} \\
\hline
\xrightarrow{\mathbf{x} \in \mathcal{R}} & \mathbf{A}\mathbf{x} \stackrel{?}{=} \mathbf{y} \\
 & \|\mathbf{x}\| \stackrel{?}{\leq} \gamma_{\log k}
\end{array}
$$

Fig. 1. Lattice Bulletproof protocol $\mathit{\Pi}_r$ for round $r \in \{0,\ldots,\log k\}$ generalised from [11].

4.1 Generalised Lattice Bulletproof

Let k be a power of 2, $k_r := k/2^r$ and $\gamma_r > 0$ for $r \in \{0,\ldots,\log k\}$, and $S_0, S_1 \subseteq \mathcal{R}$. In Figure 1 we write down a slight generalisation of the lattice Bulletproof protocol in [11], who considered $h = 1$, $\mathcal{R}$ being a power-of-2 cyclotomic ring, and $S_1 = \{1\}$. Given a matrix $\mathbf{A} \in \mathcal{R}^{h\times k_r}$, we can parse it as $\mathbf{A} = (\mathbf{A}_0, \mathbf{A}_1)$ with $\mathbf{A}_i \in \mathcal{R}^{h\times k_{r+1}}$. Similarly, given a vector $\mathbf{x} \in \mathcal{R}^{k_r}$ we can parse it as $\mathbf{x} = (\mathbf{x}_0, \mathbf{x}_1)$ with $\mathbf{x}_i \in \mathcal{R}^{k_{r+1}}$.

Lemma 4. *Suppose that $\|c\| \leq 1$ for all $c \in S_0$ and $\|d\| \leq 1$ for all $d \in S_1$ (which is the case for S constructed in Theorems 1 and 2). Let $\gamma_r = 2^{r+1} \cdot \gamma_{\mathcal{R},r+2} \cdot \beta$ for $r \in \mathbb{Z}_{\log k}$ and $\gamma_{\log k} = \gamma_{\log k-1} = k \cdot \gamma_{\mathcal{R},\log k+1} \cdot \beta$. In $\mathit{\Pi}_0$, if the prover's input $\mathbf{x}^{(0)}$ satisfies $\|\mathbf{x}\| \leq \beta$, then the verifier accepts with certainty. For $r \in [\log k]$, if for all $r' \in [r]$, the prover's input $\mathbf{x}^{(r')}$ is equal to the prover's second message sent in an honest execution of $\mathit{\Pi}_{r'-1}$, then the verifier in $\mathit{\Pi}_r$ accepts with certainty. Consequently, the recursive composition of $\mathit{\Pi}_0,\ldots,\mathit{\Pi}_{\log k}$ yields a proof system $\mathit{\Pi}$ which is perfectly complete relative to $L_{1,\beta}$.*

In case $\mathcal{R} = \mathbb{Z}[\zeta_{2^\ell}]$, S_0 is constructed from Theorem 1, and $S_1 = \{1\}$, then we can set $\gamma_r := 2^{r+1} \cdot \beta$ and $\gamma_{\log k} = k \cdot \beta$ instead.

Proof. For all $r \in \mathbb{Z}_{\log k}$, suppose that $\mathbf{A} \cdot \mathbf{x} = \mathbf{y}$, then

$$
\begin{aligned}
(c\,\mathbf{A}_0 + d\,\mathbf{A}_1) \cdot \mathbf{z} &= (c\mathbf{A}_0 + d\mathbf{A}_1) \cdot (d\mathbf{x}_0 + c\mathbf{x}_1) \\
&= d^2\,\mathbf{A}_1 \cdot \mathbf{x}_0 + c \cdot d \cdot (\mathbf{A}_0 \cdot \mathbf{x}_0 + \mathbf{A}_1 \cdot \mathbf{x}_1) + c^2\,\mathbf{A}_0 \cdot \mathbf{x}_1 \\
&= d^2\,\mathbf{l} + cd\,\mathbf{y} + c^2\,\mathbf{r}.
\end{aligned}
$$

In Π_0, if $\|\mathbf{x}\| \leq \beta$, then observe that $\|d\,\mathbf{x}_0 + c\,\mathbf{x}_1\| \leq 2\,\gamma_{\mathcal{R}}\,\beta$. Fix $r \in [\log k]$. Since for all $r' \in [r]$, the prover's input $\mathbf{x}^{(r')}$ is equal to the prover's second message sent in an honest execution of $\Pi_{r'-1}$, we have that the prover's input $\mathbf{x}^{(r)}$ is equal to a sum of 2^r terms, each term being a product of r challenges and a subvector of $\mathbf{x}^{(0)}$. If $r = \log k$, then the input $\mathbf{x}^{(\log k)}$ is sent directly to the verifier, which has norm upper bounded by $k \cdot \gamma_{\mathcal{R},\log k+1} \cdot \beta = \gamma_{\log k}$. If $r < \log k$, then the prover's second message in Π_r is a sum of 2^{r+1} terms, each term being a product of $r+1$ challenges and a subvector of $\mathbf{x}^{(0)}$. The norm of this message is thus upper bounded by $2^{r+1} \cdot \gamma_{\mathcal{R},r+2} \cdot \beta = \gamma_r$.

The strengthened claim regarding power-of-2 cyclotomic rings follows from realising that each element in S_0 is either zero or a power of ζ, and that multiplication by ζ does not increase norm. ☐

Theorem 5. *Let $\mathcal{R}$ be a prime-power cyclotomic ring of order m being a power of a prime p. Let $S_0 \subseteq_n \mathcal{R}$ be an $(s, 3)$-subtractive set of size $n = \mathsf{poly}(\lambda)$ and $S_1 = \{1\}$. For $r \in \{0, \ldots, \log k\}$, let γ_r be defined as in Lemma 4. Suppose that S_0 is constructed from Theorem 1 or Theorem 2, then $\Pi_{\log k}$ has perfect knowledge soundness relative to $L_{s,\gamma'_{\log k}}$, and Π_r has $\frac{2(r+1)}{n}$-knowledge soundness relative to L_{s,γ'_r} for $r \in \mathbb{Z}_{\log k}$, where $\gamma'_{\log k} = \gamma'_{\log k-1}$, and*

$$\gamma'_r = \begin{cases} 24 \cdot \varphi(m) \cdot \gamma_{\mathcal{R}} \cdot \gamma_r & p > 2 \\ 3 \cdot \varphi(m) \cdot \gamma_{\mathcal{R}} \cdot \gamma_r & p = 2. \end{cases}$$

Proof. For $r = \log k$, there exists a trivial $(\log k)$-th extractor $\mathcal{E}_{\log k}$ which simply outputs the prover's message. If a prover $\mathcal{A}$ successfully convinces the verifier $\mathcal{V}$, then the prover's message is exactly the witness.

For $r \in \mathbb{Z}_{\log k}$, let $\mathcal{A}$ be a prover who successfully convinces the verifier $\mathcal{V}$ in Π_r to accept a statement $(\mathbf{A}, \mathbf{y})$ with probability $\rho > 2(r+1)/n$. Consider a binary matrix H with rows indexed by the random coins χ of $\mathcal{A}$, columns indexed by $c \in S_0$, and the (χ, c)-th entry is $\langle \mathcal{A}(\chi), \mathcal{V}(\mathsf{stmt}; c)\rangle$, i.e. whether $\mathcal{V}$ accepts of rejects when $\mathcal{A}$ runs on the randomness χ and $\mathcal{V}$ chooses $c \in S_0$ as the challenge. By our assumption on $\mathcal{A}$, a ρ-fraction of the entries of H are 1. Adopting the terminologies in [17], a row of H is semi-heavy if it contains at least three 1's. Since $\rho > 2(r+1)/n \geq 2/n$, write $\rho = (2+\delta)/n$ for some $\delta > 2r$. Suppose there are in total R rows in H, so that $\rho R n = (2+\delta)R$ entries are 1. At most $2R$ of them can be located in non-semi-heavy rows, while at least δR of them are in semi-heavy rows. Therefore the fraction of 1's in semi-heavy rows among all 1's is at least $\delta/(2+\delta)$.

With the above observation, we construct the r-th knowledge extractor $\mathcal{E} = \mathcal{E}_r$ as follows. $\mathcal{E}$ runs $\langle \mathcal{A}(\chi), \mathcal{V}(\mathsf{stmt}; c_0)\rangle$ for some uniformly chosen χ and $c_0 \leftarrow\!\!\$\, S_0$. If $\langle \mathcal{A}(\chi), \mathcal{V}(\mathsf{stmt}; c_0)\rangle = 0$, $\mathcal{E}$ aborts. Otherwise, we have $\langle \mathcal{A}(\chi), \mathcal{V}(\mathsf{stmt}; c_0)\rangle = 1$, which happens with probability ρ. Then, $\mathcal{E}$ runs $\langle \mathcal{A}(\chi), \mathcal{V}(\mathsf{stmt}; c)\rangle$ for all $c \in S_0 \setminus \{c_0\}$. Note that this can be done in polynomial time since $n = \mathsf{poly}(\lambda)$. By the above observation about semi-heavy rows, since the (χ, c_0)-th entry of H is 1, with probability at least $\delta/(2+\delta)$, the row in H indexed by χ is a semi-heavy row, and in this case there are at least 2 more 1's in this row. Denote the indices of two of these entries by (χ, c_1) and (χ, c_2) respectivly. To summarise, with probability $\rho\delta/(2+\delta) = \delta/n > 2r/n \geq 0$, we have $\langle \mathcal{A}(\chi), \mathcal{V}(\mathsf{stmt}; c)\rangle = 1$ for $c \in \{c_0, c_1, c_2\}$.

Suppose the above event happens, $\mathcal{E}$ reads from the communication transcripts the responses $\tilde{\mathbf{x}}_i$ which satisfy

$$(c_i \mathbf{A}_0 + \mathbf{A}_1) \cdot \tilde{\mathbf{x}}_i = \mathbf{l} + c_i \mathbf{y} + c_i^2 \mathbf{r} \text{ and } \|\tilde{\mathbf{x}}_i\| \leq \gamma_r$$

for all $i \in \mathbb{Z}_3$. In matrix form, we can write

$$\mathbf{A} \cdot \begin{pmatrix} c_0\tilde{\mathbf{x}}_0 & c_1\tilde{\mathbf{x}}_1 & c_2\tilde{\mathbf{x}}_2 \\ \tilde{\mathbf{x}}_0 & \tilde{\mathbf{x}}_1 & \tilde{\mathbf{x}}_2 \end{pmatrix} = \begin{pmatrix} \mathbf{l} & \mathbf{y} & \mathbf{r} \end{pmatrix} \cdot V^{\mathsf{T}}_{\{c_0,c_1,c_2\}}$$

Let $\mathbf{w} = (0, 1, 0) \in \mathcal{R}^3$. By Proposition 6, the solution $\mathbf{z} = (z_0, z_1, z_2)$ to the equation $V^{\mathsf{T}}_{\{c_0,c_1,c_2\}} \cdot \mathbf{z} = s \cdot \mathbf{w}$ is given by

$$z_i = -\frac{s}{d_i} \sum_{j \in \mathbb{Z}_3 \setminus \{i\}} c_j$$

for $i \in \mathbb{Z}_3$. Define $\mathbf{x} = (\sum_{i=0}^{2} c_i\, z_i \cdot \tilde{\mathbf{x}}_i, \sum_{i=0}^{2} z_i \cdot \tilde{\mathbf{x}}_i)$. We have

$$\mathbf{A} \cdot \mathbf{x} = \mathbf{A} \cdot \begin{pmatrix} c_0\tilde{\mathbf{x}}_0 & c_1\tilde{\mathbf{x}}_1 & c_2\tilde{\mathbf{x}}_2 \\ \tilde{\mathbf{x}}_0 & \tilde{\mathbf{x}}_1 & \tilde{\mathbf{x}}_2 \end{pmatrix} \cdot \mathbf{z} = \begin{pmatrix} \mathbf{l} & \mathbf{y} & \mathbf{r} \end{pmatrix} \cdot V^{\mathsf{T}}_{\{c_0,c_1,c_2\}} \cdot \mathbf{z} = s \cdot \mathbf{y}.$$

Furthermore, we notice that $\mathbf{x}$ is a sum of 3 terms, each being a product of $c_i z_i$ and $\tilde{\mathbf{x}}_i$. Using Propositions 10 and 11 we have $\|c_i z_i\| \leq \varphi(m)$ and $8\varphi(m)$ respectively, and $\tilde{\mathbf{x}}_i$ of norm at most γ_r. The norm $\|\mathbf{x}\|$ therefore satisfies

$$\|\mathbf{x}\| \leq \begin{cases} 24 \cdot \varphi(m) \cdot \gamma_{\mathcal{R}} \cdot \gamma_r & p > 2 \\ 3 \cdot \varphi(m) \cdot \gamma_{\mathcal{R}} \cdot \gamma_r & p = 2 \end{cases} = \gamma_r'$$

Our r-th extractor $\mathcal{E}$ therefore outputs $\mathbf{x}$ as a witness of $(\mathbf{A}, \mathbf{y}) \in L_{s,\gamma_r'}$ with probability at least $\delta/n > 2r/n$. □

4.2 On the Knowledge Soundness of Recursive Composition

Knowledge error is at least $\Omega(\log k/n)$. In their original analysis, Bootle *et al.* [11] optimistically claimed without proof that the protocol Π obtained from the recursive composition of $\Pi_0, \ldots, \Pi_{\log k}$ has knowledge error $O(1/n)$. We disprove this by constructing a cheating prover who can convince the verifier in Π_r with probability at least $1/n$ for any statement $(\mathbf{A}, \mathbf{y})$. Consequently we obtain a cheating prover who can convince the verifier in Π with probability at least $1 - (1 - 1/n)^{\log k} \geq \frac{\log k}{2n} = \omega(1/n)$ assuming $n \geq \log k = \omega(1)$.

Our cheating prover $\mathcal{A}_r$ for Π_r is essentially a "zero-knowledge simulator" which does the following. Guess the challenge to be sent by the verifier as c^* uniformly at random. Sample an arbitrary vector $\tilde{\mathbf{x}} \in \mathcal{R}^{k_{r+1}}$ of norm at most γ_r. Compute $(\tilde{\mathbf{A}}, \tilde{\mathbf{y}})$ as an honest prover would. Pick an arbitrary vector $\mathbf{r} \in \mathcal{R}^h$. Compute $\mathbf{l} = \tilde{\mathbf{A}}\tilde{\mathbf{x}} - c\tilde{\mathbf{y}} - c^2\mathbf{r}$. Send $(\mathbf{l}, \mathbf{r})$ as the first message and receive a challenge

c. If $c \neq c^*$ then abort. Otherwise send $\tilde{\mathbf{x}}$ as the second message. Clearly $\mathcal{A}_r$ succeeds whenever $c = c^*$, which happens with probability at least $1/n$.

Now consider an adversary $\mathcal{A}$ against the verifier in Π. To cheat, it suffices for $\mathcal{A}$ to cheat in at least one round $r \in \mathbb{Z}_{\log k}$. The success probability of $\mathcal{A}$ is then at least $1 - (1 - 1/n)^{\log k} \geq 1 - \frac{1}{1+\log k/n} = \frac{\log k}{n+\log k} \geq \frac{\log k}{2n} = \omega(1/n)$, where we assumed $n \geq \log k = \omega(1)$. In general, if Π is obtained by recursively composing $\Pi_0, \ldots, \Pi_\ell$ for some $\ell \geq 0$, where in Π_ℓ the prover simply sends the witness, then $\mathcal{A}$ succeeds with probability at least $\Omega(\ell/n)$ which is $\omega(1/n)$ if the number of rounds ℓ is super-constant.

On achieving knowledge error $O(\log k/n)$. In the proof of Theorem 5, we showed that for $r \in \mathbb{Z}_{\log k}$ if $\mathcal{A}_r$ is a cheating prover in Π_r with success probability greater than $2(r+1)/n$, then our extractor $\mathcal{E}_r$ succeeds with probability greater than $2r/n$. This intuitively suggests that if $\mathcal{A}$ is a cheating prover in Π obtained by recursively composing $\Pi_0, \ldots, \Pi_{\log k}$ with success probability greater than $2\log k/n$, then by recursively running the extractors $\mathcal{E}_{\log k}, \ldots, \mathcal{E}_0$ one should construct an extractor $\mathcal{E}$ which succeeds with positive probability. In other words, the knowledge error of Π is intuitively at most $2\log k/n$. This does not contradict with the existence of the attacker $\mathcal{A}$ with success probability $1 - (1 - 1/n)^{\log k}$ constructed above, since by the union bound we have $1 - (1 - 1/n)^{\log k} \leq \sum_{r \in \mathbb{Z}_{\log k}} 1/n = \log k/n$. If the knowledge error is indeed at most $2\log k/n$, then repeating the protocol $\lambda/(\log n - \log\log k - 1)$ times (instead of $\lambda/\log n$ times suggested in [11]) suffices to achieve knowledge error $2^{-\lambda}$.

Formalising the above intuition requires a very strong "forking lemma" which extracts a full depth-$(\log k)$ ternary tree of accepting transcripts in expected polynomial time when given any cheating prover for Π with success probability greater than $2\log k/n$. Unfortunately, such a formalisation appears to be out of reach with the current proof techniques. Indeed, the forking lemma in [9, Lemma 1] (and its variants) used in subsequent works (e.g. [13,14]) implies a knowledge error of $n^{-1/3}k^{1.58}$. The concrete analysis in [24] implies a knowledge error of $5n^{-1/2}k^{1.58}\log k$. A common problem in these analyses is that the extractor being constructed runs the cheating prover with uniformly random challenges every time, without insisting that the challenges in each round are distinct. This incurs a substantial loss in extraction probability.

At the time of writing, the tightest bound that we are aware of is given in [19, Lemma 3.2], which implies a knowledge error of $\frac{\alpha^{\log k}}{\alpha-1}\frac{3}{n}$ for any $\alpha > \left(\frac{n}{n-3}\right)^2$. The minimum of the factor $\frac{\alpha^{\log k}}{\alpha-1}$ is $\left(1 + \frac{1}{\log k-1}\right)^{\log k} / \frac{1}{\log k-1} \leq e\log k$ attained when $\alpha = 1 + \frac{1}{\log k-1}$ and e is Euler's number. Let $n \geq 9\log k$.[10] We can check that the requirement $\alpha > \left(\frac{n}{n-3}\right)^2$ is fulfilled. We therefore obtain a knowledge error of $\frac{8.16\log k}{n}$ whenever $n \geq 9\log k$, which requires $\lambda/(\log n - \log\log k - 4)$ parallel repetitions to achieve a knowledge error of $2^{-\lambda}$.

[10] The requirement $n \geq 9\log k$ is realistic. Typically, we have $n \approx 1000$ and $\log k \ll 100$.

For a concrete feeling of the number of repetitions required, suppose we aim for around 2^{-80} knowledge error, choose a ring $\mathcal{R}$ of degree $\varphi(m) \approx 1024$, an $(s, 3)$-subtractive set of size $n \approx 2^{10}$, and $k = 2^{20}$, which encodes the assignment of the internal wires an arithmetic circuit of size 2^{30}. Then if we can achieve the (near optimal) knowledge error of $2 \log k/n$, only 20 repetitions are needed.[11] With the provable knowledge error of $8.16 \log k/n$ however, we need 50 repetitions.

4.3 On the Quality of the Extracted Witness

Suppose we are able to construct an extractor by using one of the forking lemmas, then due to the additional structural guarantee of the extracted solution, we can obtain a tighter upper bound of the norm of the extracted solution $\mathbf{x}$. Specifically, observe that by construction $\mathbf{x}$ is a sum of $3^{\log k}$ terms, each term being a product of $\log k$ terms of the form $c_i z_i$ and one more term of norm at most $\gamma'_{\log k}$.

For the prime-power case, recall that $\gamma'_{\log k} = k \cdot \gamma_{\mathcal{R},\log k+1} \cdot \beta$. From Proposition 11 we have $\|c_i z_i\| \leq 8m$ and a naive application would yield a factor of $(8m)^{\log k}$ in the bound of $\|\mathbf{x}\|$. We can obtain a slightly better bound by observing that a factor 2 in $8m$ is contributed by a multiplication by a power of ζ (cf. Proposition 11). If we collect all the $\log k$ powers of ζ and only multiply them in one shot, then $(8m)^{\log k}$ can be replaced by $2 \cdot (4m)^{\log k}$. We therefore obtain

$$\begin{aligned}
\|\mathbf{x}\| &\leq 3^{\log k} \cdot \gamma_{\mathcal{R},\log k+1} \cdot \left(2 \cdot (4m)^{\log k}\right) \cdot (k \cdot \gamma_{\mathcal{R},\log k+1} \cdot \beta) \\
&= 3^{\log k} \cdot \left(2\,(\log k + 1) \cdot \varphi(m)^{\log k}\right)^2 \cdot 2 \cdot (4m)^{\log k} \cdot k \cdot \beta \\
&= \tilde{O}(k^{3 \log m + 4.58}) \cdot \beta.
\end{aligned}$$

When when $p = \mathsf{poly}(\lambda)$, we can set $s = 1$ and choose a modulus

$$q = \tilde{O}(k^{3 \log m + 4.58}) \cdot \beta.$$

We remark that even with the more careful analysis, the factor $2 \cdot (4m)^{\log k}$ is still somewhat loose. If we instead use the empirical estimation in Proposition 11 that $\|c_i \cdot z_i\| \leq m$, we can set

$$q = O(\|\mathbf{x}\|) = \tilde{O}(k^{3 \log m + 2.58}) \cdot \beta.$$

For the power-of-2 case we recall that $\gamma'_{\log k} = k \cdot \beta$ and thus

$$\begin{aligned}
\|\mathbf{x}\| &\leq 3^{\log k} \cdot \gamma_{\mathcal{R},\log k+1} \cdot \varphi(m)^{\log k} \cdot (k \cdot \beta) \\
&= 3^{\log k} \cdot \varphi(m)^{2 \log k} \cdot k \cdot \beta \\
&= \tilde{O}(k^{2 \log m + 0.58}) \cdot \beta.
\end{aligned}$$

Since $s = 2$ for the power-of-2 case, we have a total slack of k after recursive composition. Therefore we can choose a modulus $q = \tilde{O}(k^{2 \log m + 1.58}) \cdot \beta$. For comparison, [11] give a bound of $\tilde{O}(k^{3 \log m + 4.5}) \cdot \beta$ which is larger by a factor of $\tilde{O}(k^{\log m + 3})$.

[11] A concurrent work [2] proves that the knowledge error of $\frac{2 \log k}{n}$ can be achieved.

Remark 5. We may ask if another factor of $\log k$ can be shaved off the exponent by a more careful analysis of products of the form $\prod_{0 \leq j < \log k} c_{i_j} \cdot z_{i_j}$. Experimenting with random products of this form in the power-of-2 case suggests the norm grows as $(m/4)^{2(\log k - 1)}$ in the worst case (over the choice of $c_{i_j} \cdot z_{i_j}$) which is comparable to our analytical bound. The same bound is also approached from above in the prime case as m grows. Using that these products are over randomness of the extractor, we may also consider the average case which empirically grows as $(m/4)^{\log k + o(\log k)}$. Based on this data, we speculate that $q = \tilde{O}(k^{\log m + O(1)}) \cdot \beta$ is attainable.

4.4 Impossibility

A wide class of proof systems has knowledge soundness relative to $(\mathcal{E}, L_{s,\beta})$, where $\mathcal{E}$ is a knowledge extractor conforming to the following pattern.

Definition 8 (Algebraic Extractors). *Let Π be a proof system conforming to Definition 3 with $g = 1$ (3-move). Let $\mathcal{E}$ be an extractor for $L_{s,\beta}$. We say $\mathcal{E}$ is 3-move degree-d algebraic if $\mathcal{E}^{\mathcal{P}}$ conforms to the following pattern:*

1. *$\mathcal{E}$ specifies a special monomial $M^* \in \mathcal{M}$, where $\mathcal{M}$ is the set of all f-variate degree-d homogenous monomials.*
2. *$\mathcal{E}$ runs $\mathcal{P}$ some number of times to generate t accepting transcripts for some $t \in \mathbb{N}$. In the k-th transcript, let the verifier challenges be $(c_{i,k})_{i \in \mathbb{Z}_f}$.*
3. *$\mathcal{E}$ finds coefficients $a_k \in \mathcal{R}$ for $k \in \mathbb{Z}_t$ such that*

$$\sum_{k \in \mathbb{Z}_t} a_k \cdot M(\mathbf{c}_k) = 0 \qquad \forall\ M \in \mathcal{M} \setminus \{M^*\},$$
$$\sum_{k \in \mathbb{Z}_t} a_k \cdot M^*(\mathbf{c}_k) = s.$$

4. *If $\mathcal{E}$ fails to find the coefficients a_k in the above step, it aborts.*

We justify the definition of algebraic extractors, focusing on 3-move 2-challenge protocols. One challenge protocols can be captured by setting $S_1 := \{1\}$.

We first consider a linear-size Schnorr-like proof system which is complete for $L_{1,\beta}$. Classically a knowledge extractor $\mathcal{E}$ for $L_{s,\beta'}$ for some (s, β') is of degree $d = 1$ and proceeds as follows: Suppose $\mathcal{P}$ is a convincing prover for the statement $(\mathbf{A}, \mathbf{y})$. The extractor $\mathcal{E}^{\mathcal{P}}$ collects from $t = 2$ correlated accepting transcripts an image $\tilde{\mathbf{y}}$ and two preimages $\hat{\mathbf{x}}_0$ and $\hat{\mathbf{x}}_1$, such that $\mathbf{A} \cdot \hat{\mathbf{x}}_0 = c_{1,0}\tilde{\mathbf{y}} + c_{0,0}\mathbf{y}$ and $\mathbf{A} \cdot \hat{\mathbf{x}}_1 = c_{1,1}\tilde{\mathbf{y}} + c_{0,1}\mathbf{y}$. Subtracting the two equations yields $\mathbf{A} \cdot (\hat{\mathbf{x}}_0 - \hat{\mathbf{x}}_1) = (c_{1,0} - c_{1,1}) \cdot \tilde{\mathbf{y}} + (c_{0,0} - c_{0,1}) \cdot \mathbf{y}$. The extractor $\mathcal{E}$ then attempts to solve the following system of linear equations

$$\begin{pmatrix} c_{1,0} & c_{1,1} \\ c_{0,0} & c_{0,1} \end{pmatrix} \mathbf{z} = s \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

for $\mathbf{z} = (z_0, z_1)$, and return $\mathbf{x} = z_0\hat{\mathbf{x}}_0 + z_1\hat{\mathbf{x}}_1$. The special monomial here is $M^*(\{(X_0, X_1)\}) = X_0$ for some formal variables X_i.

Next we observe that in the proof of knowledge soundness of the lattice Bulletproof protocol constructed in Section 4.1, the degree-2 knowledge extractor solves the following system of linear equations

$$\begin{pmatrix} c_{1,0}^2 & c_{1,1}^2 & c_{1,2}^2 \\ c_{0,0} \cdot c_{1,0} & c_{0,1} \cdot c_{1,1} & c_{0,2} \cdot c_{1,2} \\ c_{0,0}^2 & c_{0,1}^2 & c_{0,2}^2 \end{pmatrix} \mathbf{z} = s \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

for $\mathbf{z} = (z_0, z_1, z_2)$. The special monomial here is $M^*(\{(X_0, X_1)\}) = X_0 X_1$.

A degree-$2d$ example can be obtained by modifying the lattice Bulletproof protocol in Section 4.1, such that instead of "folding" $\mathbf{A}$ and $\mathbf{x}$ in halves when given challenges (c_0, c_1), we compute

$$\tilde{\mathbf{A}} \coloneqq \sum_{k=0}^{d} c_0^{d-k} \cdot c_1^k \cdot \mathbf{A}_k \qquad \text{and} \qquad \tilde{\mathbf{x}} \coloneqq \sum_{k=0}^{d} c_0^k \cdot c_1^{d-k} \cdot \mathbf{x}_k.$$

Let $M^*(\{(X_0, X_1)\}) = X_0^d \cdot X_1^d$ and notice that

$$\tilde{\mathbf{A}} \cdot \tilde{\mathbf{x}} \in M^*(\{(c_0, c_1)\}) \cdot \mathbf{y} + \langle \{M(\{(c_0, c_1)\}) : M \in \mathcal{M} \setminus \{M^*\}\} \rangle.$$

Remark 6. Both Definition 8 and our results below can be generalised to $g > 1$. However, we found no good candidate construction with more than three moves. Thus, to avoid preempting future generalisations we do not formalise it here.

The next technical lemma shows that the above extraction strategy forces $s \in \langle M^*(\mathbf{S}^*) - M^*(\mathbf{S}^*) \rangle \cdot \mathcal{I}^{-1}$ (a fractional ideal) for some ideal $\mathcal{I}$ and for $\mathbf{S}^* = \{(c_{0,k}, \ldots, c_{f-1,k})\}_{k \in \mathbb{Z}_t}$. Here and in what follows we extend the notation of $M^*(\cdot)$ to sets in the natural way, e.g. $M^*(X_0, X_1) = X_0 \cdot X_1$ is extended to $M^*(\{(X_0, X_1), (Y_0, Y_1)\}) = \{X_0 \cdot X_1, Y_0 \cdot Y_1\}$. To illustrate the lemma, consider the linear-size Schnorr proof with $S_1 = \{1\}$ as an example. Here the lemma states that $s \in \langle c_{0,0} - c_{0,1} \rangle$. Similarly, for the lattice Bulletproof the lemma states that $s \in \left\langle \{c_{i,0} \cdot c_{i,1} - c_{j,0} \cdot c_{j,1}\}_{i \neq j} \right\rangle$ when $\langle \{c_{i,0}^2\}, \{c_{j,0}^2\} \rangle = \mathcal{R}$ for $i, j \in \mathbb{Z}_3$.

Lemma 5. *Let $d, f, t \in \mathbb{N}$, $a_k, c_{i,k} \in \mathcal{R}$ for $i \in \mathbb{Z}_f$ and $k \in \mathbb{Z}_t$. For $i \in \mathbb{Z}_f$, write $S_i^* \coloneqq \{c_{i,k} : k \in \mathbb{Z}_t\}$, $\mathbf{S}^* = \prod_{i \in \mathbb{Z}_f} S_i^*$. For $k \in \mathbb{Z}_t$, write $\mathbf{c}_k = (c_{0,k}, \ldots, c_{f-1,k}) \in \mathbf{S}^*$. Let $\mathcal{M}$ be the set of f-variate degree-d homogeneous monomials. Fix $M^* \in \mathcal{M}$. For $M \in \mathcal{M} \setminus \{M^*\}$, let $\bar{M} \coloneqq M / \gcd(M, M^*)$. Suppose*

$$U \coloneqq \{(M, j) : M \in \mathcal{M} \setminus \{M^*\}, M(\mathbf{c}_j) \neq 0, j \in \mathbb{Z}_t\} \neq \emptyset.$$

Let $\mathcal{I} \coloneqq \bigcap_{(M,j) \in U} \langle \bar{M}(\mathbf{c}_j) \rangle$. If $\sum_{k \in \mathbb{Z}_t} a_k \cdot M(\mathbf{c}_k) = 0$ for all $M \in \mathcal{M} \setminus \{M^*\}$ then

$$s \coloneqq \sum_{k \in \mathbb{Z}_t} a_k \cdot M^*(\mathbf{c}_k) \in \langle M^*(\mathbf{S}^*) - M^*(\mathbf{S}^*) \rangle \cdot \mathcal{I}^{-1}$$

the latter being a fractional ideal in the field of fractions K of $\mathcal{R}$.

Proof. For any $(M, j) \in U$, we have $a_j = -\sum_{k \in \mathbb{Z}_t \setminus \{j\}} a_k \frac{M(\mathbf{c}_k)}{M(\mathbf{c}_j)} \in K$. Extending the given notation, let $\hat{M}^* = M^* / \gcd(M, M^*)$ (dependent on M). We obtain

$$\begin{aligned} s = \sum_{k \in \mathbb{Z}_t} a_k M^*(\mathbf{c}_k) &= \sum_{k \in \mathbb{Z}_t \setminus \{j\}} a_k M^*(\mathbf{c}_k) + a_j M^*(\mathbf{c}_j) \\ &= \sum_{k \in \mathbb{Z}_t \setminus \{j\}} a_k M^*(\mathbf{c}_k) - \left(\sum_{k \in \mathbb{Z}_t \setminus \{j\}} a_k \frac{M(\mathbf{c}_k)}{M(\mathbf{c}_j)} \right) M^*(\mathbf{c}_j) \\ &= \sum_{k \in \mathbb{Z}_t \setminus \{j\}} a_k \left(M^*(\mathbf{c}_k) M(\mathbf{c}_j) - M(\mathbf{c}_k) M^*(\mathbf{c}_j) \right) / M(\mathbf{c}_j) \\ &= \sum_{k \in \mathbb{Z}_t \setminus \{j\}} a_k \left(M^*(\mathbf{c}_k) \bar{M}(\mathbf{c}_j) - M(\mathbf{c}_k) \hat{M}^*(\mathbf{c}_j) \right) / \bar{M}(\mathbf{c}_j) \\ &\in \frac{1}{\bar{M}(\mathbf{c}_j)} \left\langle M(\mathbf{S}^*) \hat{M}^*(\mathbf{S}^*) - M^*(\mathbf{S}^*) \bar{M}(\mathbf{S}^*) \right\rangle \\ &= \frac{1}{\bar{M}(\mathbf{c}_j)} \langle \bar{M}(\mathbf{S}^*) M^*(\mathbf{S}^*) - \bar{M}(\mathbf{S}^*) M^*(\mathbf{S}^*) \rangle \\ &\subseteq \frac{1}{\bar{M}(\mathbf{c}_j)} \langle M^*(\mathbf{S}^*) - M^*(\mathbf{S}^*) \rangle. \end{aligned}$$

We conclude that

$$s \in \bigcap_{(M,j) \in U} \frac{1}{\bar{M}(\mathbf{c}_j)} \langle M^*(\mathbf{S}^*) - M^*(\mathbf{S}^*) \rangle = \langle M^*(\mathbf{S}^*) - M^*(\mathbf{S}^*) \rangle \cdot \mathcal{I}^{-1}.$$

□

We can now state the main result of this section which rules out algebraic extractors achieving inverse polynomial soundness error and small slack. We state our impossibility for 3-move protocols for simplicity. However, as mentioned above, the ideas in the proof generalise to arbitrary moves. At a high level, our proof strategy is to construct an adversary that only answers challenges such that all accepting transcripts land in the same coset $\mathfrak{c}$ of some ideal $\mathfrak{q}$ chosen by the adversary, i.e. $\mathfrak{c} \equiv c_{i,k} \bmod \mathfrak{q}$. Then, e.g. for linear-size Schnorr proofs $c_{0,0} - c_{0,1} \in \mathfrak{q}$ which implies $s \in \mathfrak{q}$ by Lemma 5.

Theorem 6. *Let $\mathcal{R}$ be a cyclotomic ring. Let $\mathfrak{q} \subseteq \mathcal{R}$ be a prime ideal of norm $N(\mathfrak{q}) = |\mathcal{R}/\mathfrak{q}| = q$. Let Π be an f-challenge 3-move public-coin proof system, where $S_i \setminus \{0\} \neq \emptyset$ for $i \in \mathbb{Z}_f$, and $\prod_{i \in \mathbb{Z}_f} |S_i| = \prod_{i \in \mathbb{Z}_f} n_i \geq q^f$. Let $\mathcal{E}$ be a degree-d algebraic extractor for $L_{s,\beta}$. Let $\kappa < q^{-f}/2$. Suppose Π has κ-knowledge soundness relative to $(\mathcal{E}, L_{s,\beta})$ for some $\beta \in \mathbb{R}$, then $s \in \mathfrak{q}^{d-1}$.*

Proof. Let $\kappa = q^{-f}/2 - \epsilon$ for some $\epsilon > 0$. Suppose the claim is false, then $s \notin \mathfrak{q}^{d-1}$.

Let M^* be the special monomial specified by $\mathcal{E}$. Pick any $i^* \in \mathbb{Z}_f$ such that $M^*(\mathbf{C}) \neq C_{i^*}^d$. Let $S_{i^*}^* \subseteq S_{i^*} \setminus \{0\}$ be a largest subset so that all elements belong to the same coset modulo $\mathfrak{q}$. For each $i \in \mathbb{Z}_f \setminus \{i^*\}$, let $S_i^* \subseteq S_i$ be a largest subset so that all elements belong to the same coset modulo $\mathfrak{q}$. We note that by construction S_i^* has the property that $S_i^* - S_i^* \subseteq \mathfrak{q}$ for all $i \in \mathbb{Z}_f$, and $S_{i^*}^*$ contains only non-zero elements. Since $\mathfrak{q}$ has q cosets, by the pigeonhole principle, $|S_i^*| \geq \lceil n_i/q \rceil$ for all $i \in \mathbb{Z}_f \setminus \{i^*\}$. For $i = i^*$, if S_{i^*} contains only non-zero elements, then $|S_{i^*}^*| \geq \lceil n_{i^*}/q \rceil$. Otherwise $|S_{i^*}^*| \geq \lceil (n_{i^*} - 1)/q \rceil$.

We construct an adversary $\mathcal{A}$. This adversary $\mathcal{A}$ behaves almost exactly like the honest prover $\mathcal{P}$, except that it insists on answering only those challenges coming from $\mathbf{S}^* := \prod_{i \in \mathbb{Z}_f} S_i^*$. If $\mathcal{A}$ is challenged with any other values, it aborts. If S_{i^*} contains only non-zero elements, then $\mathcal{A}$ successfully convinces the honest verifier $\mathcal{V}$ with probability $\rho = \prod_{i \in \mathbb{Z}_f} \lceil n_i/q \rceil / n_i \geq q^{-f} > q^{-f}/2 - \epsilon = \kappa$. Otherwise, by noting that $n_{i^*} > 1$ since S_{i^*} contains at least one non-zero element, we have $\rho = (\lceil (n_{i^*} - 1)/q \rceil / n_{i^*}) \prod_{i \in \mathbb{Z}_f \setminus \{i^*\}} (\lceil n_i/q \rceil / n_i) \geq q^{-1}(1 - 1/n_{i^*}) q^{-(f-1)} \geq q^{-f}/2 > q^{-f}/2 - \epsilon = \kappa$.

On the other hand, we see that for any algebraic extractor $\mathcal{E}$, $\mathcal{E}^{\mathcal{A}}$ fails to find algebraic combinations of differences of challenges to produce s. To see why, suppose that $\mathcal{E}$ does not abort according to Definition 8. Since $S_{i^*}^*$ is constructed such that $0 \notin S_{i^*}^*$ and $M^*(\mathbf{C}) \neq C_{i^*}^d$, the set U defined in the statement of Lemma 5 is non-empty. By Lemma 5, we have $s \in \langle M^*(\mathbf{C}) - M^*(\mathbf{C}) \rangle \cdot \mathcal{I}^{-1} \subseteq \mathfrak{q}^d \cdot \mathcal{I}^{-1}$. Since $\mathfrak{q}$ is prime, we either have $\mathfrak{q} = \mathcal{I}$, or $\mathfrak{q}$ and $\mathcal{I}$ are coprime. In the former case we have $s \in \mathfrak{q}^{d-1}$, and in the latter we have $s \in \mathfrak{q}^d \subseteq \mathfrak{q}^{d-1}$ since s is integral.

To conclude, $\mathcal{E}^{\mathcal{A}}$ always fails, which contradicts to the claim that $\mathit{\Pi}$ has κ-knowledge soundness relative to $(\mathcal{E}, L_{s,\beta})$ for some $\beta \in \mathbb{R}$. □

Remarks about the tightness of Theorem 6. The assumption that $\mathfrak{q}$ is prime is made without loss of generality: if $\mathfrak{q}$ is not prime then we can pick a prime factor of $\mathfrak{q}$. The assumption $\prod_{i \in \mathbb{Z}_f} |S_i| \geq q^f$ can typically be dropped if $\mathit{\Pi}$ admits a "zero-knowledge simulator" which simulates the prover's messages by guessing the challenge to be sent by the verifier, which can be done with probability at least q^{-f} if $\prod_{i \in \mathbb{Z}_f} |S_i| < q^f$.[12] The assumption $\kappa < q^{-f}/2$ (instead of $\kappa < q^{-f}$) is made to account for the unlikely scenario that the extractor $\mathcal{E}$ manages to collect challenge tuples which contain too many zeros. The conclusion $s \in \mathfrak{q}^{d-1}$ (instead of $s \in \mathfrak{q}^d$) is to account for the unlikely event that $\mathcal{I} \neq \mathcal{R}$.

For example, if there exists $i^* \in \mathbb{Z}_f$ such that $M^*(\mathbf{C}) \neq C_{i^*}^d$, $0 \notin S_{i^*}$, and $\mu \in S_{i^*}$ for some invertible element $\mu \in \mathcal{R}$ (e.g. $\mu = 1$), then we can assume $\kappa < q^{-f}$ instead and conclude that $s \in \mathfrak{q}^d$ using the same proof. In particular, with this additional (natural) assumption, if $s = 1$ and $\mathfrak{q} = \langle 1 - \zeta \rangle$ which has norm p, then $\mathit{\Pi}$ does not have κ-knowledge soundness relative to $(\mathcal{E}, L_{s,\beta})$ for any algebraic extractor $\mathcal{E}$, any $\beta \in \mathbb{R}$, any $\kappa < q^{-f}$, and any $f \in \mathbb{N}$.

By repeating f times a 1-challenge 3-move public-coin proof system with knowledge error p^{-1}, which can be constructed from a subtractive set of size p, such as the one constructed in Theorem 2, one can reduce the knowledge error to p^{-f} relative to an algebraic extractor. Therefore the bound $\kappa < p^{-f}$ in Theorem 6 is in a sense tight, assuming algebraic extractors.

[12] Although such a simulator usually exists naturally, it seems difficult to argue about its existence generically.

Acknowledgments

We thank Jonathan Bootle for comments on an earlier version of this work.

References

1. Abspoel, M., Cramer, R., Damgård, I., Escudero, D., Yuan, C.: Efficient information-theoretic secure multiparty computation over $\mathbb{Z}/p^k\mathbb{Z}$ via galois rings. In: Hofheinz, D., Rosen, A. (eds.) TCC 2019, Part I. LNCS, vol. 11891, pp. 471–501. Springer, Heidelberg (Dec 2019). 10.1007/978-3-030-36030-6_19 8
2. Attema1, T., Cramer, R., Kohl, L.: A compressed σ-protocol theory for lattices. Cryptology ePrint Archive, Report 2021/307 (2021), https://eprint.iacr.org/2021/307 8, 11
3. Baum, C., Bootle, J., Cerulli, A., del Pino, R., Groth, J., Lyubashevsky, V.: Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part II. LNCS, vol. 10992, pp. 669–699. Springer, Heidelberg (Aug 2018). 10.1007/978-3-319-96881-0_23 1, 1
4. Baum, C., Nof, A.: Concretely-efficient zero-knowledge arguments for arithmetic circuits and their application to lattice-based cryptography. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part I. LNCS, vol. 12110, pp. 495–526. Springer, Heidelberg (May 2020). 10.1007/978-3-030-45374-9_17 4
5. Ben-Sasson, E., Chiesa, A., Riabzev, M., Spooner, N., Virza, M., Ward, N.P.: Aurora: Transparent succinct arguments for R1CS. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part I. LNCS, vol. 11476, pp. 103–128. Springer, Heidelberg (May 2019). 10.1007/978-3-030-17653-2_4 1
6. Benhamouda, F., Camenisch, J., Krenn, S., Lyubashevsky, V., Neven, G.: Better zero-knowledge proofs for lattice encryption and their application to group signatures. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part I. LNCS, vol. 8873, pp. 551–572. Springer, Heidelberg (Dec 2014). 10.1007/978-3-662-45611-8_29 1, 3.1
7. Beullens, W.: Sigma protocols for MQ, PKP and SIS, and Fishy signature schemes. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part III. LNCS, vol. 12107, pp. 183–211. Springer, Heidelberg (May 2020). 10.1007/978-3-030-45727-3_7 1
8. Boneh, D., Lewi, K., Montgomery, H.W., Raghunathan, A.: Key homomorphic PRFs and their applications. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 410–428. Springer, Heidelberg (Aug 2013). 10.1007/978-3-642-40041-4_23 1, 3.1, 4
9. Bootle, J., Cerulli, A., Chaidos, P., Groth, J., Petit, C.: Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 327–357. Springer, Heidelberg (May 2016). 10.1007/978-3-662-49896-5_12 4.2
10. Bootle, J., Lyubashevsky, V., Nguyen, N.K., Seiler, G.: More efficient amortization of exact zero-knowledge proofs for LWE. Cryptology ePrint Archive, Report 2020/1449 (2020), https://eprint.iacr.org/2020/1449 5
11. Bootle, J., Lyubashevsky, V., Nguyen, N.K., Seiler, G.: A non-PCP approach to succinct quantum-safe zero-knowledge. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part II. LNCS, vol. 12171, pp. 441–469. Springer, Heidelberg (Aug 2020). 10.1007/978-3-030-56880-1_16 1, 1, 1, 1, 3.1, 1, 4.1, 4.2, 4.2, 4.3
12. Bootle, J., Lyubashevsky, V., Seiler, G.: Algebraic techniques for short(er) exact lattice-based zero-knowledge proofs. In: Boldyreva, A., Micciancio, D. (eds.)

CRYPTO 2019, Part I. LNCS, vol. 11692, pp. 176–202. Springer, Heidelberg (Aug 2019). 10.1007/978-3-030-26948-7_7 1
13. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G.: Bulletproofs: Short proofs for confidential transactions and more. In: 2018 IEEE Symposium on Security and Privacy. pp. 315–334. IEEE Computer Society Press (May 2018). 10.1109/SP.2018.00020 1, 4.2
14. Bünz, B., Fisch, B., Szepieniec, A.: Transparent SNARKs from DARK compilers. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 677–706. Springer, Heidelberg (May 2020). 10.1007/978-3-030-45721-1_24 4.2
15. Cohen, H.: A Course in Computational Algebraic Number Theory, vol. 138. Springer Science & Business Media (2013) 2.3
16. Dalskov, A.P.K., Lee, E., Soria-Vazquez, E.: Circuit amortization friendly encodingsand their application to statistically secure multiparty computation. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part III. LNCS, vol. 12493, pp. 213–243. Springer, Heidelberg (Dec 2020). 10.1007/978-3-030-64840-4_8 8
17. Damgård, I.: On σ-protocols. https://www.cs.au.dk/~ivan/Sigma.pdf (2010) 4.1
18. del Pino, R., Lyubashevsky, V., Seiler, G.: Lattice-based group signatures and zero-knowledge proofs of automorphism stability. In: Lie, D., Mannan, M., Backes, M., Wang, X. (eds.) ACM CCS 2018. pp. 574–591. ACM Press (Oct 2018). 10.1145/3243734.3243852 1
19. del Pino, R., Lyubashevsky, V., Seiler, G.: Short discrete log proofs for FHE and ring-LWE ciphertexts. In: Lin, D., Sako, K. (eds.) PKC 2019, Part I. LNCS, vol. 11442, pp. 344–373. Springer, Heidelberg (Apr 2019). 10.1007/978-3-030-17253-4_12 1, 4.2
20. Esgin, M.F., Nguyen, N.K., Seiler, G.: Practical exact proofs from lattices: New techniques to exploit fully-splitting rings. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 259–288. Springer, Heidelberg (Dec 2020). 10.1007/978-3-030-64834-3_9 1
21. Ganesh, C., Nitulescu, A., Soria-Vazquez, E.: Rinocchio: Snarks for ring arithmetic. Cryptology ePrint Archive, Report 2021/322 (2021), https://eprint.iacr.org/2021/322 8
22. Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J.H., Whyte, W.: NTRUSIGN: Digital signatures using the NTRU lattice. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 122–140. Springer, Heidelberg (Apr 2003). 10.1007/3-540-36563-X_9 3.3
23. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: ANTS. pp. 267–288 (1998) 1
24. Jaeger, J., Tessaro, S.: Expected-time cryptography: Generic techniques and applications to concrete soundness. In: Pass, R., Pietrzak, K. (eds.) TCC 2020, Part III. LNCS, vol. 12552, pp. 414–443. Springer, Heidelberg (Nov 2020). 10.1007/978-3-030-64381-2_15 4.2
25. Katz, J., Kolesnikov, V., Wang, X.: Improved non-interactive zero knowledge with applications to post-quantum signatures. In: Lie, D., Mannan, M., Backes, M., Wang, X. (eds.) ACM CCS 2018. pp. 525–537. ACM Press (Oct 2018). 10.1145/3243734.3243805 1
26. Kawachi, A., Tanaka, K., Xagawa, K.: Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 372–389. Springer, Heidelberg (Dec 2008). 10.1007/978-3-540-89255-7_23 1

27. Kilian, J.: A note on efficient zero-knowledge proofs and arguments (extended abstract). In: 24th ACM STOC. pp. 723–732. ACM Press (May 1992). 10.1145/129712.129782 1
28. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 1–31. Springer, Heidelberg (May 2016). 10.1007/978-3-662-49896-5_1 1
29. Ling, S., Nguyen, K., Stehlé, D., Wang, H.: Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 107–124. Springer, Heidelberg (Feb / Mar 2013). 10.1007/978-3-642-36362-7_8 1
30. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 738–755. Springer, Heidelberg (Apr 2012). 10.1007/978-3-642-29011-4_43 1
31. Lyubashevsky, V., Micciancio, D.: Generalized compact Knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006, Part II. LNCS, vol. 4052, pp. 144–155. Springer, Heidelberg (Jul 2006). 10.1007/11787006_13 2.2
32. Norton, G.H., Salagean-Mandache, A.: On the key equation over a commutative ring. Des. Codes Cryptogr. **20**(2), 125–141 (2000) 3, 8
33. Pornin, T., Prest, T.: More efficient algorithms for the NTRU key generation using the field norm. In: Lin, D., Sako, K. (eds.) PKC 2019, Part II. LNCS, vol. 11443, pp. 504–533. Springer, Heidelberg (Apr 2019). 10.1007/978-3-030-17259-6_17 3.3
34. Quintin, G., Barbier, M., Chabot, C.: On generalized reed-solomon codes over commutative and noncommutative rings. IEEE Trans. Inf. Theory **59**(9), 5882–5897 (2013). 10.1109/TIT.2013.2264797, https://doi.org/10.1109/TIT.2013.2264797 3
35. Stehlé, D., Steinfeld, R.: Making NTRUEncrypt and NTRUSign as secure as standard worst-case problems over ideal lattices. Cryptology ePrint Archive, Report 2013/004 (2013), https://eprint.iacr.org/2013/004 3.3
36. Stern, J.: A new identification scheme based on syndrome decoding. In: Stinson, D.R. (ed.) CRYPTO'93. LNCS, vol. 773, pp. 13–21. Springer, Heidelberg (Aug 1994). 10.1007/3-540-48329-2_2 1
37. Washington, L.C.: Introduction to cyclotomic fields, vol. 83. Springer Science & Business Media (1997) 2.1, 2.3
38. Yang, R., Au, M.H., Zhang, Z., Xu, Q., Yu, Z., Whyte, W.: Efficient lattice-based zero-knowledge arguments with standard soundness: Construction and applications. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part I. LNCS, vol. 11692, pp. 147–175. Springer, Heidelberg (Aug 2019). 10.1007/978-3-030-26948-7_6 1, 1