

Optimal Bucket Set Construction for Multi-scalar Multiplication with Endomorphisms

Nam Hoai Le¹  and Francesco Sica¹ 

Department of Mathematics and Statistics, Florida Atlantic University, Florida, USA
`{namle2024,sicaf}@fau.edu`

Abstract. We develop the method of Luo, Fu and Gong (LFG) – as extended by Fan, Kuchta, Sica and Xu (FKSX) to use endomorphism scalars – in order to find *best* families suitable for multi-scalar multiplication (MSM) for any number n of points and with adjustable storage. In particular we lower storage requirements by an average of 67% and decrease the number of curve operations by an average of 7% (and up to 10.6%), relative to the LFG method. Compared to Pippenger’s variant (standard when n is large), we manage to improve performance by an average 6% for an MSM with $n \in [2^{10}, 2^{21}]$, while at the same time decreasing storage by up to 15.8% using the BLS12-381 curve. We also improve the FKSX performance, due to a smaller bucket set, by around 7%. This is done by finding the optimal bucket set in the endomorphism case and by providing a fast algorithm to generate an associated Hamiltonian path with short edges.

The proposed method is suitable for immediate software deployment at all sizes where MSM is currently used commercially, such as for Zcash and blockchain. Code to generate all ordered bucket sets is provided in a repository.

Keywords: Multi-scalar multiplication · zk-SNARK · Pippenger’s bucket method · Elliptic curve endomorphisms.

1 Introduction

The protection of privacy is a central topic in cryptography. Among the methods to ensure privacy, a zero-knowledge succinct non-interactive argument of knowledge, known as zk-SNARK, provides a compact and elegant solution, with applications to electronic currencies such as Zcash [2] or smart contract verification over private inputs [6] in Ethereum. The most efficient zk-SNARKs currently rely on pairing-based cryptography [8,9]. In this situation, the implementation bottleneck for both proof generation and verification is the multi-scalar multiplication (MSM for short), described as follows.

Let E be an additive elliptic curve group with order r . The operation of MSM is the computation

$$S_{n,r} := a_1P_1 + \cdots + a_nP_n, \tag{1}$$

where $P_1, \dots, P_n$ are usually fixed (precomputed) points in E and the integer scalars $a_i \in [0, r)$.

Many methods have been proposed to accelerate MSM, especially when the number of fixed points P_i 's is large. Straus' method [15] uses precomputation tables to speed up MSM, but its storage cost grows exponentially. Pippenger's bucket method [12] and its variants addressed this issue and became the standard approach. Recently, Luo, Fu, and Gong (LFG) [10] proposed a framework in which the digits of a q -ary expansion are represented as products of multipliers and bucket elements. Their framework also uses an efficient subsum accumulation algorithm, whose cost depends on the size of the bucket set and on the maximum distance between consecutive bucket elements. Fan, Kuchta, Sica, and Xu (FKSX) [7, Section 5] later applied the LFG framework to elliptic curves with efficient endomorphisms, where the units in $\mathbb{Z}[\omega]$ can be applied on the fly. In this setting, the problem of optimizing the MSM algorithm becomes a geometric problem in the Eisenstein lattice: construct a small bucket set in $\mathbb{Z}[\omega]$ satisfying the required property (see Property 1), and order its elements as a Hamiltonian path with bounded distance. Moreover, FKSX constructed such a bucket set using a disk. This choice is well suited for building a Hamiltonian path, but it leaves room for reducing the bucket set size. However, an explicit efficient algorithm for ordering the bucket set is not provided.

Our contributions: In this paper, we develop an optimal hexagonal bucket set construction and provide an explicit ordering algorithm for our bucket set. Throughout the summary below, p denotes a prime in $\mathbb{Z}[\omega]$, $q = p^c$ for some positive integer c is the radix used for scalar recoding, M the multiplier set used for precomputation, and B the bucket set according to which the recoded points are grouped and accumulated. The related notation and LFG framework are reviewed in Section 2. Our main contributions are as follows.

1. *Optimal bucket set construction for efficient endomorphism.* The FKSX endomorphism method applied the LFG framework to the endomorphism setting with $M = \{1\}$, $p = 2 - \omega$, $q = p^c$, where the scalar recoding is formulated over $\mathbb{Z}[\omega]$. Their construction uses a disk in the Eisenstein lattice and produces a bucket set of size $\frac{7^c \pi}{9\sqrt{3}} + o(7^c)$, which is larger than the optimal lower bound. In this paper, we introduce a construction on a hexagon that yields an optimal bucket set of size $\frac{7^c + 5}{6}$ (See Table 1 and Theorem 1).
2. *A new algorithm for constructing Hamiltonian paths on bucket sets.* We design an explicit Hamiltonian path construction on our hexagonal bucket sets and prove a bound on the maximum distance between consecutive bucket elements (see Theorem 2). We further adapt the associated algorithms to the proposed hexagonal construction. Our construction is also fully algorithmic: we give explicit SageMath [16] implementations for ordering the bucket set for any exponent c and for different choices p so that $N(p) = \ell \equiv 1 \pmod{6}$ is a rational prime. The source code is available at

https://github.com/hoainam-le/msm_opt_buckets.

3. *A generalization of the larger multiplier set.* We generalize the construction beyond the case $M = \{1\}$ by considering different prime elements $p \in \mathbb{Z}[\omega]$

with $N(p) = \ell$, where $\ell \equiv 1 \pmod{6}$ is a rational prime. These different choices of p naturally lead to larger multiplier sets while preserving the same hexagonal bucket set structure, which shown in Theorem 3. In particular, the bucket set is still optimal, and the Hamiltonian path construction developed for $M = \{1\}$ can be reused without additional geometric complications.

We measure the running time in terms of elliptic curve group operations. Let A denote the cost of one point addition on E . For simplicity, we count a doubling as having the same cost as an addition. We denote by P the storage required for one point. Table 1 summarizes the cost of our construction compared with the previous methods.

Table 1. Comparison of different MSM methods

Method	Storage	Time complexity (Worst Case)
Pippenger [3,12]	$n \cdot P$	$h(n + 0.5q) \cdot A$
Pippenger variant [4]	$nh \cdot P$	$(nh + 0.5q) \cdot A$
LFG [10], $p = 2$	$3nh \cdot P$	$(nh + 0.21q) \cdot A$
Repaired LFG method [7], $p = 2$	$(3nh + n) \cdot P$	$(n(h + 1) + 0.21875q) \cdot A$
FKSX method [7] for a prime $p > 2$	$n(h + 1) M \cdot P$	$(n(h + 1) + q/(2 M) + p - 4) \cdot A$
FKSX endomorphisms method [7] for $p = 2 - \omega, M = \{1\}$	$nh \cdot P^\dagger$	$(nh + 0.2015 q ^2 + 81^*) \cdot A$
Our method for $p = 2 - \omega, M = \{1\}$	$nh \cdot P^\dagger$	$(nh + q ^2/6 + 81) \cdot A$
Our method for $ M > 1$	$n(h + 1) M \cdot P^\ddagger$	$(nh + q ^2/(6 M) + O(1)) \cdot A$

Here, $q = p^c$ for some c , h denotes the length of a scalar in its radix q representation, and $|q|^2$ denotes the squared modulus of $q \in \mathbb{Z}[\omega]$.

* updated from an incorrect number in [7, Table 1]. See Table 3.

† for $4 \leq c \leq 11, c \neq 7$; $n(h + 1) \cdot P$ when $c = 7$.

‡ This is the general worst-case complexity; (10) yields a sharper bound for specific parameters.

Paper Organization: The structure of this paper is as follows. Section 2 reviews previous methods for accelerating MSM and recalls the algebraic number theory background needed in this paper. In Section 3 we propose our approach for constructing optimal bucket sets in the case $M = \{1\}$. Then we present an implementable construction of Hamiltonian paths on the bucket set, together with detailed algorithms in Section 4. Next, in Section 5 we generalize the construction to larger multiplier sets with the unchanged optimal bucket set. Finally, Section 6 discusses the complexity of our method.

2 Preliminaries and Previous Work

In this section, we first review the Straus method, Pippenger’s bucket method, the LFG method, and the FKXS method. We then recall the basic algebraic notation and facts about $\mathbb{Z}[\omega]$ that will be used throughout the paper.

2.1 Straus Method

Let $q = 2^c$, where c is a small positive integer, and let $h = \lceil \log_q r \rceil = \lceil \log_2 r / c \rceil$. For each scalar a_i in (1), we chunk it into segments of length c .

$$a_i = a_{i,h-1} \| a_{i,h-2} \| \cdots \| a_{i,0} = \sum_{j=0}^{h-1} a_{i,j} q^j, \quad 0 \leq a_{i,j} < q.$$

The Straus method [15] precomputes all 2^{nc} points of the form

$$\sum_{i=1}^n b_i P_i, \quad 0 \leq b_i < q. \quad (2)$$

The online computation first retrieves the point

$$S_{n,q} = \sum_{i=1}^n a_{i,h-1} P_i$$

from the precomputation table. It then doubles this point c times and adds the precomputed point $\sum_{i=1}^n a_{i,h-2} P_i$, obtaining

$$S_{n,q^2} = \sum_{i=1}^n (a_{i,h-1} \| a_{i,h-2}) P_i$$

Repeating this process $h - 1$ times, we obtain

$$S_{n,q^h} = \sum_{i=1}^n (a_{i,h-1} \| a_{i,h-2} \| \cdots \| a_{i,0}) P_i = \sum_{i=1}^n a_i P_i.$$

2.2 Pippenger's Bucket Method

Pippenger's bucket method uses the same q -ary expansion of the scalars as in the Straus method, but avoids the exponential precomputation table (2).

For a fixed $j \in [0, h - 1]$, the main task is to compute

$$S_{n,2^c}^{(j)} = \sum_{i=1}^n a_{i,j} P_i, \quad \text{for } 0 \leq a_{i,j} \leq q - 1. \quad (3)$$

To compute (3), it first groups the n points P_i into $(q - 1)$ buckets according to their scalars. More precisely, define $S_k^{(j)} = \sum_{i \text{ s.t. } a_{i,j}=k} P_i$ for $1 \leq k < q$. Thus,

$$S_{n,2^c}^{(j)} = \sum_{i=1}^n a_{i,j} P_i = \sum_{k=1}^{q-1} k S_k^{(j)}.$$

Then it runs the Algorithm 1 to obtain $S_{n,2^c}^{(j)}$.

In the signed variant, one uses the fact that $-P$ can be obtained for free on an elliptic curve, so the bucket indices can be restricted to roughly $[0, q/2]$. This signed bucket viewpoint is the starting point for the LFG method below, where the full bucket set is replaced by a smaller structured bucket set.

Algorithm 1 Subsum accumulation algorithm I [10, Algorithm 1]

```

1: Input:  $S_1, S_2, \dots, S_m$ 
2: Output:  $\sum_{k=1}^m kS_k$ 
3: tmp = 0
4: tmp1 = 0
5: for  $i = m$  to 1 by  $-1$  do
6:   tmp = tmp +  $S_i$ 
7:   tmp1 = tmp1 + tmp
8: end for
9: return tmp1

```

2.3 Luo-Fu-Gong (LFG) MSM Method

The LFG method refines the signed Pippenger's idea by introducing a multiplier set M (a set of integers) and a bucket set B (a set of integers containing 0). Given the q -ary expansion

$$a_i = \sum_{j=0}^{h-1} a_{i,j} q^j,$$

the method is to rewrite each digit $a_{i,j}$ in the form

$$a_{i,j} = \epsilon_{i,j} m_{i,j} b_{i,j}, \text{ where } \epsilon_{i,j} \in \{\pm 1\}, m_{i,j} \in M, b_{i,j} \in B.$$

Then

$$S_{n,r} = \sum_{i=1}^n \left(\sum_{j=0}^{h-1} \epsilon_{i,j} m_{i,j} b_{i,j} q^j \right) P_i = \sum_{i=1}^n \sum_{j=0}^{h-1} b_{i,j} (\epsilon_{i,j} m_{i,j} q^j P_i).$$

Therefore, after precomputing $nh|M|$ points

$$\{mq^j P_i : 1 \leq i \leq n, 0 \leq j < h, m \in M\},$$

the MSM can be computed by sorting the precomputed points into buckets indexed by the elements of B .

For each $b \in B$, define the intermediate subsum

$$S_b = \sum_{\substack{0 \leq i \leq n, 0 \leq j < h-1 \\ \text{s.t. } b_{i,j} = b}} \epsilon_{i,j} m_{i,j} q^j P_i.$$

Then the remaining task is to compute $\sum_{b \in B} b S_b$.

If the elements of B are ordered as $0 = b_0 < b_1 < \dots < b_{|B|-1}$ and

$$d = \max_{1 \leq k < |B|} (b_k - b_{k-1}),$$

Algorithm 2 Subsum accumulation algorithm II [10, Algorithm 3]

```

1: Input:  $b_1, b_2, \dots, b_m, S_1, S_2, \dots, S_m$  where  $1 \leq b_1 < b_2 < \dots < b_m$ .
2: Output:  $S = \sum_{i=1}^m b_i S_i$ 
3: Define a length- $(d+1)$  array  $\text{tmp} = [0] \times (d+1)$ 
4: for  $i = m$  to 1 by  $-1$  do
5:    $\text{tmp}[0] = \text{tmp}[0] + S_i$ 
6:    $k = b_i - b_{i-1}$ 
7:   if  $k \geq 1$  then
8:      $\text{tmp}[k] = \text{tmp}[k] + \text{tmp}[0]$ 
9:   end if
10: end for
11: return  $1 \cdot \text{tmp}[1] + 2 \cdot \text{tmp}[2] + \dots + d \cdot \text{tmp}[d]$ 

```

then Algorithm 2 computes $\sum_{b \in B} b S_b$ using at most $(2(|B| - 1) + d - 3) \cdot A$. Hence the total cost of computing $S_{n,r}$ is at most

$$(nh + |B| + d - 4) \cdot A,$$

with $nh|M|$ precomputed points.

Therefore, to apply the LFG framework efficiently, one must balance the size of the multiplier set M , which affects the storage complexity, the size of the bucket set B , and the maximum neighboring difference d , which should be bounded, ideally $O(1)$.

2.4 Combining LFG framework with Endomorphisms

FKSX [7, Section 5] applied the LFG framework to elliptic curves with efficient endomorphisms. Many pairing-friendly curves over finite field $\mathbb{F}$ have j -invariant 0 and can be written in the form $y^2 = x^3 + b$, $b \in \mathbb{F}$. Such curves have an endomorphism of order 3, denoted by ω . Furthermore, applying ω or its powers to a point requires a negligible cost.

The corresponding endomorphism ring of these curves can be identified with the Eisenstein integer ring $\mathbb{Z}[\omega]$ where $\omega = \frac{-1+i\sqrt{3}}{2}$. Therefore, instead of using only the signs $\{\pm 1\}$, one may take advantage of the full unit group

$$U = \{\pm 1, \pm \omega, \pm \omega^2\}.$$

FKSX [7, Section 5] considered in particular the case $p = 2 - \omega$, $q = p^c$, $M = \{1\}$. They construct a bucket set satisfying

Property 1. For all $t \in \mathbb{Z}[\omega]$, there exists $\epsilon_t \in U, m_t \in M, b_t \in B$ such that

$$t \equiv \epsilon_t m_t b_t \pmod{q}.$$

From this viewpoint, the construction of bucket sets becomes a geometric problem in the Eisenstein lattice. One needs to construct a small bucket set $B \subset \mathbb{Z}[\omega]$ and also order the elements of B so that the consecutive differences remain small.

2.5 Algebraic Preliminaries in $\mathbb{Z}[\omega]$

Let $K = \mathbb{Q}(\omega)$ where $\omega = \frac{-1+\sqrt{-3}}{2}$ satisfies $\omega^2 + \omega + 1 = 0$. The ring of Eisenstein integers is the imaginary quadratic field $\mathbb{Z}[\omega] = \text{span}_{\mathbb{Z}}\{1, \omega\} \subset \mathbb{C}$. Specially, for each $z = a + b\omega \in \mathbb{Z}[\omega]$, its K -conjugate is the same as its complex conjugate $\bar{z} = a + b\omega^2$. So the norm of each $a + b\omega \in \mathbb{Z}[\omega]$ is

$$N(a + b\omega) = |a + b\omega|^2 = a^2 - ab + b^2.$$

Moreover, $(\mathbb{Z}[\omega])^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ contains precisely 6 the elements of norm 1, called units. Multiplication by a unit preserves the norm and it acts geometrically on the Eisenstein lattice as a rotation by a multiple of $\pi/3$.

Also recall that the rational prime $\ell \in \mathbb{Z}$ is called *ramified* if $\ell\mathbb{Z}[\omega] = \mathfrak{p}^2$, *splits* if $\ell\mathbb{Z}[\omega] = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$, *inert* when $\ell\mathbb{Z}[\omega]$ remains a prime ideal. We can easily prove the lemma as follows.

Lemma 1. *Let $\ell \in \mathbb{Z}$ be a rational prime. Then ℓ splits in $\mathbb{Z}[\omega]$ if and only if $\ell \equiv 1 \pmod{3}$. In this case, there exist $a, b \in \mathbb{Z}$ such that $\ell = a^2 - ab + b^2$. Hence $p := a + b\omega$ is a prime element in $\mathbb{Z}[\omega]$ with $N(p) = \ell$. Moreover, ℓ is inert in $\mathbb{Z}[\omega]$ if and only if $\ell \equiv 2 \pmod{3}$, and ramified if and only if $\ell = 3$.*

Proof. See Appendix A □

Furthermore, $\mathbb{Z}[\omega]$ is norm-Euclidean by [14, Theorem 4.19] then it is a PID. So, by Lemma 1, for every rational prime $\ell \equiv 1 \pmod{3}$, one has $\ell\mathbb{Z}[\omega] = \mathfrak{p}_1\mathfrak{p}_2$. We choose a prime p so that $\mathfrak{p} = (p)$, one obtains $\ell = p\bar{p} = N(p)$. The choice of p is unique up to multiplication by a unit.

3 Optimal Bucket Sets for Efficient MSM Endomorphisms when $M = \{1\}$

In this section, we develop the hexagonal viewpoint underlying our construction. We begin by introducing hexagons in the Eisenstein lattice and establishing several structural properties that will be used in later sections. We then prove the main theorem describing the optimal bucket set in the sense that its size attains the smallest possible lower bound. First, we also have the argument about lower bound of the bucket set size, which is an analog of [7, Theorem 1].

Proposition 1. *If Property 1 holds, then*

$$6 \cdot |B| \cdot |M| \geq N(q).$$

Proof. This is because the right-hand side is the number of complete set of representatives modulo q , whereas the left-hand side is the number of integers $t \in \mathbb{Z}[\omega]$ of the form ϵmb where $\epsilon \in U, m \in M, b \in B$. □

3.1 Hexagons in $\mathbb{Z}[\omega]$

We now define the hexagon associated with an element $q \in \mathbb{Z}[\omega]$. We denote the principal ideal (sublattice) generated by an element $q \in \mathbb{Z}[\omega]$ by

$$q\mathbb{Z}[\omega] = \{qx : x \in \mathbb{Z}[\omega]\}.$$

Definition 1. Let q be an arbitrary element of $\mathbb{Z}[\omega]$. We define

$$\mathcal{H}_q := \{z \in \mathbb{C} : |z| \leq |z - x|, \forall x \in q\mathbb{Z}[\omega]\}$$

is the set of points at least close to the origin as to any other lattice point in sublattice $q\mathbb{Z}[\omega]$.

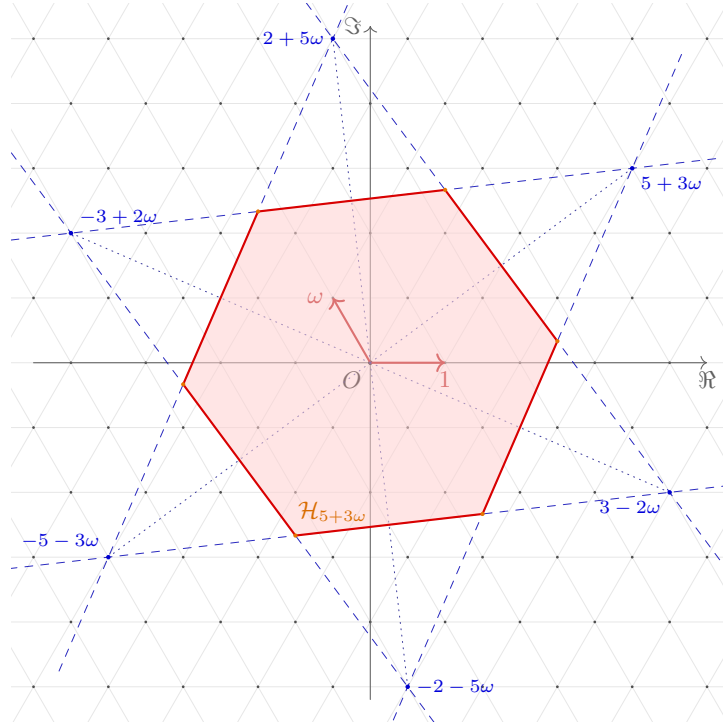


Fig. 1. Hexagon $\mathcal{H}_q$ for $q = 5 + 3\omega$

According to this definition, it is clear that the boundary of $\mathcal{H}_q$ consists of the perpendicular bisectors of the segments joining 0 to its nearest neighbors $qU = \{\pm q, \pm q\omega, \pm q\omega^2\}$. We illustrate it for the example $q = 5 + 3\omega$ in Figure 1.

Moreover, it is obvious that

$$\begin{aligned}
 \mathcal{H}_q &= \{z \in \mathbb{C} : |z| \leq |z - x|, \forall x \in q\mathbb{Z}[\omega]\} \\
 &= \bigcap_{w \in qU} \{z \in \mathbb{C} : |z| \leq |z - w|\} \\
 &= \mathcal{H}_{qu}, \forall u \in U.
 \end{aligned}$$

In particular, when q is a unit, one has

$$\mathcal{H}_1 = \{z \in \mathbb{C} : |z| \leq |z - u|, \forall u \in U\}. \quad (4)$$

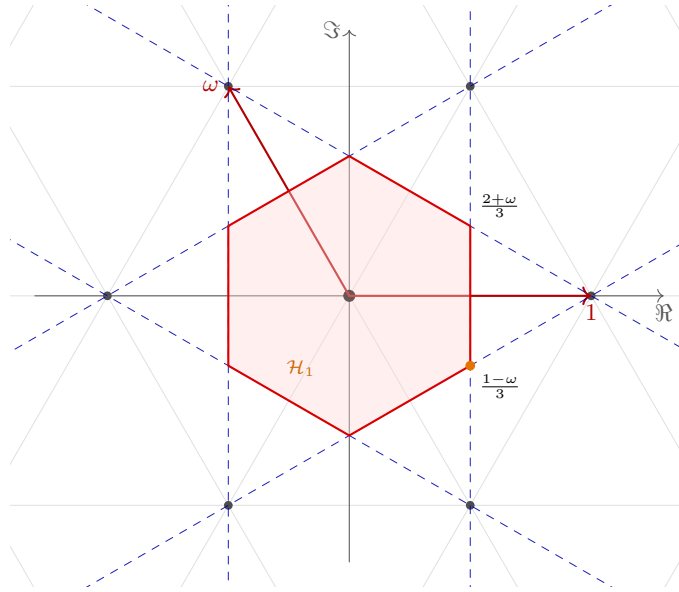


Fig. 2. $\mathcal{H}_1$ with vertices $\frac{1-\omega}{3}$ and its associates

Therefore, as shown in Figure 2, $\mathcal{H}_1$ is a regular hexagon in $\mathbb{Z}[\omega]$ at center 0 with circumradius $\frac{1}{\sqrt{3}}$ and inradius $\frac{1}{2}$. We have the important lemma as follows.

Lemma 2. *For every $z = m + ni \in \mathbb{C}$, there exists $\kappa = a + b\omega \in \mathbb{Z}[\omega]$ such that $z - \kappa \in \mathcal{H}_1$.*

Proof. We rewrite z in the basis $\{1, \omega\}$ as follows

$$z = m + ni = m + \frac{n}{\sqrt{3}} + \frac{2}{\sqrt{3}}n\omega.$$

Choose $a = \left\lfloor m + \frac{n}{\sqrt{3}} \right\rfloor$, $b = \left\lfloor \frac{2}{\sqrt{3}}n \right\rfloor$ where $\lfloor x \rfloor := \lfloor x + 1/2 \rfloor$ denote the nearest integer to x . Consider $r = a + b\omega \in \mathbb{Z}[\omega]$, one has

$$z - r = \left(m + \frac{n}{\sqrt{3}} - \left\lfloor m + \frac{n}{\sqrt{3}} \right\rfloor \right) + \left(\frac{2}{\sqrt{3}}n - \left\lfloor \frac{2}{\sqrt{3}}n \right\rfloor \right) \omega$$

Therefore, $z - r \in \mathcal{P} = \{u + v\omega : u, v \in [-\frac{1}{2}, \frac{1}{2}]\}$. Furthermore, it is clear to see in the Figure 3 that every point of $\mathcal{P}$ lies on one of $\mathcal{H}_1$ or $\mathcal{H}_1 + u$ for some $u \in U$. Thus, among 7 possibilities

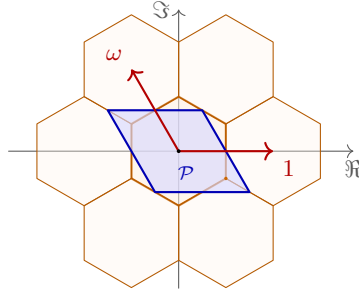


Fig. 3. $\mathcal{P}$ is covered by the union $\bigcup_{u \in U \cup \{0\}} \mathcal{H}_1 + u$

$$a + b\omega, (a \pm 1) + b\omega, a + (b \pm 1)\omega, (a - 1) + (b - 1)\omega, (a + 1) + (b + 1)\omega,$$

we obtain at least one κ such that $z - \kappa \in \mathcal{H}_1$ by checking the conditions in (4). $\square$

We collect the basic properties of $\mathcal{H}_q$ in the following proposition.

Proposition 2. *For any $q \in \mathbb{Z}[\omega]$, we have the following.*

- (i) $\mathcal{H}_q = q\mathcal{H}_1$.
- (ii) Each vertex of $\mathcal{H}_q$ is a center of a unit equilateral triangle in $\mathbb{Z}[\omega]$ if and only if $(1 - \omega) \nmid q$.
- (iii) Let $q = a + b\omega$. The boundary of $\mathcal{H}_q$ contains no lattice points if and only if

$$\gcd(2a - b, a - 2b) = 1.$$

Proof. See Appendix A. $\square$

Remark 1. (a) From Proposition 2 (i), one obtains $\mathcal{H}_q$ is a regular hexagon at center 0 with circumradius $\frac{|q|}{\sqrt{3}}$ and inradius $\frac{|q|}{2}$.

- (b) With $\mathcal{C}$ described in the proof of Proposition 2 (ii), the set $\frac{1-\omega}{3} + \mathbb{Z}[\omega]$ contains the centers of downward-pointing triangles, whereas $\frac{2+\omega}{3} + \mathbb{Z}[\omega]$ consists of the centers of upward-pointing ones.
- (c) It is more convenient to modify the condition in the Proposition 2 (iii) that

$$\begin{aligned} \gcd(2a - b, a - 2b) = 1 &\iff \gcd(a, b) = 1 \text{ and } a + b \not\equiv 0 \pmod{3} \\ &\iff \gcd(a, b) = 1 \text{ and } (1 - \omega) \nmid q. \end{aligned}$$

We verify this equivalence in Appendix A.

3.2 Reconstructing the Implementation Framework

We now turn to the implementation framework. Using the hexagonal description established above, we revisit the construction of [7, Section 5]. We work in the case $M = \{1\}$ and let $p = 2 - \omega \in \mathbb{Z}[\omega]$ be a prime element of norm $N(p) = 7$. In addition, for some integer $c \geq 2$, let $q = p^c$ then $N(q) = 7^c$.

The following lemma shows that the conditions in Proposition 2 (ii), (iii) hold for $q = p^c$ in our construction.

Lemma 3. *Let $\ell \equiv 1 \pmod{3}$ be a rational prime, and let $p \in \mathbb{Z}[\omega]$ be a prime so that $\ell = up\bar{p}$ for some $u \in U$, where $\bar{p}$ denoted by the complex conjugate of p . If $q = p^c = a + b\omega$ for some $c \geq 1$, then*

$$\gcd(a, b) = 1 \text{ and } (1 - \omega) \nmid q.$$

Proof. See Appendix A. □

The next corollary provides the key step in proving the main theorem.

Corollary 1. *For all $t \in \mathbb{Z}[\omega]$, there exists $\kappa \in \mathbb{Z}[\omega]$ such that*

$$r := t - q\kappa \in \mathcal{H}_q$$

Furthermore, every class in $\mathbb{Z}[\omega]/(q)$ has a unique representative in $\mathcal{H}_q$.

Proof. Consider $z = t/q \in \mathbb{C}$. By Lemma 2, there exists $\kappa \in \mathbb{Z}[\omega]$ such that $z - \kappa \in \mathcal{H}_1$. Therefore, we obtain $q(z - \kappa) \in q\mathcal{H}_1$. It implies that $r := t - q\kappa \in \mathcal{H}_q$ by Proposition 2 (i).

Moreover, assume that we have $t, r \in \mathcal{H}_q$ such that $t \equiv r \pmod{q}$. Then there exists $\kappa \in \mathbb{Z}[\omega]$ such that $t - r = \kappa q$. Note that the difference of any two elements of $\mathcal{H}_q$ has the magnitude at most $\frac{2|q|}{\sqrt{3}}$ as the circumradius of $\mathcal{H}_q$ is $\frac{|q|}{\sqrt{3}}$. Since $t - r \in \mathcal{H}_q$, then

$$|\kappa||q| = |t - r| \leq \frac{2|q|}{\sqrt{3}} \implies |N(\kappa)| = |\kappa|^2 \leq \frac{4}{3}.$$

It implies that $N(\kappa) \in \{-1, 0, 1\}$, then κ is either a unit or zero. If κ is a unit, then $t - r = uq$ for some $u \in U$. Thus, $t - r$ is among 6 directions of q , so t and r must be on the boundary of $\mathcal{H}_q$. However, in our setting $N(p) = 7 \equiv 1 \pmod{3}$, for any $c \geq 1$, $q = p^c$, we use Lemma 3 and Proposition 2 (iii) to imply that the boundary of $\mathcal{H}_q$ cannot contain t and r . Hence, $\kappa = 0$, which means $t = r$.

In other words, every class in $\mathbb{Z}[\omega]/(q)$ has a unique representative in $\mathcal{H}_q$. □

We define the hexagon

$$\mathcal{H}_q^+ := 1 + \mathcal{H}_q$$

by shifting $\mathcal{H}_q$ one unit to the right. It makes sense to obtain the next lemma.

Lemma 4. *Every class of $\mathbb{Z}[\omega]/(q)$ has a unique representative in $\mathcal{H}_q^+$.*

Proof. Let $t \in \mathbb{Z}[\omega]$. By Corollary 1 applied to $t - 1$, there exists $\kappa \in \mathbb{Z}[\omega]$ such that $r_0 := (t - 1) - q\kappa \in \mathcal{H}_q$. Set $r := r_0 + 1$. Then $r \in 1 + \mathcal{H}_q = \mathcal{H}_q^+$ and $t - r = t - (t - 1 - q\kappa + 1) = q\kappa \in (q)$. Hence $r \equiv t \pmod{q}$. $\square$

We now establish the main result of this section. In [7, Theorem 5], the bucket set is constructed using a disk. However, the disk approach may contain more than one representative of the same residue class modulo q , which results in a bucket set larger than necessary. Here, instead, we recover the bucket set from the hexagon $\mathcal{H}_q^+$, which gives a unique representative for each residue class modulo q (by Lemma 4). Consequently, this yields a bucket set of size $\frac{7^c}{6} + \frac{5}{6}$, improving the previous size $\frac{7^c\pi}{9\sqrt{3}} + o(7^c)$. Moreover, by Proposition 1, this value is the smallest possible, so the resulting bucket set is optimal.

Theorem 1. *For every $c \in \mathbb{Z}_{>}$, Property 1 holds for $q = p^c$, $M = \{1\}$ and the bucket set*

$$B = \{0\} \cup \bigcup_{k=0}^{c-1} B_k$$

where

$$B_k = \{b \in \mathcal{H}_q^+ \cap \mathbb{Z}[\omega] : b = p^k\beta \text{ and } \beta \equiv 1 \pmod{p}\}.$$

Furthermore, the size of the bucket set is

$$|B| = \frac{7^c}{6} + \frac{5}{6}.$$

Proof. Although the argument closely follows that of [7, Theorem 5], we will present the proof here because the notations introduced along the way will be used repeatedly in the later sections.

For any $t \in \mathbb{Z}[\omega]$, we obtain $t = p^k\alpha$ where $p \nmid \alpha$ and $k = v_p(t)$. If $k \geq c$, then $t \equiv 0 \pmod{p^c}$ and we take $b = 0 \in B$. Assume $k < c$. Since $p \nmid \alpha$ and $(\mathbb{Z}[\omega]/(p))^\times = U$, there exists a unique $\epsilon \in U$ such that $\alpha \equiv \epsilon \pmod{p}$. Set $\beta' := \epsilon^{-1}\alpha$, so $\beta' \equiv 1 \pmod{p}$.

We consider the class of $p^k\beta'$ modulo $q = p^c$. By Lemma 4, there exists $b \in \mathcal{H}_q^+ \cap \mathbb{Z}[\omega]$ such that $p^k\beta' \equiv b \pmod{q}$, so $b = p^k\beta$ for some $\beta \in \mathbb{Z}[\omega]$, thus $\beta' \equiv \beta \pmod{p^{c-k}}$, then $\beta \equiv \beta' \equiv 1 \pmod{p}$. Then $b \in B_k \subset B$ by construction, and

$$t = p^k\alpha = p^k\epsilon\beta' \equiv \epsilon p^k\beta = \epsilon b \pmod{q}.$$

Now we compute the size of each B_k . We have

$$\begin{aligned} B_k &= \{b = p^k \beta \in \mathcal{H}_q^+ \cap \mathbb{Z}[\omega] : \beta \equiv 1 \pmod{p}\} \\ &= \{p^k(1 + p\kappa) \in \mathcal{H}_q^+ \cap \mathbb{Z}[\omega], \kappa \in \mathbb{Z}[\omega]\} \\ &= p^k(1 + pB'_k), \end{aligned}$$

where $B'_k = \left\{ \kappa \in \mathbb{Z}[\omega] : \kappa \in \mathcal{H}_{p^{c-k-1}} + \frac{1}{p^{k+1}} - \frac{1}{p} \right\}.$

Furthermore, by Corollary 1 each $\mathcal{H}_{p^{c-k-1}} \cap \mathbb{Z}[\omega]$ is a complete set of representatives modulo p^{c-k-1} , it implies that

$$|B_k| = |B'_k| = |\mathcal{H}_{p^{c-k-1}} \cap \mathbb{Z}[\omega]| = |\mathbb{Z}[\omega]| / (p^{c-k-1}) = N(p^{c-k-1}) = 7^{c-k-1}.$$

Hence,

$$|B| = 1 + \sum_{k=0}^{c-1} 7^{c-k-1} = 1 + \sum_{j=0}^{c-1} 7^j = 1 + \frac{7^c - 1}{6} = \frac{7^c}{6} + \frac{5}{6}.$$

□

In the next section, we present a constructive method for building a Hamiltonian path in the bucket set described in Theorem 1. We also revisit several algorithms in [7] and develop new algorithms for this construction.

4 Hamiltonian Paths on the Optimal Bucket Set and Algorithms

In the original LFG framework over $\mathbb{Z}$, the bucket elements are simply sorted in increasing order. To extend this idea to $\mathbb{Z}[\omega]$, one needs to arrange the bucket set so that consecutive elements remain as close as possible. In [7, Section 5], the authors work with a disk and show that it satisfies the Ziggurat property, which allows the bucket set to be labeled in such a way that the squared distance between consecutive elements is at most $\frac{13}{4} \cdot 7$ (we correct this in Lemma 6).

In our hexagonal approach, the bucket set does not satisfy the Ziggurat property. However, the geometric structure of the hexagon allows us to construct a Hamiltonian path on the bucket set described in Theorem 1, with the same bound as $\frac{13}{4} \cdot 7$. Moreover, unlike their construction, our approach is straightforward to implement, thanks to its simple and explicit geometric description.

4.1 Hamiltonian Path Construction

With the bucket set B described in Theorem 1, we first compute the distance between two points in the bucket set $\bigcup_{k=0}^{c-1} B_k$.

- If $b_i = p^k(1 + p\kappa_i), b_j = p^k(1 + p\kappa_j)$ in the same B_k for some k then

$$|b_i - b_j|^2 = |p^{k+1}(\kappa_i - \kappa_j)|^2 \geq |p^{k+1}|^2 = 7^{k+1}.$$

Thus,

$$\min_{b_i \neq b_j \in B_k} |b_i - b_j|^2 \geq 7^{k+1} \text{ for } 0 \leq k \leq c-1. \quad (5)$$

- If $b_i = p^k(1 + p\kappa_i) \in B_k, b_j = p^l(1 + p\kappa_j) \in B_l$ where $1 \leq k < l$, then

$$|b_i - b_j|^2 = |p^k[(1 + p\kappa_i) - p^{l-k}(1 + p\kappa_j)]|^2 \geq 7^k.$$

Therefore,

$$\min_{\substack{b_i \in B_k, \\ b_j \in B_l, k \neq l}} |b_i - b_j|^2 \geq 7^{\min\{k, l\}} \text{ for } 0 \leq k, l \leq c-1. \quad (6)$$

The lower bounds in (5) and (6) explains why it is natural to first construct a Hamiltonian path with edge length $\sqrt{7}$ on

$$B_0 = 1 + pB'_0, \text{ where } B'_0 = \mathcal{H}_{p^{c-1}} \cap \mathbb{Z}[\omega].$$

Before turning to the main theorem, we introduce an additional notation. For $u \in \{1, 1 + \omega, \omega\}$, and for $m, n, t \in \mathbb{Z}$ where $m \leq n$, the u -layer of height t and range $[m, n]$ is defined by

$$\mathcal{L}_u(m, n; t) := \{z \in \mathbb{Z}[\omega] : uz = a + b\omega, m \leq a \leq n, b = t\}.$$

Thus $\mathcal{L}_u(m, n; t)$ is the set of consecutive lattice points lying on the row $\Im(uz) = \frac{\sqrt{3}}{2}t$, whose $\Re(uz)$ -coordinates range from $m - \frac{t}{2}$ to $n - \frac{t}{2}$. We have the following lemma.

Lemma 5. *Let l be a line, $u \in \{1, 1 + \omega, \omega\}$ and assume that the angle between l and lattice rows in direction unit u is not less than $\pi/3$. For each u -layer of height t , let e_t be the endpoints lying closest to d . Then $e_{t+1} - e_t \in \{1, \omega, 1 + \omega\}$. In other words, the endpoints of consecutive u -layers on the side facing d can be connected by a unit edge.*

Proof. See Appendix A. □

Now we are able to prove the main result of this section.

Theorem 2. *There exists a way to label the elements of B as*

$$B = \{b_0, b_1, \dots, b_{|B|-1}\} \subseteq \mathbb{Z}[\omega]$$

such that

$$|b_{i+1} - b_i|^2 \leq \frac{13}{4} \cdot 7, \text{ for all } 1 \leq i \leq |B| - 2.$$

Proof. The proof follows the same two steps as in [7, Theorem 6].

- Construct the Hamiltonian path with edges of length 1 in B'_0 .
- Rescale to $B_0 = 1 + pB'_0$ and insert each point $z \in \bigcup_{k=1}^{c-1} B_k$ into the Hamiltonian path of B_0 .

However we give a complete argument here, since the first step is adapted to our hexagonal approach with a detailed, implementable description, while the second step requires a correction.

Now let's construct a Hamiltonian path in B'_0 of edge length 1. Even though [13, Theorem 3] showed the existence of a desired Hamiltonian path of B'_0 in general, we want to construct a Hamiltonian path in this special case ($\mathcal{H}_{p^{c-1}}$ is symmetric under rotations by $\pi/3$ centered at the origin).

We call a regular hexagon standard-oriented if its vertices lie on the six rays generated by the units. We first define the largest standard-oriented regular hexagon inside $\mathcal{H}_{p^{c-1}}$. Since $\mathcal{H}_{p^{c-1}}$ is invariant under rotations by $\pi/3$, it is enough to choose its vertex on the positive real axis. Let

$$a = \max\{r \in \mathbb{Z}_{>0} : r \in \mathcal{H}_{p^{c-1}}\}, \quad z = a \in \mathbb{Z}[\omega], \quad (7)$$

and set $\mathcal{H} := \mathcal{H}_z$, whose vertices are uz , $u \in U$. Then $\mathcal{H} \subseteq \mathcal{H}_{p^{c-1}}$, is the largest standard-oriented regular hexagon inside $\mathcal{H}_{p^{c-1}}$.

Let $\mathcal{R} := \mathcal{H}_{p^{c-1}} \setminus (\mathcal{H} \setminus \partial\mathcal{H})$ be a region between the outer and inner hexagons, where $\partial\mathcal{H}$ denotes the set of lattice points in $\mathcal{H}$ which does not have all adjacent neighbors in $\mathcal{H}$. Since a Hamiltonian path in $\mathcal{H} \setminus \partial\mathcal{H}$ can be constructed easily by starting from the outermost layer and spiraling inward until one reaches the origin, it remains to handle $\mathcal{R}$.

Recall that the Eisenstein lattice decomposes into six natural sectors determined by the six lattice directions from the origin. By rotational symmetry, it is enough to work in one sector. We choose $\{a + b\omega : b \geq 0, 0 \leq a \leq b\}$, bounded by the rays generated by ω and $1 + \omega$, and set

$$\mathcal{R}^* = \mathcal{R} \cap \{a + b\omega : b \geq 0, 0 \leq a \leq b\}.$$

It remains to construct a Hamiltonian path in $\mathcal{R}^*$ with prescribed endpoints on the two boundary rays; the corresponding paths in the other five sectors are obtained by multiplying by units. Without loss of generality, we take these endpoints to be the vertices P, Q of the top side of $\mathcal{H}$. Thus the problem reduces to constructing a Hamiltonian path from P to Q through all points of $\mathcal{R}^*$.

Next, we choose a line d through the vertex V of $\mathcal{H}_{p^{c-1}}$ in $\mathcal{R}^*$, parallel to a lattice row, depending on the local configuration in the $2\pi/3$ degree at V . By Proposition 2(ii) and Remark 1, there are only two possible cases.

- V is a center of an upward-pointing unit equilateral triangle, see Figure 4(a). Since the angle at V and the angle $\angle EVM$ are both equal to $2\pi/3$, and since the boundary of $\mathcal{H}_{p^{c-1}}$ contains no lattice points (by Proposition 2(iii)), then exactly one vertex of this unit triangle lies in $\mathcal{R}^*$. We denote this vertex by

- M . Among the neighbors of M that remain in $\mathcal{R}^*$, we choose a point N such that there exists a line d passing through V , parallel to one of the lattice-row directions, with M and N lying on opposite sides of d .
- V is a center of downward-pointing unit equilateral triangles, see Figure 4(b). In this case, exactly one vertex of this unit triangle lies in $\mathcal{R}^*$; we denote this vertex by M . Let E and N be the two neighbors of M lying on the same horizontal lattice row as M . Since the angle at V and the angle $\angle EVN$ are both equal to $2\pi/3$, exactly one of these two neighbors lies in $\mathcal{R}^*$. We denote this neighbor by N . Finally, we choose the lattice-row line d passing through V so that M and N lie on opposite sides of d .

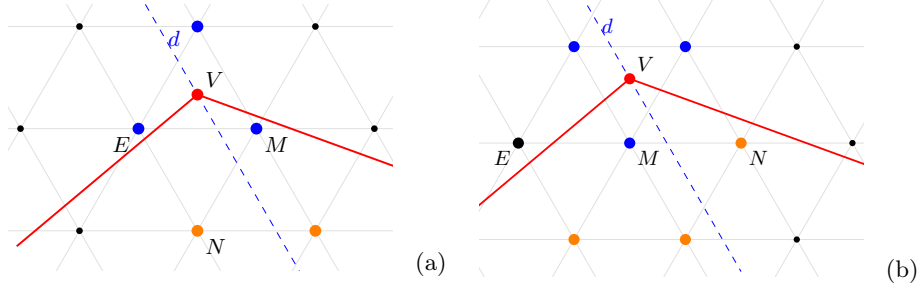


Fig. 4. Two local configurations at V . In case (a), V is the center of an upward-pointing unit triangle; in case (b), V is the center of a downward-pointing unit triangle. Blue points denote the vertices of the corresponding triangle. The point M is the vertex contained in $\mathcal{R}^*$, while the orange points denote the neighbors of M contained in $\mathcal{R}^*$. The point N is selected from these orange points as described.

In both cases, we can choose a line d passing through the vertex V parallel to the lattice row direction, together with two adjacent lattice points $M, N \in \mathcal{R}^*$, such that M and N lie on opposite sides of d . Without loss of generality, we relabel the two sides so that M and P lie on the left side of d , while N and Q lie on the right side.

The construction is illustrated in Figure 5. We will describe a Hamiltonian path from P to M on the left side of d , and a Hamiltonian path from N to Q on the right side. Since M and N are adjacent, reversing the first path and concatenating the two paths by the edge MN gives a Hamiltonian path from P to Q through all points of $\mathcal{R}^*$.

Let T_0 and T_1 denote the sets of lattice points on the two sides of the line d , where T_0 is the side containing M and P , and T_1 is the side containing N and Q . We write T_0 as a disjoint union of $(1 + \omega)$ -layers, while T_1 as a disjoint union of ω -layers. In T_0 , the point M lies on the $(1 + \omega)$ -layer with the largest height t_0 . Starting from M , we go the entire layer with height t_0 , then by Lemma 5 we are able to move to the next layer with height $t_0 - 1$, traverse it completely, and continue in the same way, layer by layer, until reaching P . Dually, in T_1 ,

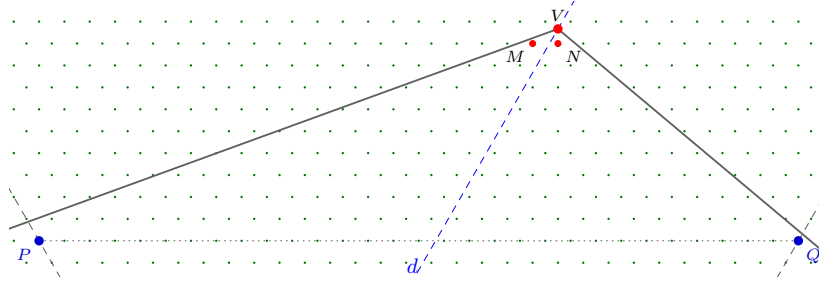


Fig. 5. The sector $\mathcal{R}^*$ and the choice of the line d such that the adjacent points M and N lie on opposite sides of d .

the point N lies on the ω -layer with smallest height t_1 , we traverse the entire layer with height t_1 , then move to the next layer with height $t_1 + 1$, traverse it completely, and continue likewise until reaching Q .

Hence we obtain a Hamiltonian path from M to P in T_0 , and a Hamiltonian path from N to Q in T_1 . Reversing the former gives a Hamiltonian path from P to M . Since M and N are neighbors, we may concatenate these two paths through the edge MN , thereby obtaining the desired Hamiltonian path from P to Q , as shown in Figure 6.

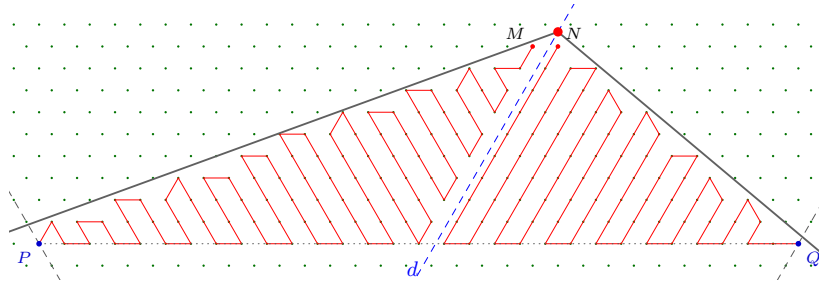


Fig. 6. Hamiltonian paths for T_0 and T_1

We now have an ordering of B_0 such that the distance between any two consecutive elements is $\sqrt{7}$. In the next step, we revisit the insertion argument used in [7, Theorem 6].

The argument in [7, Theorem 6] said that each point $z \in \bigcup_{k=1}^{c-1} B_k$ lies in a unit equilateral triangle with at least two vertices in B_0 . However, there may exist points z in general for which no unit equilateral triangle containing z has a side equal to a consecutive pair in the path on B_0 (see Figure 7). Such points cannot be inserted by the modification $z_n, z_{n+1} \rightarrow z_n, z, z_{n+1}$ without increasing edge length. We correct this point by the lemma as follows.

Lemma 6. Suppose $z \in \bigcup_{k=1}^{c-1} B_k$ is not contained in any unit equilateral triangle having one side equal to an edge of the Hamiltonian path on B_0 . Then z must occur in one of the local configurations shown in Figure 7. In this case, z can still be inserted into the Hamiltonian path by choosing an appropriate adjacent pair of vertices. This insertion may increase the maximal edge length, but only up to $\frac{\sqrt{13}}{2} \cdot \sqrt{7}$.

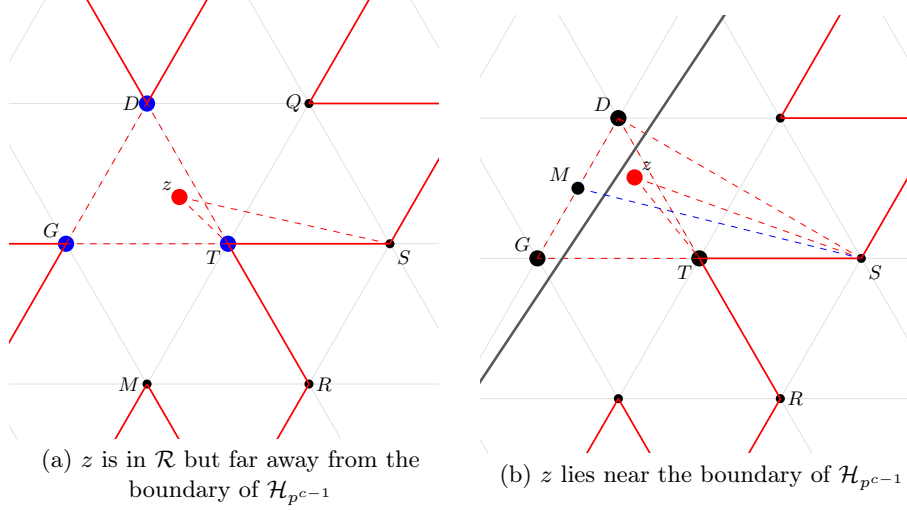


Fig. 7. Local configurations for points that are not covered by any equilateral triangle containing an edge of the Hamiltonian path of B_0 .

Proof. See Appendix A. □

Finally, by using Lemma 6 after inserting all points of $\bigcup_{k=1}^{c-1} B_k$, we obtain an ordering $B = \{b_0, b_1, \dots, b_{|B|-1}\}$ such that

$$|b_{i+1} - b_i|^2 \leq \frac{13}{4} \cdot 7 \text{ for all } 0 \leq i < |B| - 2.$$

□

- Remark 2.* (1) By equations (12) and (13), one may reduce the bound $\frac{\sqrt{13}}{2} \cdot \sqrt{7}$ to $\sqrt{3} \cdot \sqrt{7}$ by adding the point to the bucket set in case (b) and modifying the path $TzDS$ (Note that this bound is still larger than $\frac{\sqrt{7}}{\sqrt{3}} + \sqrt{7}$ in (12)). This slightly increases the size of the bucket set, but only in a few boundary cases, so the asymptotic size of B remains unchanged.
- (2) Another possible way to keep the ideal minimal bound $\sqrt{7}$ is to first determine the positions of the points $z \in \bigcup_{k=1}^{c-1} B_k$, and then prescribe in advance

which possible edges must appear in the Hamiltonian path on B'_0 . However, constructing a Hamiltonian path under such constraints seems to be an open problem in graph theory.

4.2 Algorithms and Examples

We now describe the algorithmic part of the construction. In particular, we collect the procedures needed for implementation.

Take an element $a \in \mathbb{Z}[\omega]$, we want to write an algorithm to find pairs $\{(\epsilon_j, b_j)\}_{0 \leq j \leq h}$, $\epsilon_j \in U$, $b_j \in B$ such that

$$a = \sum_{j=0}^h \epsilon_j b_j q^j.$$

Set $\kappa_0 := a$, by applying Corollary 1 and Theorem 1 repeatedly, we have

$$\begin{aligned} \kappa_j &= q\delta_j + a_j, \text{ where } a_j \in \mathcal{H}_q \\ a_j &= \epsilon_j b_j + q\gamma_j, \\ \kappa_{j+1} &= \delta_j + \gamma_j, \text{ for } 0 \leq j \leq h, \text{ where } h = \left\lceil \frac{\log |a|}{\log |q|} \right\rceil. \end{aligned}$$

Therefore,

$$\kappa_j = \varepsilon_j m_j b_j + q\kappa_{j+1}. \quad (8)$$

Since $\mathcal{H}_q$ is contained in the disk of radius $|q|/\sqrt{3}$, the same length bound as in [7, Lemma 4] holds for the digits a_j . Thus the proof of [7, Lemma 4] carries over without change, and we obtain a base- q expansion with at most $h + 1$ digits. Hence, we have

$$a = \sum_{j=0}^h \epsilon_j b_j q^j.$$

Moreover, as in the remark before [7, Theorem 6], when instantiating our method on the BLS12-381 elliptic curve [1] the base- q expansion is at most h digits long for $4 \leq c \leq 11$, $c \neq 7$.

We are now able to present the algorithms. First of all, by Corollary 1, we replace [7, Algorithm 7] by Algorithm 3. Therefore, [7, Algorithm 8] is replaced by Algorithm 4.

Algorithm 3 Finding the representative in $\mathcal{H}_q$

```

1: Input:  $t, q \in \mathbb{Z}[\omega]$ 
2: Output:  $\text{REPR}(t, q) = (r, k)$ 
3: Compute  $z = t/q := m + ni \in \mathbb{C}$ 
4:  $a \leftarrow \left\lfloor m + \frac{n}{\sqrt{3}} \right\rfloor, b \leftarrow \left\lfloor \frac{2}{\sqrt{3}}n \right\rfloor$ 
5:  $S \leftarrow \{a + b\omega, (a \pm 1) + b\omega, a + (b \pm 1)\omega, (a - 1) + (b - 1)\omega, (a + 1) + (b + 1)\omega\}$ 
6:  $\kappa \leftarrow a + b\omega$ 
7: for each  $\kappa' \in S$  do
8:   if  $|z| \leq |z - u|$  for all  $u \in U$  then
9:     if  $N(\kappa') < N(\kappa)$  then ▷ Choose  $\kappa$  with the smallest norm
10:     $\kappa \leftarrow \kappa'$ 
11:   end if
12: end if
13: end for
14:  $r \leftarrow t - q\kappa$ 
15: return  $(\kappa, r)$ 

```

Algorithm 4 New complex scalar recording

```

1: Input:  $a \in \mathbb{Z}[\omega], q = (2 - \omega)^c$  for  $c \in \mathbb{Z}_{>}$ 
2: Output:  $\{(\epsilon_j, b_j)\}_{0 \leq j \leq h}, \epsilon_j \in U, b_j \in B$  so that  $a = \sum_{j=0}^h \epsilon_j b_j q^j$  ▷  $h = \left\lceil \frac{\log |a|}{\log |q|} \right\rceil$ 
3:  $\kappa \leftarrow a$ 
4:  $h \leftarrow \left\lceil \frac{\log |a|}{\log |q|} \right\rceil$ 
5: list  $\leftarrow \{\}$ 
6: for from  $j = 0$  to  $h$  do
7:    $(\delta, r) \leftarrow \text{REPR}(\kappa, q)$ 
8:   if  $r = 0$  then
9:      $\epsilon_j = 1, b_j = 0$ 
10:  else
11:     $t \leftarrow r$ 
12:     $k \leftarrow 0$ 
13:    while  $p \mid t$  do
14:       $t \leftarrow t/p$ 
15:       $k \leftarrow k + 1$ 
16:    end while
17:    Take  $\epsilon_j \in U$  such that  $t \equiv \epsilon_j \pmod{p}$  ▷ use Euclidean Algorithm
18:     $\beta' \leftarrow \epsilon_j^{-1}t$ 
19:     $(\gamma, b) \leftarrow \text{REPR}(p^k \beta' - 1, q)$ 
20:     $b_j \leftarrow b + 1$  ▷  $p^k \beta' = q\gamma + b_j$  where  $b_j \in \mathcal{H}_q^+$ 
21:  end if
22:  list.append( $(\epsilon_j, b_j)$ )
23:   $\kappa \leftarrow \delta + \gamma$ 
24: end for
25: return list

```

Algorithm 5 Subsum accumulation algorithm with endomorphisms (Repaired)

```

1: Input:  $p, S_1, S_2, \dots, S_{|B|-1}, B = \{0\} \cup \{b_1, b_2, \dots, b_{|B|-1}\}$  as in Theorem 2.
2: Output:  $S = b_1 S_1 + \dots + b_{|B|-1} S_{|B|-1}$ 
3:  $\ell \leftarrow N(p)$ 
4: Determine  $D_\ell$  as defined and computed in (11) and Table 3
5: Define a length  $D_\ell$  array  $\text{tmp} = [0] \times D_\ell$ 
6: for  $i = |B| - 1$  to 1 by  $-1$  do
7:    $\text{tmp}[0] = \text{tmp}[0] + S_i$ 
8:    $k = b_i - b_{i-1}$ 
9:   if  $|k|^2 \geq 1$  then
10:     $\text{tmp}[k] = \text{tmp}[k] + \text{tmp}[0]$ 
11:   end if
12: end for
13: return  $\sum_{|k|^2 \leq 3.25\ell} k \cdot \text{tmp}[k]$ 

```

Note that by Theorem 2, [7, Algorithm 9] is designed based on an incorrect insertion argument. Thus, it needs to be revised as Algorithm 5.

Algorithm 6 below implements the first step in the proof of Theorem 2. Recall that T_0 and T_1 denote the sets of points on the two sides of $\mathcal{R}^*$ as shown in Figure 5. Let $z = a + b\omega \in \mathbb{Z}[\omega]$. We have

$$(1 + \omega)z = (a - b) + a\omega, \quad \omega z = -b + (a - b)\omega,$$

then the ω -layers are indexed by the height $a - b$, while the $(1 + \omega)$ -layers are indexed by the height a . Thus, to sort T_0 , we first sort by a and then within each layer by $a - b$; to sort T_1 , we first sort by $a - b$ and then within each layer by $-b$.

Moreover, the points inside a fixed layer are ordered by the remaining coordinate, either increasingly or decreasingly, depending on which choice makes the first point of the new layer adjacent to the last point of the current path.

Also, Algorithm 7 is based on the second step in the proof of Theorem 2.

Algorithm 6 Sorting the set B'_0

```

1: Input: an unsorted set  $B'_0 = \mathcal{H}_{p^{c-1}} \cap \mathbb{Z}[\omega]$ 
2: Output:  $B'_0 = \{b'_0, b'_1, \dots, b'_m\}$  s.t  $|b'_{i+1} - b'_i| = 1$  for all  $0 \leq i \leq m-1$ 
3: procedure GROUPBYHEIGHT( $T, i$ ) ▷ Sort each set  $T_i$ 
4:   if  $i = 0$  then
5:     for  $z = a + b\omega \in T$  do
6:        $h(z) \leftarrow a, r(z) \leftarrow a - b$ 
7:     end for
8:   else
9:     for  $z = a + b\omega \in T$  do
10:       $h(z) \leftarrow a - b, r(z) \leftarrow -b$ 
11:    end for
12:   end if
13:   Partition  $T$  into layers  $T = \bigsqcup_t L_t, L_t := \{z \in T : h(z) = t\}$ .
14:   if  $i = 0$  then
15:     Order the layers decreasingly by  $h$ .
16:   else
17:     Order the layers increasingly by  $h$ .
18:   end if
19:   Sort each layer increasingly by  $r$ 
20:   return  $(L_1, \dots, L_m)$ 
21: end procedure
22: procedure CONSTRUCTPATH( $((L_1, \dots, L_m), S)$ )
23:    $P \leftarrow L_1$ 
24:   for  $j$  from 2 to  $m$  do
25:     if  $P[-1] - L_j[0] \in U$  then
26:        $L_j \leftarrow \text{reverse}(L_j)$ 
27:     end if
28:      $P \leftarrow P \parallel L_j$ 
29:   end for
30:   return  $P$ 
31: end procedure
32: Construct the largest standard-oriented regular hexagon  $\mathcal{H} := \mathcal{H}_z \subseteq \mathcal{H}_{p^{c-1}}$  as
    described in (7).
33: Set  $\mathcal{R} := \mathcal{H}_{p^{c-1}} \setminus \mathcal{H} \cup \partial\mathcal{H}$  and choose the topmost sector  $\mathcal{R}^*$ 
34: Choose a line  $d$  splitting  $\mathcal{R}^*$  into two parts  $T_0$  and  $T_1$  as described in Theorem 2.
35:  $(L_1^{(0)}, \dots, L_m^{(0)}) \leftarrow \text{GROUPBYHEIGHT}(T_0, 0)$ 
36:  $(L_1^{(1)}, \dots, L_m^{(1)}) \leftarrow \text{GROUPBYHEIGHT}(T_1, 1)$ 
37:  $P_0 \leftarrow \text{CONSTRUCTPATH}((L_1^{(0)}, \dots, L_m^{(0)}), M)$ 
38:  $P_1 \leftarrow \text{CONSTRUCTPATH}((L_1^{(1)}, \dots, L_m^{(1)}), N)$ 
39:  $P_{\mathcal{R}^*} \leftarrow \text{reverse}(P_0) \parallel P_1$ 
40:  $P_{\mathcal{R}^*} = P_{\mathcal{R}^*}.\text{remove}(P_{\mathcal{R}^*}[0])$  ▷ remove first vertex to make sure that the path will
    end at P after rotation
41:  $P_{\mathcal{R}} \leftarrow P_{\mathcal{R}^*} \parallel (-\omega)P_{\mathcal{R}^*} \parallel (-1-\omega)P_{\mathcal{R}^*} \parallel (-1)P_{\mathcal{R}^*} \parallel \omega P_{\mathcal{R}^*} \parallel (1+\omega)P_{\mathcal{R}^*}$ .
42: Construct Hamiltonian path  $P_{\mathcal{H}}$  of  $\mathcal{H} \setminus \partial\mathcal{H}$  starting from  $(z-1)\omega$ .
43: return  $P_{\mathcal{R}} \parallel P_{\mathcal{H}}$ 

```

Algorithm 7 Sorting the bucket set B

```

1: Input:  $B_0, \dots, B_{c-1}$ 
2: Output:  $B = \{b_0, b_1, \dots, b_m\}$  s.t  $|b_{i+1} - b_i|^2 \leq \frac{13}{4} \cdot 7$  for all  $0 \leq i \leq m-1$ 
3: Run Algorithm 6 to get  $B'_0 = \{b'_0, b'_1, \dots, b'_m\}$  s.t  $|b'_{i+1} - b'_i| = 1$  for all  $0 \leq i \leq m-1$ 
4: Set  $B_0 = 1 + pB'_0$ 
5:  $B \leftarrow B_0$ 
6: for each  $z \in \bigcup_{k=1}^{c-1} B_k$  do
7:   if there is an edge  $b_i b_{i+1}$  of  $B_0$  such that  $z$  lies in a unit equilateral triangle
     with side  $b_i b_{i+1}$  then
8:     Insert  $z$  between  $b_i$  and  $b_{i+1}$  in  $B$ .
9:   else
10:    Choose  $T$  be a closest vertex of  $B_0$  to  $z$ .
11:    Choose  $S$  be the neighbor of  $T$  in the path closest to  $z$ .
12:    Insert  $z$  between  $T$  and  $S$  in  $B$ .
13:   end if
14: end for
15: return  $B$ 

```

Finally, we end this section with a few examples illustrating the construction. The examples below were generated by SageMath. We only visualize the cases $c = 2, 3, 4$ here, while examples for larger values of c can be found in our GitHub repository.

In Figures 8 and 9, blue points represent the vertices of B_0 . Green points represent the points in $\bigcup_{k=1}^{c-1} B_k$ that lie in a unit equilateral triangle having one side equal to an edge of the Hamiltonian path on B_0 . Red points represent the remaining points as shown in Lemma 6.

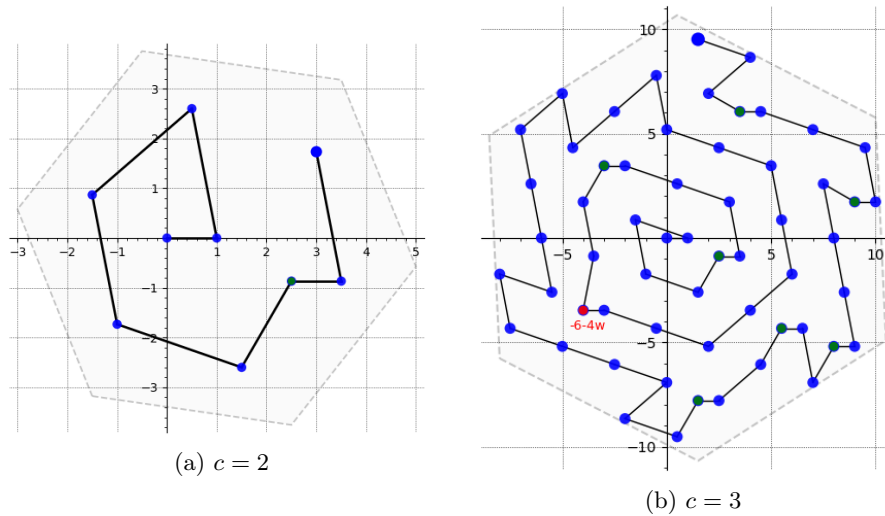


Fig. 8. Hamiltonian path for the bucket set B when $c = 2, 3$

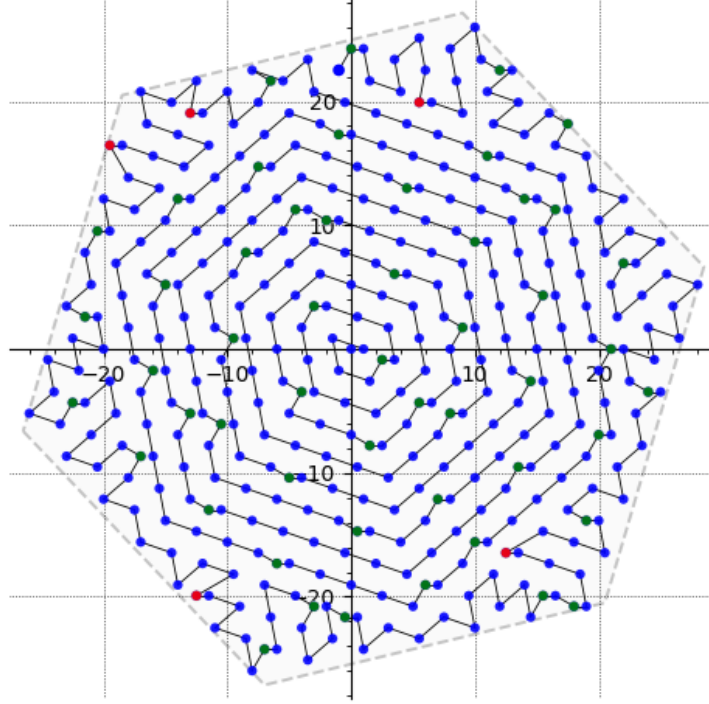


Fig. 9. Hamiltonian path for the bucket set B when $c = 4$

5 Generalization to Larger Multiplier Sets

In this section, we will present the construction of the larger multiplier sets with the same optimal bucket set described in Theorem 1. First of all, the following lemma is classical, we provide a proof in Appendix A for completeness.

Lemma 7. *Let K be a number field with the ring of integers $\mathcal{O}_K$. Assume that there is a rational prime $\ell \in \mathbb{Z}$ such that a prime ideal P of $\mathcal{O}_K$ lies over ℓ satisfies the ramification index $e(P \mid \ell)$ and residue degree $f(P \mid \ell)$ are both equal 1. Then*

$$\mathcal{O}_K/P^k \cong \mathbb{Z}/\ell^k\mathbb{Z} \text{ for any } k \in \mathbb{Z}_{>}.$$

Proof. See Appendix A. □

Moreover, if we choose a rational prime $\ell = 6e + 1$, then by Lemma 1 there exists a prime element $p = a + b\omega \in \mathbb{Z}[\omega]$, with $a, b \in \mathbb{Z}$, such that

$$\ell = p\bar{p} = a^2 - ab + b^2.$$

We are interested in such prime elements $p \in \mathbb{Z}[\omega]$. Since p is prime then $\mathbb{Z}[\omega]/(p)$ is a field of ℓ element, that is $\mathbb{Z}[\omega]/(p) \cong \mathbb{F}_\ell$. Then the multiplicative group $(\mathbb{Z}[\omega]/(p))^\times$ has order $6e$.

Recall that one of the key arguments in Theorem 1 is $(\mathbb{Z}[\omega]/(2-\omega))^\times = U$, so in the general case, we try to see the quotient group $(\mathbb{Z}[\omega]/(p))^\times/U$, which is presented in the lemma as follows.

Lemma 8. *Let ℓ be a rational prime of the form $\ell = 6e+1$, and a prime $p \in \mathbb{Z}[\omega]$ so that $N(p) = \ell$. Then*

$$M := \{a + b\omega \in \mathbb{Z}[\omega] : a > |b|, b \leq 0\} \cap \mathcal{H}_p \quad (9)$$

is the complete set of e representatives of the quotient $(\mathbb{Z}[\omega]/(p))^\times/U$. Furthermore, for any $k \in \mathbb{N}$, we have a partition

$$(\mathbb{Z}[\omega]/(p^k))^\times = \bigsqcup_{\epsilon \in U, m \in M} \epsilon m \left((\mathbb{Z}[\omega]/(p^k))^\times \right)^{6e},$$

that is, $UM = \{\epsilon m : \epsilon \in U, m \in M\}$ is the complete set of representatives $(\mathbb{Z}[\omega]/(p^k))^\times$ modulo $6e$ -th powers.

Proof. Note that by Corollary 1, $\mathcal{H}_p \cap \mathbb{Z}[\omega]$ is the complete set of representatives modulo p , we have $|\mathcal{H}_p \cap \mathbb{Z}[\omega]| = 6e + 1$, then $|M| = e$. Moreover, when consider the quotient group of this group by the unit group, we can pick the representatives in the sector $\{a + b\omega \in \mathbb{Z}[\omega] : a > |b|, b \leq 0\}$. Thus,

$$(\mathbb{Z}[\omega]/(p))^\times = \bigsqcup_{i=1}^e m_i U, \text{ where } m_i \in M.$$

Additionally, since ℓ splits in $\mathbb{Z}[\omega]$, let's say $(\ell) = (p)(\bar{p})$ then we have $e(p | \ell) = f(p | \ell) = 1$. For any $k \in \mathbb{N}$, applying Lemma 7, one has

$$\mathbb{Z}[\omega]/(p^k) \cong \mathbb{Z}/\ell^k \mathbb{Z}.$$

Moreover, since ℓ is an odd prime then by [5, Corollary 20, Ch. 9], $(\mathbb{Z}/\ell^k \mathbb{Z})^\times$ is a cyclic group of order $\ell^{k-1}(\ell-1)$. Therefore, $(\mathbb{Z}[\omega]/(p^k))^\times$ is a cyclic group and $\left| (\mathbb{Z}[\omega]/(p^k))^\times \right| = \ell^{k-1}(\ell-1)$. This shows that $6e$ divides $\left| (\mathbb{Z}[\omega]/(p^k))^\times \right|$, so the group $\left((\mathbb{Z}[\omega]/(p^k))^\times \right) / \left((\mathbb{Z}[\omega]/(p^k))^\times \right)^{6e}$ has order $6e$. Now for any $r, s \in UM$, by Hensel's lemma, the equation

$$r \equiv sx^{6e} \pmod{p} \text{ solvable in } \mathbb{Z}[\omega] \iff r \equiv sx^{6e} \pmod{p^k} \text{ solvable in } \mathbb{Z}[\omega].$$

Then

$$(\mathbb{Z}[\omega]/(p^k))^\times = \bigsqcup_{\epsilon \in U, m \in M} \epsilon m \left((\mathbb{Z}[\omega]/(p^k))^\times \right)^{6e}.$$

□

Remark 3. We choose the representatives in sector $\{a + b\omega \in \mathbb{Z}[\omega] : a > |b|, b \leq 0\}$ because, in the precomputation step for the multiplier set M , it is desirable to use representatives $a + b\omega$ with minimal $|a| + |b|$. In fact, among the six unit associates of a nonzero Eisenstein integer, the representative lying in this sector achieves the smallest value of $|a| + |b|$. Table 2 presents few small cases.

Table 2. Multiplier sets M for few first rational primes ℓ and the size of M

p	ℓ	M	$ M $
$2 - \omega$	7	1	1
$3 - \omega$	13	$1, 1 - \omega$	2
$3 - 2\omega$	19	$1, 1 - \omega, 2$	3
$5 - \omega$	31	$1, 1 - \omega, 2, 2 - \omega, 1 - 2\omega$	5
$4 - 3\omega$	37	$1, 1 - \omega, 2, 2 - \omega, 1 - 2\omega, 3$	6
$6 - \omega$	42	$1, 1 - \omega, 2, 2 - \omega, 1 - 2\omega, 3, 2 - 2\omega$	7
$5 - 4\omega$	61	$1, 1 - \omega, 2, 2 - \omega, 1 - 2\omega, 3, 2 - 2\omega, 4, 3 - \omega, 1 - 3\omega$	10
$7 - 2\omega$	67	$1, 1 - \omega, 2, 2 - \omega, 1 - 2\omega, 3, 2 - 2\omega, 4, 3 - \omega, 1 - 3\omega, 2 - 3\omega$	11
$8 - \omega$	73	$1, 1 - \omega, 2, 2 - \omega, 1 - 2\omega, 3, 2 - 2\omega, 4, 3 - \omega, 1 - 3\omega, 2 - 3\omega, 3 - 2\omega$	12

The following theorem is the analog of [7, Theorem 4] in $\mathbb{Z}[\omega]$.

Theorem 3. *With a prime $p \in \mathbb{Z}[\omega]$ such that $N(p) = \ell = 6e + 1$ is a rational prime, for every $c \in \mathbb{Z}_{>}$, Property 1 holds for $q = p^c$,*

$$M = \{a + b\omega \in \mathbb{Z}[\omega] : a > |b|, b \leq 0\} \cap \mathcal{H}_p$$

and the bucket set

$$B = \{0\} \cup \bigcup_{k=0}^{c-1} B_k$$

where

$$B_k = \{b \in \mathcal{H}_q^+ \cap \mathbb{Z}[\omega] : b = p^k \beta \text{ and } \beta \equiv 1 \pmod{p}\},$$

Hence, we can reorder the bucket set that the maximal squared distance between two consecutive integers is $\frac{13}{4} \cdot \ell$ and the size of the bucket set is

$$|B| = 1 + \frac{\ell^c - 1}{6e}.$$

Proof. For any $t \in \mathbb{Z}[\omega]$, we have $t = p^k \alpha$ where $p \nmid \alpha$ and $k = v_p(t)$. If $k \geq c$, then $t \equiv 0 \pmod{p^c}$ and we take $b = 0 \in B$.

Assume that $k < c$. Since $p \nmid \alpha$, then $\alpha \in (\mathbb{Z}[\omega]/(p^{c-k}))^\times$, so by Lemma 8 there exist $\epsilon \in U, m \in M$ and $\beta \in \left((\mathbb{Z}[\omega]/(p^{c-k}))^\times\right)^{6e}$ such that

$$\alpha \equiv \epsilon m \beta \pmod{p^{c-k}}.$$

Hence

$$t = p^k \alpha \equiv p^k \epsilon m \beta = \epsilon m b \pmod{q}.$$

Furthermore, by using the fact (we have seen in the proof of Lemma 8) that

$$\beta \in \left((\mathbb{Z}[\omega]/(p^{c-k}))^\times \right)^{6e} \iff \beta \in \left((\mathbb{Z}[\omega]/(p))^\times \right)^{6e},$$

and $\left((\mathbb{Z}[\omega]/(p))^\times \right)^{6e} = \{1\}$, one obtain $\beta \equiv 1 \pmod{p}$.

Next, we use the similar argument to the proof of Theorem 1, one has the size of the bucket set is

$$|B| = 1 + \sum_{k=0}^{c-1} \ell^{c-k-1} = 1 + \sum_{j=0}^{c-1} \ell^j = 1 + \frac{\ell^c - 1}{\ell - 1} = 1 + \frac{\ell^c - 1}{6e}.$$

Finally, because the bucket set B is of the same form as in Theorem 1, then we may apply Theorem 2 to complete the proof. $\square$

Remark 4. Increasing the size of the multiplier set comes at the cost of increasing both storage and maximal distance, independent of c and h ; see Table 3.

The first few good values of $|M|$ are summarized in Table 2. Nevertheless, there remain several values of $|M|$, for instance 4, 8, 9, $\dots$, for which it is not yet known whether an optimal bucket set can be constructed within this framework.

6 Complexity Analysis

We now analyze the storage and time complexity of our construction. First, we adapt the proof of [7, Lemma 4]. From (8), we obtain

$$|\kappa_h| \leq \frac{\sqrt{r}}{\sqrt{3}|q|^h} + \frac{|q|/\sqrt{3} + 1}{|q| - 1} (1 - |q|^{-h}) \max_{m \in M} |m|, \quad (10)$$

where $h = \left\lceil \frac{\log r}{\log |q|^2} \right\rceil$. Moreover, (9) gives $\max_{m \in M} |m| \leq |p|/\sqrt{3}$.

To facilitate a direct comparison with LFG and FKSX, we use the same BLS12-381 parameters. For $M = \{1\}$, this recovers the bound used in [7]. For $M = \{1, 1 - \omega\}$, $p = 3 - \omega$, we have $\max_{m \in M} |m| = \sqrt{3}$. For $4 \leq c \leq 8$, (10) gives $|\kappa_h| < \sqrt{3}$. Hence κ_h is either 0 or unit. Therefore, the storage is at most $(2nh + n) \cdot P$.

It remains to estimate the cost of the subsum accumulation step (needed for Algorithm 5). It is enough to count the Eisenstein integers whose norm is at most $\frac{13}{4}\ell$. We define

$$D_\ell = \# \left\{ z \in \mathbb{Z}[\omega] : N(z) \leq \frac{13}{4}\ell \right\}. \quad (11)$$

Table 3. n_ℓ for the first few rational primes $\ell \equiv 1 \pmod{6}$

p	ℓ	$ M $	D_ℓ
$2 - \omega$	7	1	85
$3 - \omega$	13	2	151
$3 - 2\omega$	19	3	223
$5 - \omega$	31	5	367
$4 - 3\omega$	37	6	433
$6 - \omega$	42	7	511
$5 - 4\omega$	61	10	721
$7 - 2\omega$	67	11	793
$8 - \omega$	73	12	859

It is not hard to compute D_ℓ in Table 3.

We now compare the theoretical storage and computation cost of our construction when $p = 2 - \omega$, $M = \{1\}$ (in other words $\ell = 7$) with previous methods when computing $S_{n,r}$ over BLS12-381 for $n = 2^e$ ($10 \leq e \leq 21$). The computation costs of the Repaired LFG method and the FKSX method are taken from [7, Table 6]. For each n , we search the parameter c that minimizes the theoretical computation cost of our construction. A summary comparison is reported in Table 4, while the full parameter table is given in Table 6 in Appendix B.

In Table 4, the columns Improve1, Improve2 and Improve3 compare our construction with the Pippenger variant, the Repaired LFG, and the FKSX, respectively. With C and S denote the number of Additions and the number of precomputed points, we compute for each baseline method

$$I_C = (C_{\text{base}} - C_{\text{ours}})/C_{\text{base}}, \quad I_S = (S_{\text{base}} - S_{\text{ours}})/S_{\text{base}}$$

As shown in the column Improve2 of Table 4, our construction saves a significant amount of storage compared with the Repaired LFG method, which uses $(3nh + n) \cdot P$ precomputed points (see Table 1). We also make Table 5 for the case $p = 3 - \omega$, hence $\ell = N(p) = 13$, $M = \{1, 1 - \omega\}$. It needs $(2nh + n) \cdot P$ precomputed points, and we compare it with Repaired LFG.

7 Conclusion

Multi-scalar multiplication (MSM) is a major bottleneck in many pairing-based zk-SNARK schemes. A common strategy for accelerating MSM is to trade additional precomputation storage for reduced online computation, as in Pippenger’s variant, the LFG framework, and the FKSX method.

In this paper, we proposed a new optimal bucket set construction using the geometry of regular hexagons in the Eisenstein lattice $\mathbb{Z}[\omega]$. The construction is designed for MSM with efficient endomorphisms and achieves the optimal bucket size. We also gave an explicit Hamiltonian path algorithm for the bucket set. Finally, we generalized the construction to larger multiplier sets, which leads

Table 4. Theoretical improvement of our construction when $\ell = 7$ with previous methods for computing $S_{n,r}$ in BLS12-381.

n	Our Construction for $\ell = 7$				Improve1		Improve2		Improve3	
	q	h	C	S	I_C	I_S	I_C	I_S	I_C	I_S
2^{10}	$(2 - \omega)^5$	19	2.23×10^4	19×2^{10}	9.10%	13.64%	4.12%	68.85%	6.53%	0%
2^{11}	$(2 - \omega)^5$	19	4.18×10^4	19×2^{11}	7.24%	5.00%	6.08%	67.24%	5.87%	0%
2^{12}	$(2 - \omega)^5$	19	8.07×10^4	19×2^{12}	6.17%	5.00%	5.61%	67.24%	5.38%	0%
2^{13}	$(2 - \omega)^6$	16	1.51×10^5	16×2^{13}	7.98%	15.79%	2.10%	67.35%	7.51%	0%
2^{14}	$(2 - \omega)^6$	16	2.82×10^5	16×2^{14}	4.43%	0.00%	3.81%	67.35%	6.68%	0%
2^{15}	$(2 - \omega)^6$	16	5.44×10^5	16×2^{15}	2.35%	0.00%	4.73%	67.35%	6.37%	0%
2^{16}	$(2 - \omega)^7$	13	9.89×10^5	13×2^{16}	8.51%	12.50%*	10.06%	67.44%	8.40%	0%
2^{17}	$(2 - \omega)^7$	13	1.84×10^6	13×2^{17}	12.20%	6.67%*	10.62%	65.00%	8.39%	0%
2^{18}	$(2 - \omega)^7$	13	3.55×10^6	13×2^{18}	9.84%	0.00%*	9.10%	65.00%	7.44%	0%
2^{19}	$(2 - \omega)^7$	13	6.95×10^6	13×2^{19}	5.27%	-7.69%*	8.03%	65.00%	7.42%	0%
2^{20}	$(2 - \omega)^8$	12	1.35×10^7	12×2^{20}	4.32%	7.69%	6.59%	67.57%	8.49%	0%
2^{21}	$(2 - \omega)^8$	12	2.61×10^7	12×2^{21}	4.17%	0.00%	7.35%	67.57%	8.00%	0%

C : number of elliptic curve Additions S : number of precomputed points

* The storage when $c = 7$ is $n(h + 1) \cdot P$ instead of $nh \cdot P$ normally. A sharper analysis may show that h digits suffice also in this case.

Table 5. Theoretical improvement of our construction when $\ell = 13$ with the Repaired LFG method for computing $S_{n,r}$ in BLS12-381.

n	Our Construction for $\ell = 13$				Improv2	
	q	h	C	S	I_C	I_S
2^{10}	$(3 - \omega)^4$	18	2.01×10^4	37×2^{10}	10.04%	39.34%
2^{11}	$(3 - \omega)^4$	18	3.94×10^4	37×2^{11}	11.48%	36.21%
2^{12}	$(3 - \omega)^4$	18	7.63×10^4	37×2^{12}	10.81%	36.21%
2^{13}	$(3 - \omega)^5$	14	1.46×10^5	29×2^{13}	5.34%	40.82%
2^{14}	$(3 - \omega)^5$	14	2.61×10^5	29×2^{14}	11.10%	40.82%
2^{15}	$(3 - \omega)^5$	14	4.90×10^5	29×2^{15}	14.21%	40.82%
2^{16}	$(3 - \omega)^5$	14	9.49×10^5	29×2^{16}	13.76%	32.56%
2^{17}	$(3 - \omega)^5$	14	1.87×10^6	29×2^{17}	9.41%	27.50%
2^{18}	$(3 - \omega)^6$	12	3.55×10^6	25×2^{18}	9.02%	37.50%
2^{19}	$(3 - \omega)^6$	12	6.69×10^6	25×2^{19}	11.46%	37.50%
2^{20}	$(3 - \omega)^6$	12	1.30×10^7	25×2^{20}	10.45%	32.43%
2^{21}	$(3 - \omega)^6$	12	2.56×10^7	25×2^{21}	9.33%	32.43%

to the trade-offs between storage and computation that can reduce the bucket set size when more precomputation is allowed in the FKSX setting.

Moreover, substantial further improvements in computation are limited, since the cost is always greater than nh . Furthermore, whenever $|M| = e$ and $6e + 1$ is

prime, our construction gives an optimal bucket set size. Thus, for these multiplier set sizes, further storage reduction is essentially precluded. The remaining possible improvement is to extend the construction to multiplier set sizes not covered by this condition, such as $|M| = 4, 8, 9, \dots$, for which optimal bucket set constructions are not yet known.

References

1. Barreto, P.S., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: International conference on security in communication networks. pp. 257–267. Springer (2002)
2. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: 2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18–21, 2014. pp. 459–474. IEEE Computer Society (2014). <https://doi.org/10.1109/SP.2014.36>
3. Bernstein, D.J., Doumen, J., Lange, T., Oosterwijk, J.J.: Faster batch forgery identification. In: International Conference on Cryptology in India. pp. 454–473. Springer (2012)
4. Brickell, E.F., Gordon, D.M., McCurley, K.S., Wilson, D.B.: Fast exponentiation with precomputation. In: Workshop on the Theory and Application of Cryptographic Techniques. pp. 200–207. Springer (1992)
5. Dummit, D., Foote, R.: Abstract algebra. 3rd ed. Chichester: Wiley, 3 edn. (2004)
6. Eberhardt, J.: ZoKrates. <https://zokrates.github.io/>
7. Fan, X., Kuchta, V., Sica, F., Xu, L.: Speeding up multi-scalar multiplications for pairing-based zkSNARKs: X. fan et al. Journal of Cryptology **38**(2), 21 (2025)
8. Groth, J.: Short pairing-based non-interactive zero-knowledge arguments. In: Abe, M. (ed.) Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5–9, 2010. Proceedings. pp. 321–340. Lecture Notes in Computer Science, Springer (2010). https://doi.org/10.1007/978-3-642-17373-8_19
9. Groth, J.: On the size of pairing-based non-interactive arguments. In: Fischlin, M., Coron, J. (eds.) Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8–12, 2016, Proceedings, Part II. pp. 305–326. Lecture Notes in Computer Science, Springer (2016). https://doi.org/10.1007/978-3-662-49896-5_11
10. Luo, G., Fu, S., Gong, G.: Speeding up multi-scalar multiplication over fixed points towards efficient zkSNARKs. IACR Transactions on Cryptographic Hardware and Embedded Systems pp. 358–380 (2023)
11. Marcus, D.A., Sacco, E.: Number fields, vol. 1995. Springer (1977)
12. Pippenger, N.: On the evaluation of powers and related problems. In: 17th Annual Symposium on Foundations of Computer Science (sfcs 1976). pp. 258–263. IEEE Computer Society (1976)
13. Polishchuk, V., Arkin, E.M., Mitchell, J.S.: Hamiltonian cycles in triangular grids. In: CCCG (2006)
14. Stewart, I., Tall, D.: Algebraic Number Theory and Fermat’s Last Theorem. Chapman and Hall/CRC, 4th edn. (2015). <https://doi.org/10.1201/b19331>

15. Straus, E.G.: Addition chains of vectors (problem 5125). American Mathematical Monthly **70**(806-808), 16 (1964)
16. The Sage Developers: SageMath, the Sage Mathematics Software System (Version 10.6) (2025), <https://www.sagemath.org>

A Additional Proofs

Proof of Lemma 1. Apply [11, Theorems 24 and 25] by using the fact that $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ with discriminant -3 , we have ℓ is ramified if and only if $\ell = 3$. Besides, when $\ell \neq 3$ we also have

$$\left(\frac{-3}{\ell}\right) = \left(\frac{-1}{\ell}\right) \left(\frac{3}{\ell}\right) = (-1)^{(\ell-1)/2} \left(\frac{\ell}{3}\right) (-1)^{(\ell-1)/2} = \left(\frac{\ell}{3}\right),$$

thus showing our lemma. $\square$

Proof of Proposition 2.

(i) We have

$$\begin{aligned} w \in q\mathcal{H}_1 &\iff \omega/q \in \mathcal{H}_1 \\ &\iff |w/q| \leq |w/q - u|, \forall u \in U \\ &\iff |w| \leq |q| \cdot |w/q - u| = |w - qu|, \forall u \in U \\ &\iff w \in \mathcal{H}_q. \end{aligned}$$

$\square$

(ii) We have $\frac{1-\omega}{3}, \frac{2+\omega}{3}$ are the centers of the unit equilateral triangles as in Figure 2, they are also the vertices of $\mathcal{H}_1$, so the set of all centers of equilateral triangles in $\mathbb{Z}[\omega]$ is

$$\mathcal{C} := \left(\frac{1-\omega}{3} + \mathbb{Z}[\omega]\right) \cup \left(\frac{2+\omega}{3} + \mathbb{Z}[\omega]\right).$$

Consider one of the vertices of $\mathcal{H}_q$, namely $\frac{q(1-\omega)}{3}$ (other vertices of $\mathcal{H}_q$ are its associates). Thus,

$$\begin{aligned} \frac{q(1-\omega)}{3} \in \mathcal{C} &\iff \frac{q(1-\omega)}{3} = \frac{\epsilon(1-\omega)}{3} + \kappa, \text{ where } \epsilon \in U, \kappa \in \mathbb{Z}[\omega] \\ &\iff q(1-\omega) = \epsilon(1-\omega) + 3\kappa \\ &\iff q - \epsilon = -\omega^2\kappa(1-\omega) \quad (\text{since } 3 = -\omega^2(1-\omega)^2) \\ &\iff q \equiv \epsilon \pmod{1-\omega} \\ &\iff (1-\omega) \nmid q \quad (\text{since } \mathbb{Z}[\omega]/(1-\omega) \cong \mathbb{F}_3). \end{aligned}$$

$\square$

(iii) Since $\mathcal{H}_q$ is symmetric under rotations by $\pi/3$ centered at the origin, it suffices to prove that there is no lattice points on one edge of $\mathcal{H}_q$.

Note that we have $\frac{1-\omega}{3}, \frac{2+\omega}{3}$ are two adjacent vertices of $\mathcal{H}_1$, then by Proposition 2 (i), $\mathcal{H}_q = q\mathcal{H}_1$ has two adjacent vertices

$$V_1 = \frac{q(2+\omega)}{3}, V_2 = \frac{q(1-\omega)}{3}$$

Let $q = a + b\omega$ where $a, b \in \mathbb{Z}$. An arbitrary point on the edge V_1V_2 is of the form $tV_1 + (1-t)V_2$ where $0 \leq t \leq 1, t \in \mathbb{R}$. We have

$$\begin{aligned} z_t &:= tV_1 + (1-t)V_2 \\ &= t \frac{(a+b\omega)(2+\omega)}{3} + (1-t) \frac{(a+b\omega)(1-\omega)}{3} \\ &= \frac{1}{3} \left[t(2a-b) + (1-t)(a+b) \right] + \frac{1}{3} \left[t(a+b) + (1-t)(-a+2b) \right] \omega \\ &= \frac{1}{3} \left[(a+b) + t(a-2b) \right] + \frac{1}{3} \left[(-a+2b) + t(2a-b) \right] \omega \end{aligned}$$

Therefore, V_1V_2 contains a lattice point if there exist $t \in \mathbb{R}$ so that $z_t \in \mathbb{Z}[\omega]$. One has

$$\begin{aligned} z_t \in \mathbb{Z}[\omega] &\iff \left[(a+b) + t(a-2b) \right] + \left[(-a+2b) + t(2a-b) \right] \omega \in 3\mathbb{Z}[\omega] \\ &\iff \begin{cases} (a+b) + t(a-2b) \in 3\mathbb{Z} \\ (-a+2b) + t(2a-b) \in 3\mathbb{Z} \end{cases} \quad (*) \end{aligned}$$

First of all, both conditions imply that $t \in \mathbb{Q}$. Let $X = a - 2b, Y = 2a - b$ then we have $tX, tY \in \mathbb{Z}$, which means the denominator of t must divide both X, Y . It follows

$$t = \frac{r}{d} \text{ where } d = \gcd(X, Y), r \in \mathbb{Z}.$$

Then the condition $0 \leq t \leq 1$ gives $0 \leq r \leq d$.

Furthermore, we observe that if $3 \mid d$ then 3 divides both X, Y . So, there exists a $0 \leq t \leq 1$ so that the condition (*) holds. Indeed, pick $t = 0$, then (*) becomes $a+b, -a+2b \in 3\mathbb{Z}$. These conditions hold since $a+b = Y-X$ and $-a+2b = -X$. Hence, V_1V_2 contains a lattice points if $3 \mid \gcd(a-2b, 2a-b)$. We now consider the case when $3 \nmid d$. Let $X = dX', Y = dY'$ where $\gcd(X', Y') = 1$. Note that $X+Y = 3(a-b) \equiv 0 \pmod{3}$, so $Y \equiv -X \pmod{3}$. Since $3 \nmid d$, then $Y' \equiv -X' \pmod{3}$. It implies $3 \nmid X', Y'$.

Thus, the second condition of (*) becomes

$$\begin{aligned} -X + tY \equiv 0 \pmod{3} &\iff Y(1+t) \equiv 0 \pmod{3} \iff Y'(d+r) \equiv 0 \pmod{3} \\ &\iff d+r \equiv 0 \pmod{3} \end{aligned}$$

If $d > 1$ then we can always choose $0 \leq r \leq d$ so that $r \equiv -d \pmod{3}$. Thus, $t = r/d$ satisfies the second condition of (*). We also verify that the first condition of (*) also holds for this t . Indeed, it becomes

$$Y - X + \frac{r}{d}X \equiv 0 \pmod{3},$$

which is true since $Y - X + \frac{r}{d}X \equiv -X + 2X + \frac{r}{d}X \equiv X'(r+d) \equiv 0 \pmod{3}$. Finally, if $d = 1$, then we can not find r such that $d+r \equiv 0 \pmod{3}$. Therefore, there is no $0 \leq t \leq 1, t \in \mathbb{Q}$ satisfy (*). In this case, V_1V_2 contains no lattice points. $\square$

Proof of Remark 1(c). For the forward direction we assume that $\gcd(2a - b, a - 2b) = 1$. First of all, $a + b$ must be non zero modulo 3 since otherwise $a \equiv -b \pmod{3}$, and then $2a - b \equiv a - 2b \pmod{3}$. Moreover, let $d = \gcd(a, b)$ then d divides both $2a - b$ and $a - 2b$, so d must be 1.

We now assume $\gcd(a, b) = 1$ and $a + b \not\equiv 0 \pmod{3}$. For the sake of contradiction, let p be a common prime divisor of $2a - b$ and $a - 2b$. Thus, one has

$$\begin{cases} p \mid (2a - b) \\ p \mid (a - 2b) \end{cases} \implies \begin{cases} p \mid (a + b) \\ p \mid 3(a - b) \end{cases}$$

Since p is prime then either $p \mid 3$ or $p \mid (a - b)$. If $p \mid (a - b)$, then we imply that $p \mid 2a$ and $p \mid 2b$. So $p \mid \gcd(2a, 2b) = 2$. Then $p = 2$. But when $p = 2$, we have $2a - b, a - 2b$ are even, so both a, b are even, which contradicts to our assumption $\gcd(a, b) = 1$. If $p \mid 3$, then $p = 3$. Thus, $3 \mid (a + b)$, it follows that $a + b \equiv 0 \pmod{3}$, which is also a contradiction.

In addition, with $q = a + b\omega \in \mathbb{Z}[\omega]$, by using the facts that $q = a + b - b(1 - \omega)$ and $3 = -\omega^2(1 - \omega)^2$ we can easily prove that

$$a + b \not\equiv 0 \pmod{3} \iff (1 - \omega) \nmid q.$$

In conclusion, the boundary of $\mathcal{H}_q$ contains no lattice points if and only if

$$\gcd(a, b) = 1 \text{ and } (1 - \omega) \nmid q.$$

□

Proof of Lemma 3. Indeed, if $(1 - \omega) \mid q$ then taking the norm both sides we have $3 \mid \ell^c$, impossible. Moreover, if a rational prime r divides both a and b , then $r \mid q$, hence $r^2 \mid N(q) = \ell^c$. Thus $r = \ell$. But $\ell = up\bar{p}$ and $\ell \mid p^c$ implies $\bar{p} \mid p^{c-1}$, contradicting that p and $\bar{p}$ are not associate. Therefore no rational prime divides both a and b . Hence, $\gcd(a, b) = 1$. □

Proof of Lemma 5. We can assume that $u = 1$ without loss of generality, so the 1-layers are now horizontal rows

$$\mathcal{L}_1(m, n; t) = \{z \in \mathbb{Z}[\omega] : z = a + b\omega, m \leq a \leq n, b = t\}.$$

Assume the equation of the line l is $y = mx + b$, where $|m| > \sqrt{3}$ (the case $m = \pm\sqrt{3}$ is obvious since the endpoints are on the lattice row). Without loss of generality, we might assume that $m > \sqrt{3}$ and consider the half space H separated by the line l

$$H = \{x + yi : y < mx + b\}.$$

The endpoint e_t on the layers t in H is of the form

$$e_t = a_t + t\omega = a_t - \frac{t}{2} + \frac{\sqrt{3}}{2}ti.$$

Since $e_t \in H$ then $\frac{\sqrt{3}}{2}t < m \left(a_t - \frac{t}{2} \right) + b$, so

$$a_t > \frac{1}{m} \left(\frac{\sqrt{3}}{2}t - b \right) + \frac{t}{2} = \frac{1}{2} \left(\frac{\sqrt{3}}{m} + 1 \right) t - \frac{b}{m}.$$

Since e_t is the endpoint of layer height t , then a_t must be chosen by

$$a_t = \left\lceil \frac{1}{2} \left(\frac{\sqrt{3}}{m} + 1 \right) t - \frac{b}{m} \right\rceil.$$

Moreover, for the endpoint $e_{t+1} = a_{t+1} + (t+1)\omega$ on the layer of height $t+1$ in H , one has

$$a_{t+1} = \left\lceil \frac{1}{2} \left(\frac{\sqrt{3}}{m} + 1 \right) t - \frac{b}{m} + \frac{1}{2} \left(\frac{\sqrt{3}}{m} + 1 \right) \right\rceil.$$

We also have $m > \sqrt{3}$ then $0 < \frac{1}{2} \left(\frac{\sqrt{3}}{m} + 1 \right) < 1$. Therefore, $a_{t+1} - a_t \in \{0, 1\}$.

It implies $e_{t+1} - e_t \in \{\omega, 1 + \omega\}$. $\square$

Proof of Lemma 6. First of all, the equations (5),(6) show that two distinct points of $\bigcup_{k=1}^{c-1} B_k$ cannot lie in the same triangle. Moreover, if two equilateral triangles share an edge of B_0 , then their union contains at most one point of $\bigcup_{k=1}^{c-1} B_k$. Indeed, suppose $z \in T, z' \in T'$ and two triangle T, T' share an edge. Then $T \cup T'$ is a rhombus with the longest diagonal of length $\sqrt{21}$, so $|z - z'|^2 < 21$.

On the other hand, $z - z' \in p\mathbb{Z}[\omega]$, then $z - z' = p\kappa$, $\kappa \in \mathbb{Z}[\omega]$. So $|\kappa|^2 < 3$, then $\kappa \in U$. Thus one obtains $z = z' + p\kappa$. But translation by $p\kappa$ preserves the orientation of elementary triangles, whereas adjacent triangles sharing an edge have opposite orientations, which is impossible.

Therefore, if z is landed in the largest standard-oriented regular hexagon $\mathcal{H}$, then z lies in a unit equilateral triangle with two vertices in B_0 . It remains to consider the case $z \in \mathcal{R}$. In this region, there are only two possible local configurations, as shown in Figure 7.

In case (a), z is in the triangle TDG but none of the sides of this triangle is used as an edge of the Hamiltonian path on B_0 . We assume that T is a closest vertex of the triangle to z . Since $T \in B_0$, say locally it contains the subpath RTS , we may assume that z is more closer to S than R without loss of generality, we then insert z by replacing the edge TS with the two edges Tz and zS . Thus

$$|z - S| \leq |z - T| + |T - S| \leq \frac{\sqrt{7}}{\sqrt{3}} + \sqrt{7} < \frac{\sqrt{13}}{2} \cdot \sqrt{7}. \quad (12)$$

In case (b), z lies near the boundary, it is clear from the Figure 7(b) that

$$|z - S| \leq |SM| = \frac{\sqrt{13}}{2} \cdot \sqrt{7}. \quad (13)$$

Therefore, in both cases, z can be inserted into the Hamiltonian path while increasing the maximal edge length to at most $\frac{\sqrt{13}}{2} \cdot \sqrt{7}$. $\square$

Proof of Lemma 7. Consider the composition $\phi := \iota \circ \pi$ of the embedding ι and projection π

$$\phi : \mathbb{Z} \xrightarrow{\iota} \mathcal{O}_K \xrightarrow{\pi} \mathcal{O}_K/P^k, n \mapsto n \bmod P^k$$

Then ϕ is a ring homomorphism. We now prove that $\ker \phi = p^k \mathbb{Z}$.

Let $n = p^k m \in p^k \mathbb{Z}$ then $\phi(n) = n \bmod P^k = p^k m \bmod P^k = 0 \bmod P^k$ since $P^k \mid p^k$ for any k . Thus, $p^k \mathbb{Z} \subseteq \ker \phi$. Conversely, let $n \in \ker \phi$ then $P^k \mid (n)$ in $\mathcal{O}_K$. In $\mathbb{Z}$, we write $n = p^t m$ where $t = v_p(n)$ and $p \nmid m$. Since $e(P \mid p) = 1$, then the ideal (n) contains a factor P^t and P is not in the ideal factorization of (m) . So $P^k \mid (n) \implies t \geq k$. It implies $p^k \mid p^t m = n$, which means $n \in p^k \mathbb{Z}$. Therefore, one obtains $\ker \phi \subseteq p^k \mathbb{Z}$ and hence $\ker \phi = p^k \mathbb{Z}$.

By the First Isomorphism Theorem we have

$$\mathbb{Z}/p^k \mathbb{Z} \cong \text{Im } \phi \subseteq \mathcal{O}_K/P^k.$$

Now we show that $|\mathbb{Z}/p^k \mathbb{Z}| = |\mathcal{O}_K/P^k|$. Indeed, since $f(P \mid p) = 1$ then $N(P) = p^{f(P \mid p)} = p$. It follows that $|\mathcal{O}_K/P^k| = N(P^k) = N(P)^k = p^k = |\mathbb{Z}/p^k \mathbb{Z}|$.

Hence,

$$\mathcal{O}_K/P^k \cong \mathbb{Z}/p^k \mathbb{Z}.$$

$\square$

B Additional theoretical cost comparisons over BLS12-381 curve

Table 6. Theoretical comparison of parameters, storage, and computation costs when $\ell = 7$ for computing $S_{n,r}$ in BLS12-381.

Pippenger Variant					Repaired LFG					FKSX					Our Construction for $\ell = 7$				
n	q	h	C	S	q	h	C	S	q	h	C	S	q	h	C	S			
2^{10}	2^{12}	22	2.46×10^4	22×2^{10}	2^{13}	20	2.33×10^4	$(3 \cdot 20 + 1) \times 2^{10}$	$(2 - \omega)^5$	19	2.39×10^4	19×2^{10}	$(2 - \omega)^5$	19	2.23×10^4	19×2^{10}	$(2 - \omega)^5$	19×2^{10}	
2^{11}	2^{13}	20	4.50×10^4	20×2^{11}	2^{14}	19	4.45×10^4	$(3 \cdot 19 + 1) \times 2^{11}$	$(2 - \omega)^5$	19	4.44×10^4	19×2^{11}	$(2 - \omega)^5$	19	4.18×10^4	19×2^{11}	$(2 - \omega)^5$	19×2^{11}	
2^{12}	2^{13}	20	8.60×10^4	20×2^{12}	2^{14}	19	8.55×10^4	$(3 \cdot 19 + 1) \times 2^{12}$	$(2 - \omega)^5$	19	8.53×10^4	19×2^{12}	$(2 - \omega)^5$	19	8.07×10^4	19×2^{12}	$(2 - \omega)^5$	19×2^{12}	
2^{13}	2^{14}	19	1.64×10^5	19×2^{13}	2^{16}	16	1.54×10^5	$(3 \cdot 16 + 1) \times 2^{13}$	$(2 - \omega)^6$	16	1.63×10^5	16×2^{13}	$(2 - \omega)^6$	16	1.51×10^5	16×2^{13}	$(2 - \omega)^6$	16×2^{13}	
2^{14}	2^{16}	16	2.95×10^5	16×2^{14}	2^{16}	16	2.93×10^5	$(3 \cdot 16 + 1) \times 2^{14}$	$(2 - \omega)^6$	16	3.02×10^5	16×2^{14}	$(2 - \omega)^6$	16	2.81×10^5	16×2^{14}	$(2 - \omega)^6$	16×2^{14}	
2^{15}	2^{16}	16	5.57×10^5	16×2^{15}	2^{16}	16	5.71×10^5	$(3 \cdot 16 + 1) \times 2^{15}$	$(2 - \omega)^6$	16	5.81×10^5	16×2^{15}	$(2 - \omega)^6$	16	5.44×10^5	16×2^{15}	$(2 - \omega)^6$	16×2^{15}	
2^{16}	2^{16}	16	1.08×10^6	16×2^{16}	2^{19}	14	1.10×10^6	$(3 \cdot 14 + 1) \times 2^{16}$	$(2 - \omega)^7$	13	1.08×10^6	13×2^{16}	$(2 - \omega)^7$	13	9.89×10^5	13×2^{16}	$(2 - \omega)^7$	13×2^{16}	
2^{17}	2^{18}	15	2.10×10^6	15×2^{17}	2^{20}	13	2.06×10^6	$(3 \cdot 13 + 1) \times 2^{17}$	$(2 - \omega)^7$	13	2.01×10^6	13×2^{17}	$(2 - \omega)^7$	13	1.84×10^6	13×2^{17}	$(2 - \omega)^7$	13×2^{17}	
2^{18}	2^{19}	14	3.93×10^6	14×2^{18}	2^{20}	13	3.90×10^6	$(3 \cdot 13 + 1) \times 2^{18}$	$(2 - \omega)^7$	13	3.83×10^6	13×2^{18}	$(2 - \omega)^7$	13	3.55×10^6	13×2^{18}	$(2 - \omega)^7$	13×2^{18}	
2^{19}	2^{20}	13	7.34×10^6	13×2^{19}	2^{20}	13	7.56×10^6	$(3 \cdot 13 + 1) \times 2^{19}$	$(2 - \omega)^7$	13	7.51×10^6	13×2^{19}	$(2 - \omega)^7$	13	6.95×10^6	13×2^{19}	$(2 - \omega)^7$	13×2^{19}	
2^{20}	2^{20}	13	1.42×10^7	13×2^{20}	2^{22}	12	1.45×10^7	$(3 \cdot 12 + 1) \times 2^{20}$	$(2 - \omega)^8$	12	1.48×10^7	12×2^{20}	$(2 - \omega)^8$	12	1.35×10^7	12×2^{20}	$(2 - \omega)^8$	12×2^{20}	
2^{21}	2^{22}	12	2.73×10^7	12×2^{21}	2^{22}	12	2.82×10^7	$(3 \cdot 12 + 1) \times 2^{21}$	$(2 - \omega)^8$	12	2.84×10^7	12×2^{21}	$(2 - \omega)^8$	12	2.61×10^7	12×2^{21}	$(2 - \omega)^8$	12×2^{21}	
C : number of elliptic curve additions										S : number of precomputed points									

C : number of elliptic curve Additions S : number of precomputed points