Perfect Codes Correcting a Single Burst of Limited-Magnitude Errors

Hengjia Wei and Moshe Schwartz, *Senior Member, IEEE*

***Abstract*— Motivated by applications to DNA-storage, flash memory, and magnetic recording, we study perfect burst-correcting codes for the limited-magnitude error channel. These codes are lattices that tile the integer grid with the appropriate error ball. We construct two classes of such perfect codes correcting a single burst of length 2, where each error affects the corresponding position by increasing it by one, both for cyclic and non-cyclic bursts. We also present a generic construction that requires a primitive element in a finite field with specific properties. We then show that in various parameter regimes such primitive elements exist, and hence, infinitely many perfect burst-correcting codes exist.**

***Index Terms*— Integer coding, perfect codes, burst-correcting codes, lattices, limited-magnitude errors.**

I. Introduction

IN MANY communication or storage systems, errors tend to occur in close proximity to each other, rather than occurring independently of each other. If the errors are confined to an interval of positions of length b, they are referred to as a *burst of length* b. Note that not all the positions in the interval are necessarily erroneous. A code that can correct any single burst of length b is called a *b-burst-correcting code*.

The design of burst-correcting codes has been researched in the error models of substitutions, deletions and insertions. Concerning the substitutions, Abdel-Ghaffar et al. [1], [2] showed the existence of optimum cyclic b-burst-correcting codes for any fixed b, and Etzion [11] gave a construction for perfect binary 2-burst-correcting codes. As for deletions and insertions, it has been shown in [21] that correcting a single burst of deletions is equivalent to correcting a single burst of insertions. Codes correcting a burst of exactly b consecutive deletions, or a burst of up to b consecutive deletions, were presented in [18] and [21], with the redundancy being of optimal asymptotic order. The b-burst-correcting codes pertaining to deletions were treated in [3], called codes correcting localized deletions therein, and a class of such codes of asymptotically optimal redundancy was proposed. Similarly, permutation codes correcting a single burst of b consecutive deletions were studied in [9].

This paper focuses on the model of *limited-magnitude errors*, which could be found in several applications, including high-density magnetic recording channels [17], [19], flash memories [8], and some DNA-based storage systems [15], [29]. In all of these applications, information is encoded as a vector of integers $\mathbf{x} \in \mathbb{Z}^n$. A (k_+, k_-)-limited-magnitude error affects a position by increasing it by as much as k_+ or decreasing it by as much as k_-. The design of codes combating random limited-magnitude errors has been extensively researched, see e.g., [5], [6], [12], [14], [16], [23], [25], [26], [27], [29], [30], [31], [32], [33], and [34]. However, the applications which exhibit limited-magnitude errors are prone to errors occurring in a burst. The coding schemes for magnetic recording channels [17], [19], and the DNA-based storage system of [15], all employ a constrained code as part of the system. Decoders for constrained codes are usually finite state machines, and an error in their decoding process causes a burst of errors in their output (e.g., see [20, Section 5.5]). Similarly, flash memories suffer from inter-cell interference [10], leading again to bursts of errors. To the extent of our knowledge, there is no research in the literature on codes correcting a single burst of limited-magnitude errors. We therefore focus in this paper on such codes, and in particular, perfect codes.

Following the research on bursts of substitutions, e.g., [1], [2], and [11], we distinguish between *cyclic bursts* and *non-cyclic bursts*, of limited-magnitude errors. In the examples mentioned here, [1], [2] study cyclic bursts, whereas [11] studies non-cyclic bursts. We follow suit, and study both types of bursts. Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ be the set of integers mod n. If a word $\mathbf{x} \in \mathbb{Z}^n$ suffers a cyclic burst of length b, then we can write the corrupted vector as $\mathbf{x} + \mathbf{e}$ for some $\mathbf{e}$ in the error ball

$$\begin{aligned}&\mathcal{E}^{\circ}(n, b, k_+, k_-) \triangleq \\ &\{(e_0, e_1, \ldots, e_{n-1}) \in [-k_-, k_+]^n \mid \text{ there is an } i \in \mathbb{Z}_n \text{ s.t.} \\ &\ e_\ell = 0 \text{ for all } \ell \in \mathbb{Z}_n \setminus \{i, i+1, \ldots, i+b-1\}\}. \end{aligned} \tag{1}$$

If $\mathbf{x}$ suffers a non-cyclic burst of length b, then the corrupted vector is $\mathbf{x} + \mathbf{e}$ for some $\mathbf{e}$ in the error ball

$$\begin{aligned}&\mathcal{E}(n, b, k_+, k_-) \triangleq \\ &\{\mathbf{e} = (e_1, e_2, \ldots, e_n) \in [-k_-, k_+]^n \mid \text{ there is an } i \in [1, n] \\ &\text{ s.t. } e_\ell = 0 \text{ for all } \ell \in [1, n] \setminus [i, \min\{n, i+b-1\}]\}. \end{aligned} \tag{2}$$

Manuscript received 6 January 2022; revised 24 July 2022; accepted 5 October 2022. Date of publication 10 October 2022; date of current version 20 January 2023. This work was supported in part by the Israel Science Foundation (ISF) under Grant 270/18. An earlier version of this paper was presented in part at ISIT 2022. *(Corresponding author: Hengjia Wei.)*

Hengjia Wei is with the Peng Cheng Laboratory, Shenzhen 518000, China (e-mail: hjwei05@gmail.com).

Moshe Schwartz is with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer Sheva 8410501, Israel (e-mail: schwartz@ee.bgu.ac.il).

Communicated by A.-L. Horlemann-Trautmann, Associate Editor for Coding and Decoding.

Digital Object Identifier 10.1109/TIT.2022.3213239

TABLE I
SUMMARY OF PERFECT-CODE CONSTRUCTIONS (q IS A PRIME POWER)

b	k_+	k_-	n	Cyclic	Source	Comments
2	1	0	$n = 2^r$	N	[11]	$r \geqslant 4$
2	1	0	$n \geqslant 2$	N	Theorem 5	
2	1	0	$4 \leqslant n \equiv 1 \pmod 3$	Y	Theorem 6	
2	1	0	$n = \frac{q-1}{2}$	Y	Theorem 9	$q \geqslant 7$ odd
2	1	1	$n = \frac{q-1}{6}$	Y	Theorem 14	$q \equiv 7 \bmod 12$ sufficiently large
2	1	1	$n = \frac{q-1}{6}$	Y	Theorem 18	$q \equiv 13 \bmod 24$ sufficiently large
3	1	0	$n = \frac{q-1}{4}$	Y	Theorem 15	$q \equiv 1 \bmod 4$ sufficiently large
3	1	1	$n = \frac{q-1}{18}$	Y	Theorem 16	$q \equiv 19 \bmod 36$ sufficiently large

Note that in the cyclic case we use $\mathbb{Z}_n$ to label the coordinates and the addition is done in $\mathbb{Z}_n$ (i.e., modulo n), while in the non-cyclic case we use the set $[1, n]$ to label the coordinates and the addition is operated in $\mathbb{Z}$.

The subject of interest for this paper is perfect codes correcting a single burst of limited-magnitude errors. Our main contributions are:

1) For each $n \geqslant 2$, we construct a perfect code of length n which can correct a non-cyclic 2-burst of $(1, 0)$-limited-magnitude errors.
2) For each $n \equiv 1 \pmod 3$, we construct a perfect code of length n which can correct a cyclic 2-burst of $(1, 0)$-limited-magnitude errors.
3) We present a generic construction based on finite fields for cyclic codes correcting a cyclic b-burst of (k_+, k_-)-limited-magnitude errors. This construction requires, as input, a primitive element that satisfies some conditions, and our goal is to show that such a primitive element indeed exists. Combining this construction and the approach in [2], we show the existence of a class of perfect cyclic b-burst-correcting codes for each $(b, k_+, k_-) \in \{(2, 1, 0), (2, 1, 1), (3, 1, 0), (3, 1, 1)\}$.

The parameters of the code constructions are summarized in Table I. We have the following two comments on our results.

1) In this paper, we choose $\mathbb{Z}^n$ as the space of transmitted/stored messages, and the codes presented in this paper are lattice codes, i.e., additive subgroups of $\mathbb{Z}^n$. Although this makes the analysis simpler, in practice we need codes over a finite alphabet, i.e., $\{0, 1, \ldots, q-1\}$. To this end, let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice code, we can take $\mathcal{C}_{\mathbf{v}} = (\Lambda + \mathbf{v}) \cap \{0, 1, \ldots, q-1\}$ for an arbitrary vector $\mathbf{v} \in \mathbb{Z}^n$. If Λ can correct a burst of limited-magnitude errors, then the q-ary code $\mathcal{C}_{\mathbf{v}}$ can correct the same kind of errors. Furthermore, if Λ is a perfect code, then according to the pigeonhole principle, there is a vector $\mathbf{v} \in \mathbb{Z}^n$ such that $\mathcal{C}_{\mathbf{v}}$ has size at least $q^n / |\mathcal{E}(n, b, k_+, k_-)|$ or $q^n / |\mathcal{E}^\circ(n, b, k_+, k_-)|$. For a detailed discussion on practical applications of lattice codes, the reader is referred to [22, Section II.B].
2) All the codes presented in this paper have the parameter $k_+ = 1$. For $k_+ \geqslant 2$, finding a perfect lattice becomes more difficult. Discussions and some computer search results for $k_+ \geqslant 2$ are presented in Section V. We note that in practice one could use q-ary substitution-correcting codes to combat limited-magnitude errors. If $k_+ + k_- + 1$ is close to q, the size of the error ball pertaining to limited-magnitude errors is close to that of the ball pertaining to substitutions, and so, using substitution-correcting codes would not increase the redundancy significantly. Therefore, the limited-magnitude errors are usually studied in the region where $k_+ + k_-$ is small.

The paper is organized as follows. We begin, in Section II, by providing notation and basic known results used throughout the paper. Section III is devoted to the constructions of perfect codes correcting a 2-burst of $(1, 0)$-limited-magnitude errors. Both non-cyclic bursts and cyclic bursts are considered. Section IV presents the generic construction for codes correcting a single cyclic b-burst, and uses it to treat the cases of $(b, k_+, k_-) \in \{(2, 1, 0), (2, 1, 1), (3, 1, 0), (3, 1, 1)\}$. In Section V we summarize the results, and comment on extensions and open questions.

II. PRELIMINARIES

For integers $a \leqslant b$ we define $[a, b] \triangleq \{a, a+1, \ldots, b\}$. For a sequence $\mathbf{s}$, we use $\mathbf{s}[i, j]$ to denote the subsequence of $\mathbf{s}$ which starts at the position i and ends at the position j. We use $\mathbb{Z}_m$ to denote the cyclic group of integers with addition modulo m, and $\mathbb{F}_q$ to denote the finite field of size q.

We say $\mathcal{B} \subseteq \mathbb{Z}^n$ *packs* $\mathbb{Z}^n$ by $T \subseteq \mathbb{Z}^n$, if the translates of $\mathcal{B}$ by elements from T do not intersect, namely, for all $\mathbf{v}, \mathbf{v}' \in T$, $\mathbf{v} \neq \mathbf{v}'$,

$$(\mathbf{v} + \mathcal{B}) \cap (\mathbf{v}' + \mathcal{B}) = \varnothing.$$

We say $\mathcal{B}$ *covers* $\mathbb{Z}^n$ by T if

$$\bigcup_{\mathbf{v} \in T} (\mathbf{v} + \mathcal{B}) = \mathbb{Z}^n.$$

If $\mathcal{B}$ both packs and covers $\mathbb{Z}^n$ by T, then we say that $\mathcal{B}$ *tiles* $\mathbb{Z}^n$ by T, or we say that T is a *tiling* of $\mathbb{Z}^n$ with $\mathcal{B}$. It now follows that a perfect code capable of correcting a cyclic burst in our setting is equivalent to a tiling of $\mathbb{Z}^n$ with $\mathcal{E}^\circ(n, b, k_+, k_-)$ defined in (1), and a perfect code capable of

correcting a non-cyclic burst in our setting is equivalent to a tiling of $\mathbb{Z}^n$ with $\mathcal{E}(n,b,k_+,k_-)$ defined in (2).

A code $\Lambda \subseteq \mathbb{Z}^n$ is called a *lattice code* if it is an additive subgroup of $\mathbb{Z}^n$. Similarly, a tiling T of $\mathbb{Z}^n$ with $\mathcal{B}$ is called a *lattice tiling* if T is an additive subgroup of $\mathbb{Z}^n$. Throughout the paper, we shall only consider lattice codes, since these are easier to analyze, construct, and encode, than non-lattice codes.

The following result provides a way to convert a code over $\mathbb{F}_p$ which can correct a burst of substitutions to a lattice code which can correct a burst of limited-magnitude errors.

Theorem 1: Let p be a prime. Let $\mathcal{C} \subseteq \mathbb{F}_p^n$ be a linear code which can correct a cyclic/non-cyclic burst of b substitutions. If $k_+ + k_- + 1 = p$, then

$$\Lambda \triangleq \{\mathbf{x} \in \mathbb{Z}^n \mid (\mathbf{x} \bmod p) \in \mathcal{C}\}$$

is a lattice code which can correct a cyclic/non-cyclic burst of b (k_+,k_-)-limited-magnitude errors. Furthermore, if $\mathcal{C}$ is perfect, then Λ is perfect.

Proof: According to its definition, Λ is closed under addition and under multiplication by integers. Thus, Λ is a lattice.

Denote $\mathcal{B} \triangleq \mathcal{E}(n,b,k_+,k_-)$ (or $\mathcal{E}^\circ(n,b,k_+,k_-)$ for the cyclic case). We now prove $\mathcal{B}$ packs $\mathbb{Z}^n$ by Λ. Assume that $\mathbf{v}+\mathbf{e} = \mathbf{v}'+\mathbf{e}'$, for some $\mathbf{v},\mathbf{v}' \in \Lambda$ and $\mathbf{e},\mathbf{e}' \in \mathcal{B}$. Then $\mathbf{e}-\mathbf{e}' = \mathbf{v}'-\mathbf{v} \in \Lambda$. By the definition of Λ, we have $\mathbf{e}'' \triangleq ((\mathbf{e}-\mathbf{e}') \bmod p) \in \mathcal{C}$. We note that $\mathbf{e}$ has nonzero entries only in an interval of length b, and so does $\mathbf{e}'$. Since $\mathbf{e}''+\mathbf{e}' \equiv \mathbf{0}+\mathbf{e} \pmod p$ and $\mathcal{C}$ can correct a burst of b substitutions, necessarily $((\mathbf{e}-\mathbf{e}') \bmod p) = \mathbf{e}'' = \mathbf{0}$. Since every entry of $\mathbf{e}-\mathbf{e}'$ is in the range $[-(k_+ + k_-), k_+ + k_-]$, and since $k_+ + k_- + 1 = p$, we have that $\mathbf{e}-\mathbf{e}' = \mathbf{0}$, which in turn implies $\mathbf{v} = \mathbf{v}'$. It follows that $\mathcal{B}$ packs $\mathbb{Z}^n$ by Λ.

To show tiling, let $\mathbf{x} \in \mathbb{Z}^n$ be any integer vector. Then $\mathbf{x}' \triangleq (\mathbf{x} \bmod p) \in \mathbb{F}_p^n$. Since $\mathcal{C}$ is a perfect code, there exists $\mathbf{v}' \in \mathcal{C}$ and $\mathbf{e}' \in \mathbb{F}_p^n$, where the support set of $\mathbf{e}'$ is contained in an interval of length b, such that $\mathbf{x}' = \mathbf{v}'+\mathbf{e}'$. Since $k_+ + k_- + 1 = p$, there exists $\mathbf{e} \in \mathcal{B}$ such that $(\mathbf{e} \bmod p) = \mathbf{e}'$. But then $\mathbf{x}-\mathbf{e} \equiv \mathbf{v}' \bmod p$ and by definition $\mathbf{x}-\mathbf{e} \in \Lambda$. Hence, $\mathcal{B}$ covers $\mathbb{Z}^n$ by Λ. Combing the arguments above, we have that Λ is a tiling of $\mathbb{Z}^n$ with $\mathcal{B}$ if $\mathcal{C}$ is perfect. ■

To the best of our knowledge, the only known perfect burst-correcting codes with respect to substitutions are the ones proposed in [11], which have block length n that is a power of 2, and can correct a non-cyclic burst of two substitutions. Thus, using Theorem 1 we can obtain a class of perfect lattice which can correct a non-cyclic burst of two $(1,0)$-limited-magnitude errors. In this paper, we shall construct more perfect burst-correcting codes for limited-magnitude errors.

A. Group Splitting

Perfect lattice codes that correct a single (k_+,k_-)-limited-magnitude error are equivalent to lattice tilings of $\mathbb{Z}^n$ with $\mathcal{E}(n,1,k_+,k_-)$. Some papers consider an equivalent tiling of $\mathbb{R}^n$ instead of $\mathbb{Z}^n$ as follows: The *unit cube* is defined as $Q_n \triangleq [0,1)^n \subseteq \mathbb{R}^n$. For each point of $\mathcal{E}(n,1,k_+,k_-)$, we place a unit cube, Q_n, centered at it. Then the union of these unit cubes is called a *cross* when $k_+ = k_-$, a *semi-cross* when $k_- = 0$, and a *quasi-cross* when $k_+ \geqslant k_- \geqslant 0$. The study of lattice tilings of $\mathbb{R}^n$ with these shapes can be traced back to 1960's (e.g., see [24]), and is usually connected with group splitting (e.g., [12], [14], [22], [23], and [25]). For an excellent treatment and history, the reader is referred to [27] and the many references therein. More recent results may be found in [31] and the references therein.

To construct codes that correct multiple errors, the notion of group splitting was generalized in [6]. Lattice tilings of chairs, or equivalently perfect lattice codes that correct $n-1$ random $(k_+,0)$-limited-magnitude errors, were constructed there. Additionally, several non-existence results for perfect codes that correct multiple random errors can be found in [6] and [28]. In this paper, we shall study lattice codes that correct a single burst of limited-magnitude errors by using the concept of (generalized) group splitting.

Let G be a finite Abelian group, where $+$ denotes the group operation. For $m \in \mathbb{Z}$ and $g \in G$, let $mg = g+g+\cdots+g$ (with m copies of g) if $m \geqslant 0$ and $mg = (-m)(-g)$ if $m < 0$. For a sequence $\mathbf{m} = (m_1, m_2, \ldots, m_n) \in \mathbb{Z}^n$ and a sequence $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in G^n$, we denote

$$\mathbf{m} \cdot \mathbf{s} \triangleq \sum_{i=1}^{n} m_i s_i.$$

Definition 2: A set $\mathcal{A} \subset \mathbb{Z}^n$ *splits* an Abelian group G with a *splitting sequence* $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in G^n$ if the set $\{\mathbf{a} \cdot \mathbf{s} \mid \mathbf{a} \in \mathcal{A}\}$ contains $|\mathcal{A}|$ distinct elements of G. This operation is called a *(generalized) splitting*.

The following theorem shows the connection between a lattice tiling and a group splitting.

Theorem 3 (Corollary 1 in [6]): Let $\mathcal{A} \subset \mathbb{Z}^n$ be a finite subset. A lattice tiling of $\mathbb{Z}^n$ with $\mathcal{A}$ exists if and only if there exists an Abelian group G of order $|\mathcal{A}|$ such that $\mathcal{A}$ splits G.

In our context of b-burst-correcting codes with respect to (k_+,k_-)-limited-magnitude errors, we need to take $\mathcal{A} = \mathcal{E}(n,b,k_+,k_-)$ or $\mathcal{A} = \mathcal{E}^\circ(n,b,k_+,k_-)$, and the code construction problem becomes that of finding an Abelian group G of order $|\mathcal{A}|$ and a vector $\mathbf{s} \in G^n$ such that $\mathcal{A}$ splits G with $\mathbf{s}$.

Splittings with $\mathcal{E}(n,b,k_+,k_-)$ can also be used to characterize codes that correct a single burst of substitutions. Let p be a prime and let k_+ and k_- be non-negative integers such that $k_+ + k_- + 1 = p$. Let $\mathcal{C}$ be an $[n, n-r]_p$-linear code with parity-check matrix H. We treat the columns of H as elements of $\mathbb{F}_p^r$ and denote them as $h_1, h_2, \ldots, h_n$. Then $\mathcal{C}$ is a perfect b-burst-correcting code with respect to substitutions if and only if $p^r = |\mathcal{E}(n,b,k_+,k_-)|$ and the additive group $\mathbb{F}_p^r$ can be split by $\mathcal{E}(n,b,k_+,k_-)$ with the sequence $\mathbf{h} = (h_1, h_2, \ldots, h_n)$. Binary perfect 2-burst-correcting codes pertaining to substitutions were studied in [11] and a construction for their parity-check matrices was presented. The existence result of such codes could be stated as follows in the language of splittings.

Theorem 4 [11]: For each $r \geqslant 5$, there exists a splitting of $\mathbb{F}_2^r$ by $\mathcal{E}(2^{r-1}, 2, 1, 0)$.

In the following two sections we are going to present some other constructions of splittings by $\mathcal{E}(n,b,k_+,k_-)$ or $\mathcal{E}^\circ(n,b,k_+,k_-)$. Then according to Theorem 3, the corresponding lattice tilings are obtained.

III. Perfect 2-Burst-Correcting Codes for $(1,0)$-Limited-Magnitude Errors

In this section, we present a class of constructions for 2-burst-correcting codes with $(1,0)$-limited-magnitude errors, both for cyclic bursts as well as for non-cyclic bursts. Our constructions are based on splitting the cyclic group $\mathbb{Z}_g$, where $g=2n$ for the non-cyclic burst and $g=2n+1$ for the cyclic burst. Using these constructions, together with Theorem 3, we show that $\mathbb{Z}^n$ can be lattice tiled by $\mathcal{E}(n,2,1,0)$ for all $n\geqslant 2$, and that $\mathbb{Z}^n$ can be lattice tiled by $\mathcal{E}^\circ(n,t,1,0)$ for all $n\equiv 1 \pmod 3$.

The basic idea behind these constructions comes from design theory: we start with a short sequence $(a_1,a_2,\ldots,a_s)$ that satisfies a certain property, and develop it by adding a series of numbers $(0,b,2b,\ldots,tb)$ to each element a_i. In this way, we obtain a long sequence

$$(a_1,a_2,\ldots,a_s,a_1+b,\ a_2+b,\ldots,a_s+b,\ldots,\\ a_1+tb,a_2+tb,\ldots,a_{i_0}+tb)$$

for some $1\leqslant i_0\leqslant s$, which is usually the desired splitting sequence. We note that $\{0,b,2b,\ldots,tb\}$ need not form a subgroup of $\mathbb{Z}_g$.

Since the operation described above repeats throughout our construction, we introduce the following succinct notation. Let $\mathbf{a}=(a_1,a_2,\ldots,a_n)\in\mathbb{Z}_g^n$ and $\mathbf{b}=(b_1,b_2,\ldots,b_m)\in\mathbb{Z}_g^m$ be two vectors, not necessarily of the same length. We define

$$\begin{aligned}\mathbf{a}\boxplus\mathbf{b}&\triangleq\mathbf{1}_m\otimes\mathbf{a}+\mathbf{b}\otimes\mathbf{1}_n\\&=(a_1+b_1,a_2+b_1,\ldots,a_n+b_1,a_1+b_2,a_2+b_2,\ldots,\\&\quad a_n+b_2,\ldots,a_1+b_m,a_2+b_m,\ldots,a_n+b_m),\end{aligned}$$

where $\otimes$ denotes the Kronecker product, and $\mathbf{1}_\ell$ denotes a row vector of all ones with length ℓ. If we wish to keep only the first ℓ entries of $\mathbf{a}\boxplus\mathbf{b}$ we shall use the notation we have already defined, $(\mathbf{a}\boxplus\mathbf{b})[1,\ell]$.

We first give our constructions in the case of non-cyclic bursts. In this case, we have $|\mathcal{E}(n,2,1,0)|=2n$, and we are going to split the group $\mathbb{Z}_{2n}$ by $\mathcal{E}(n,2,1,0)$.

Theorem 5: Let $n\geqslant 2$. Then $\mathbb{Z}^n$ can be lattice tiled by $\mathcal{E}(n,2,1,0)$. Namely, there exists a perfect lattice code in $\mathbb{Z}^n$ which can correct a single non-cyclic 2-burst of $(1,0)$-limited-magnitude errors.

Proof: The proof proceeds by considering the following three cases.

Case 1: Assume $n=2m+1$ where $m\geqslant 1$ is an integer. Working in the group $G=\mathbb{Z}_{4m+2}$, let us define

$$\mathbf{s}\triangleq(1,3,5,\ldots,4m-1,4m+1).$$

Note that

$$\{\mathbf{s}[i]\mid 1\leqslant i\leqslant n\}=\{1,3,5,\ldots,4m+1\}$$

and

$$\{\mathbf{s}[i]+\mathbf{s}[i+1]\mid 1\leqslant i\leqslant n-1\}=\{2,4,6,\ldots,4m\}.$$

Thus, G is split by $\mathcal{E}(n,2,1,0)$ with $\mathbf{s}$.

Case 2: Assume $n=2m$ where $m\geqslant 1$ is even. This time we work in $G=\mathbb{Z}_{4m}$, and we define

$$\begin{aligned}\mathbf{s}&\triangleq(m+1,3m+1)\boxplus(0,2,4,\ldots,2(m-1))\\&=(m+1,3m+1,m+3,3m+3,\ldots,m+1+2(m-1)\\&=3m-1,3m+1+2(m-1)=m-1).\end{aligned}$$

Then

$$\begin{aligned}&\{\mathbf{s}[i]\mid 1\leqslant i\leqslant n\}\\&=\{m+1,m+3,\ldots,3m-1,3m+1,3m+3,\ldots,m-1\}\\&=\{1,3,5,\ldots,4m-1\}\end{aligned}$$

and

$$\{\mathbf{s}[i]+\mathbf{s}[i+1]\mid 1\leqslant i\leqslant n-1\}=\{2,4,6,\ldots,4m-2\}.$$

It follows that G is split by $\mathcal{E}(n,2,1,0)$ with $\mathbf{s}$.

Case 3: Assume $n=2m$ where $m\geqslant 1$ is odd. We again work in $G=\mathbb{Z}_{4m}$, but this time the splitting is more involved. For $m=1$, it is easily seen that $\mathbb{Z}_4$ is split by $\mathcal{E}(2,2,1,0)$ with the splitting sequence $(1,2)$. For $m\geqslant 3$, consider the following sequences

$$\begin{aligned}\mathbf{s}_1&\triangleq(1,3,5,\ldots,2m-3),\\\mathbf{s}_2&\triangleq(2m+1,2m+5,2m+9,\ldots,4m-1),\\\mathbf{s}_3&\triangleq(4m-3,4m-7,4m-11,\ldots,2m-1).\end{aligned}$$

Denote

$$\mathbf{s}\triangleq\mathbf{s}_1\mathbf{s}_2\mathbf{s}_3.$$

Then $\mathbf{s}$ has length $n=2m$ and

$$\{\mathbf{s}[i]\mid 1\leqslant i\leqslant 2m\}=\{1,3,5,\ldots,4m-1\}.$$

We have that

$$\begin{aligned}&\{\mathbf{s}_1[i]+\mathbf{s}_1[i+1]\mid 1\leqslant i\leqslant m-2\}\\&=\{4,8,12,\ldots,4m-8\},\\&\{\mathbf{s}_2[i]+\mathbf{s}_2[i+1]\mid 1\leqslant i\leqslant\frac{m-1}{2}\}\\&=\{6,14,22,\ldots,4m-6\},\\&\{\mathbf{s}_3[i]+\mathbf{s}_3[i+1]\mid 1\leqslant i\leqslant\frac{m-1}{2}\}\\&=\{2,10,18,\ldots,4m-10\}.\end{aligned}$$

Additionally,

$$\begin{aligned}\mathbf{s}_1[m-1]+\mathbf{s}_2[1]&=2m-3+2m+1=4m-2\\\mathbf{s}_2\left[\frac{m+1}{2}\right]+\mathbf{s}_3[1]&=4m-1+4m-3=4m-4.\end{aligned}$$

So,

$$\{\mathbf{s}[i]+\mathbf{s}[i+1]\mid 1\leqslant i\leqslant 2m-1\}=\{2,4,\ldots,4m-2\}.$$

Thus, G is split by $\mathcal{E}(n,2,1,0)$ with $\mathbf{s}$. ∎

We now move to the case of cyclic bursts. In this case, we have $|\mathcal{E}^\circ(n,2,1,0)|=2n+1$, and so we consider the group $\mathbb{Z}_{2n+1}$.

Theorem 6: Let $n\geqslant 4$ be a positive integer such that $n\equiv 1 \pmod 3$. Then $\mathbb{Z}^n$ can be lattice tiled by $\mathcal{E}^\circ(n,2,1,0)$.

Namely, there exists a perfect lattice code in $\mathbb{Z}^n$ which can correct a single cyclic 2-burst of $(1,0)$-limited-magnitude errors.

Proof: We divide our proof depending on the residue n leaves modulo 6.

Case 1: Assume that $n = 6m+1$, $m \geqslant 1$. We work in the group $G = \mathbb{Z}_{12m+3}$ and show that it can be split by $\mathcal{E}^\circ(n,2,1,0)$. Let

$$\begin{array}{lll} a = 3m+1, & b = 3m+2, & c = 6m+2, \\ d = 6m+4, & e = 2, & f = 9m+5, \end{array}$$

and define

$$\begin{aligned} \mathbf{s} &\triangleq ((a,b,c,d,e,f) \boxplus (0,3,6,\ldots,3m))[1,n] \\ &= (a,b,\ldots,f,a+3,b+3,\ldots,f+3,\ldots,a+3(m-1), \\ &\quad b+3(m-1),\ldots,f+3(m-1),a+3m). \end{aligned}$$

We now observe that

$$\begin{aligned} &\{a+3i \mid 0 \leqslant i \leqslant m\} \cup \left(\bigcup_{i=0}^{m-1} \{d+3i, b+c+6i, e+f+6i\} \right) \\ &= \{1,4,7,\ldots,12m+1\}, \\ &\left(\bigcup_{i=0}^{m-1} \{b+3i, c+3i, e+3i, f+3i\} \right) \cup \{2a+3m\} \\ &= \{2,5,8,\ldots,12m+2\}, \\ &\bigcup_{i=0}^{m-1} \{a+b+6i, c+d+6i, d+e+6i, f+a+3+6i\} \\ &= \{3,6,9,\ldots,12m\}. \end{aligned}$$

Hence, G is split by $\mathcal{E}^\circ(n,2,1,0)$ with $\mathbf{s}$.

Case 2: Assume that $n = 6m+4$. We now work in the group $G = \mathbb{Z}_{12m+9}$ and show that it can be split by $\mathcal{E}^\circ(n,2,1,0)$. For $m = 0$, it is easily seen that $\mathbb{Z}_9$ is split by $\mathcal{E}^\circ(4,2,1,0)$ with the splitting sequence $(1,3,2,6)$. For $m \geqslant 1$, let

$$\begin{array}{lll} a = 1, & b = 9m+10, & c = 3m+2, \\ d = 3m+7, & e = 6m+7, & f = 6m+8, \end{array}$$

and define

$$\begin{aligned} \mathbf{s}_1 &\triangleq (a,b,c,d,e,f) \boxplus (0,3,6,\ldots,3(m-1)) \\ &= (a,b,\ldots,f,a+3,b+3,\ldots,f+3,\ldots,a+3(m-1), \\ &\quad b+3(m-1),\ldots,f+3(m-1)), \\ \mathbf{s}_2 &\triangleq (6m+5, 12m+6, 6m+6, 9m+7). \end{aligned}$$

Define $\mathbf{s}$ to be the concatenation of $\mathbf{s}_1$ and $\mathbf{s}_2$, i.e.,

$$\mathbf{s} \triangleq \mathbf{s}_1 \mathbf{s}_2.$$

Note that

$$\begin{aligned} &\bigcup_{i=0}^{m-1} \{a+3i, b+3i, d+3i, e+3i\} \\ &= \{1,4,7,\ldots,12m+7\} \setminus \{3m+1, 3m+4, 9m+7\}, \\ &\bigcup_{i=0}^{m-1} \{c+3i, f+3i, a+b+6i, d+e+6i\} \\ &= \{2,5,8,\ldots,12m+8\} \setminus \{6m+2, 6m+5, 9m+8\}, \end{aligned}$$

and

$$\begin{aligned} &\left(\bigcup_{i=0}^{m-1} \{b+c+6i, c+d+6i, e+f+6i\} \right) \\ &\quad \bigcup \{f+a+3+6i \mid 0 \leqslant i \leqslant m-2\} \\ &= \{3,6,9,\ldots,12m+3\} \setminus \{6m+3, 6m+6\}. \end{aligned}$$

Furthermore, we have

$$\{\mathbf{s}_2[i] \mid 1 \leqslant i \leqslant 4\} = \{6m+5, 12m+6, 6m+6, 9m+7\}$$

and

$$\begin{aligned} &\{f+3(m-1)+\mathbf{s}_2[1], \mathbf{s}_2[1]+\mathbf{s}_2[2], \mathbf{s}_2[2]+\mathbf{s}_2[3], \\ &\quad \mathbf{s}_2[3]+\mathbf{s}_2[4], \mathbf{s}_2[4]+a\} \\ &= \{3m+1, 6m+2, 6m+3, 3m+4, 9m+8\}. \end{aligned}$$

Hence, G is split by $\mathcal{E}^\circ(n,2,1,0)$ with $\mathbf{s}$. ■

IV. Perfect $\leqslant$ 3-Cyclic-Burst-Correcting Codes for $(1,1)$ and $(1,0)$-Limited-Magnitude Errors

In this section, we present a construction for the splitting of the additive group of $\mathbb{F}_q$ by $\mathcal{E}^\circ(n,t,k_+,k_-)$. Thus, throughout this section, we let G be the additive group of $\mathbb{F}_q$. This is in contrast with the previous section, where we split only cyclic groups. Denote

$$e \triangleq (k_+ + k_-)(k_+ + k_- + 1)^{b-1}. \tag{3}$$

Let q be a prime power such that $e | q-1$, and denote

$$n \triangleq (q-1)/e. \tag{4}$$

Then

$$|\mathcal{E}^\circ(n,b,k_+,k_-)| = en + 1 = q. \tag{5}$$

Let $\alpha \in \mathbb{F}_q^*$ be a primitive element. For any $z \in \mathbb{F}_q^*$, we use $\log_\alpha(z)$ to denote the unique integer $a \in [0, q-2]$ such that $z = \alpha^a$.

The splitting sequence we shall use most in this section is defined as

$$\mathbf{s}_\alpha \triangleq (\alpha^0, \alpha^e, \alpha^{2e}, \ldots, \alpha^{(n-1)e}).$$

We also define

$$\begin{aligned} \mathcal{F}_b^{k_+,k_-} \triangleq \{&(1, x^e, \ldots, x^{(b-1)e}) \cdot \mathbf{c} \mid \mathbf{c} = (c_0, c_1, \ldots, c_{b-1}) \in \\ &[-k_-, k_+]^b \text{ and } c_0 \neq 0\}. \end{aligned} \tag{6}$$

Hence, $\mathcal{F}_b^{k_+,k_-}$ is a set containing e distinct polynomials. The following proposition provides sufficient conditions on α such that the group G can be split by $\mathcal{E}^\circ(n,b,k_+,k_-)$ with $\mathbf{s}_\alpha$.

Proposition 7: Assume the setting above, and $n \geqslant 2b-1$. Let α be a primitive element of $\mathbb{F}_q^*$, and assume $f(\alpha) \neq 0$ for all $f(x) \in \mathcal{F}_b^{k_+,k_-}$. If

$$\{\log_\alpha(f(\alpha)) \bmod e \mid f(x) \in \mathcal{F}_b^{k_+,k_-}\} = \{0,1,2,\ldots,e-1\}, \tag{7}$$

then $\mathcal{E}^\circ(n,b,k_+,k_-)$ splits G (the additive group of $\mathbb{F}_q$) with the splitting sequence $\mathbf{s}_\alpha$.

Proof: For each vector $\mathbf{c} = (c_0, c_1, \ldots, c_{b-1}) \in [-k_-, k_+]^b$, let

$$\mathcal{E}^\circ_{\mathbf{c}} \triangleq \{\mathbf{e} = (e_0, e_1, \ldots, e_{n-1}) \in \mathcal{E}^\circ(n, b, k_+, k_-) \mid \text{ there is an integer } i \text{ such that } \mathbf{e}[i, i+b-1] = \mathbf{c}\},$$

where the indices of $\mathbf{e}$ are taken cyclically, i.e., modulo n. Since $n \geqslant 2b-1$, it follows that $\mathcal{E}^\circ(n, b, k_+, k_-) \setminus \{\mathbf{0}\}$ can be partitioned into $\mathcal{E}^\circ_{\mathbf{c}}$'s, where $\mathbf{c} = (c_0, c_1, \ldots, c_{b-1}) \in [-k_-, k_+]^b$ and $c_0 \neq 0$.

Note that $\alpha^{en} = \alpha^{q-1} = 1$. For each $\ell \in [0, n-1]$, $\mathbf{s}_\alpha[\ell, \ell+b-1] = (\alpha^{\ell e}, \alpha^{(\ell+1)e}, \ldots, \alpha^{(\ell+b-1)e})$, where the indices of $\mathbf{s}_\alpha$ are modulo n. Hence,

$$\begin{aligned}
&\{\mathbf{e} \cdot \mathbf{s}_\alpha \mid \mathbf{e} \in \mathcal{E}^\circ_{\mathbf{c}}\} \\
&= \{\mathbf{c} \cdot \mathbf{s}_\alpha[\ell, \ell+b-1] \mid \ell \in [0, n-1]\} \\
&= \{\alpha^{e\ell}(c_0 + c_1\alpha^e + \cdots + c_{b-1}\alpha^{(b-1)e}) \mid \ell \in [0, n-1]\} \\
&= \{\alpha^{e\ell+a} \mid \ell \in [0, n-1]\},
\end{aligned}$$

where $a = \log_\alpha(c_0 + c_1\alpha^e + c_2\alpha^{2e} + \cdots + c_{b-1}\alpha^{(b-1)e})$.

Since (7) holds, the collection of sets of the form $\{\mathbf{e} \cdot \mathbf{s}_\alpha; \mathbf{e} \in \mathcal{E}^\circ_{\mathbf{c}}\}$, where $\mathbf{c} \in [-k_-, k_+]^b$ with $c_0 \neq 0$, are exactly the e cosets of the multiplicative subgroup $\langle \alpha^e \rangle$ in $\mathbb{F}_q^*$. It then follows that

$$\begin{aligned}
&\{\mathbf{e} \cdot \mathbf{s}_\alpha \mid \mathbf{e} \in \mathcal{E}^\circ(n, b, k_+, k_-)\} \\
&= \{0\} \cup \left(\bigcup_{\substack{\mathbf{c} \in [-k_-, k_+]^b \\ c_0 \neq 0}} \{\mathbf{e} \cdot \mathbf{s}_\alpha; \mathbf{e} \in \mathcal{E}^\circ_{\mathbf{c}}\} \right) = \mathbb{F}_q.
\end{aligned}$$

Hence, in conjunction with (5), $\mathcal{E}^\circ(n, b, k_+, k_-)$ splits G with $\mathbf{s}_\alpha$. ∎

If we find an α satisfying condition (7), then, according to Theorem 3, the splitting in Proposition 7 yields a lattice tiling of $\mathbb{Z}^n$ by $\mathcal{E}^\circ(n, b, k_+, k_-)$, or equivalently, a perfect lattice code which can correct a cyclic b-burst of (k_+, k_-)-limited-magnitude errors. Furthermore, noting that $(x_0, x_1, \ldots, x_{n-1}) \cdot \mathbf{s}_\alpha = 0$ implies that $(x_{n-1}, x_0, \ldots, x_{n-2}) \cdot \mathbf{s}_\alpha = \alpha^e \cdot ((x_0, x_1, \ldots, x_{n-1}) \cdot \mathbf{s}_\alpha) = 0$, the code itself is cyclic.

Let us start examining specific values of the code parameters. When $b = 2$ and $(k_+, k_-) = (1, 0)$, we have $e = 2$ and $q = en + 1$ is odd. As we shall soon observe and use, the sufficient condition (7) is reduced to that of $1 + \alpha^2$ being a quadratic non-residue in $\mathbb{F}_q$. Since any primitive element of $\mathbb{F}_q$, $q \geqslant 3$, is always a quadratic non-residue, the following result can be used for our construction.

Lemma 8 ([4, Theorem 1]): Let q be an odd prime power which does not belong to the following set:

$$E \triangleq \{3, 5, 7, 9, 11, 13, 19, 23, 25, 29, 31, 37, 41, 43, 49, 61, 67, 71, 73, 79, 121, 127, 151, 211\}. \tag{8}$$

Then there is a primitive element $\alpha \in \mathbb{F}_q$ such that $1 + \alpha^2$ is also a primitive element of $\mathbb{F}_q$.

Theorem 9: Let $q \geqslant 7$ be an odd prime power, and let $n = (q-1)/2$. Then there is a perfect lattice code of $\mathbb{Z}^n$ which can correct a single cyclic 2-burst of $(1, 0)$-limited-magnitude errors.

Proof: For $q = 7$, let $G = \mathbb{Z}_7$ and $\mathbf{s} = (1, 2, 4)$. Then $|G| = |\mathcal{E}^\circ(3, 2, 1, 0)|$ and G is split by $\mathcal{E}^\circ(3, 2, 1, 0)$ with $\mathbf{s}$. According to Theorem 3, there is a lattice tiling of $\mathbb{Z}^3$ by $\mathcal{E}^\circ(3, 2, 1, 0)$. Since $n = 3$, any two errors can be treated as a cyclic burst of length 2. So, this specific case is a perfect tiling with a chair [6].

For $q \geqslant 9$, let G be the additive group of $\mathbb{F}_q$. With the parameters in the hypothesis of this theorem, we have

$$\mathcal{F}_2^{1,0} = \{1, 1 + x^2\}.$$

We would like to use Proposition 7 to construct the splitting. With regard to (7), since $\log_\alpha(1) = 0$, we need $\log_\alpha(1 + \alpha^2) \equiv 1 \pmod 2$. We contend that it suffices to require that $1 + \alpha^2$ is a quadratic non-residue. In this case, assume to the contrary that $\log_\alpha(1 + \alpha^2) \equiv 0 \pmod 2$, since $q - 1$ is even, $\log_\alpha(1 + \alpha^2) \equiv 2m \pmod{q-1}$ for some integer m. Then $1 + \alpha^2 = \alpha^{2m} = (\alpha^m)^2$, which is a quadratic residue, a contradiction.

If $q \notin E$ of (8), then Lemma 8 shows that there is a primitive α such that $1 + \alpha^2$ is also primitive, and hence, $1 + \alpha^2$ is a quadratic non-residue. If $q \in E$ and $q \geqslant 9$, a computer search shows that there is a primitive element $\alpha \in \mathbb{F}_q$ with $1 + \alpha^2$ being a quadratic non-residue. According to Proposition 7, $\mathcal{E}^\circ(n, 2, 1, 0)$ splits G with $\mathbf{s}_\alpha$. The conclusion then follows from Theorem 3 and the fact that $|G| = |\mathcal{E}^\circ(n, 2, 1, 0)|$. ∎

We note that both Theorem 6 and Theorem 9 concern the tiling of the ball $\mathcal{E}^\circ(n, 2, 1, 0)$, but in different regimes. In Theorem 9 the size $|\mathcal{E}^\circ(n, 2, 1, 0)|$ is q, a prime power, while in Theorem 6 the size $|\mathcal{E}^\circ(n, 2, 1, 0)|$ is divisible by 3.

For the other cases, we adapt the approach in [2] to show the existence of α which satisfies condition (7). Recall that a *multiplicative character* of $\mathbb{F}_q^*$ is a group homomorphism $\chi : \mathbb{F}_q^* \to \mathbb{C}$, where for all $\beta, \gamma \in \mathbb{F}_q^*$ we have $\chi(\beta\gamma) = \chi(\beta)\chi(\gamma)$. For example, $\chi(\alpha^i) = e^{2\pi i/(q-1)}$, where α is a primitive element of $\mathbb{F}_q$, defines a multiplicative character of $\mathbb{F}_q^*$. We use $\chi^i(\beta) = (\chi(\beta))^i$ to avoid awkward parentheses, hence the superscript i denotes taking the ith power of $\chi(\beta)$ and not function composition. We say that χ has order i if i is the minimal positive integer such that $\chi^i(\beta) = 1$ for all $\beta \in \mathbb{F}_q^*$. Thus, the order of χ divides $q - 1$. Let χ_i denote an arbitrary multiplicative character of order i. In particular, χ_1 is the function sending all the elements of $\mathbb{F}_q^*$ to 1. It is convenient to extend the definition by letting $\chi(0) = 0$ for all characters. We also recall the definition of the Möbius function, $\mu : \mathbb{N} \to \{-1, 0, 1\}$. If $n \in \mathbb{N}$ is a natural number, $n = \prod_{i=1}^s p_i^{m_i}$, where $m_i \in \mathbb{N}$ and the p_i are distinct primes, then

$$\mu(n) = \begin{cases} 0 & m_i \geqslant 2 \text{ for some } i, \\ (-1)^s & \text{otherwise.} \end{cases}$$

The following sequence of lemmas will help us establish the existence of perfect codes.

Lemma 10 ([7, Lemma 4]): For all $\alpha \in \mathbb{F}_q^*$ we define

$$\psi(\alpha) \triangleq \sum_{k \mid q-1} \frac{\mu(k)}{k} \sum_{\chi^k = \chi_1} \chi(\alpha), \tag{9}$$

where μ is the Möbius function, and the inner summation runs over all characters χ whose k-th power is the identity. Then

$$\psi(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is primitive,} \\ 0 & \text{otherwise.} \end{cases}$$

In the following we also use the convention that $0^0 = 0$ to simplify derivations.

Lemma 11: Let ψ be defined as in (9). Furthermore, let $\mathcal{F} = \{f_1, f_2, \ldots, f_M\} \subseteq \mathbb{F}_q[x]$ be a collection of polynomials over $\mathbb{F}_q$, and let h be an integer such that $h|q-1$. For any $\alpha \in \mathbb{F}_q^*$ we define

$$\Theta(\alpha) \triangleq \psi(\alpha) \prod_{i=1}^{M} \sum_{j=0}^{h-1} \chi_h^j(\alpha^{-\ell_i} f_i(\alpha)), \tag{10}$$

where $\ell_i \in \mathbb{Z}$ for all i. Then

$$\Theta(\alpha) = \begin{cases} h^M & \text{if } \alpha \text{ is primitive and for all } 1 \leqslant i \leqslant M, \\ & f_i(\alpha) \neq 0 \text{ and } \log_\alpha(f_i(\alpha)) \equiv \ell_i \bmod h; \\ 0 & \text{otherwise.} \end{cases}$$

Proof: If α is not primitive, then by Lemma 10, $\psi(\alpha) = 0$, and therefore also $\Theta(\alpha) = 0$. If $f_i(\alpha) = 0$ for some i, then again, $\Theta(\alpha) = 0$. We are therefore left with the case that α is primitive, and $f_i(\alpha) \neq 0$ for all i. Let $\gamma \in \mathbb{F}_q^*$, and assume $\log_\alpha(\gamma) = m$. Then

$$\chi_h(\gamma) = \chi_h(\alpha^m) = \chi_h^m(\alpha).$$

Thus, $\chi_h(\gamma) = 1$ if and only if $m = \log_\alpha(\gamma) \equiv 0 \pmod h$. If indeed $\chi_h(\gamma) = 1$, then

$$\sum_{j=0}^{h-1} \chi_h^j(\gamma) = \sum_{j=0}^{h-1} 1 = h.$$

Otherwise, $\chi_h(\gamma) \neq 1$ and we have

$$\sum_{j=0}^{h-1} \chi_h^j(\gamma) = \frac{\chi_h^h(\gamma) - 1}{\chi_h(\gamma) - 1} = 0.$$

Using this observation we note that

$$\sum_{j=0}^{h-1} \chi_h^j(\alpha^{-\ell_i} f_i(\alpha)) = \begin{cases} h & \text{if } \log_\alpha(f_i(\alpha)) \equiv \ell_i \bmod h, \\ 0 & \text{otherwise.} \end{cases}$$

The conclusion now easily follows. ∎

Since we are working with characters, we shall also need a bound on character sums over $\mathbb{F}_q^*$, which can be derived from the Weil bound (see [2]).

Lemma 12 [2]: Let χ be a multiplicative character of order $m > 1$, and let $f \in \mathbb{F}_q[x]$ be a polynomial that cannot be written as $c \cdot (g(x))^m$ with $c \in \mathbb{F}_q$ and $g(x) \in \mathbb{F}_q[x]$. Let N_f be the number of distinct roots of f in its splitting field. Then for every $a \in \mathbb{F}_q$ we have

$$\left| \sum_{x \in \mathbb{F}_q^*} \chi(af(x)) \right| \leqslant N_f \sqrt{q}.$$

For the next lemma we recall the definitions of Euler's function $\phi(n)$ and the divisor function $d(n)$, for all $n \in \mathbb{N}$,

$$\phi(n) \triangleq |\{1 \leqslant i \leqslant n \mid \gcd(i,n) = 1\}|,$$
$$d(n) \triangleq \sum_{i|n} 1.$$

Lemma 13: Consider the setting of Lemma 11. Suppose that for any $(i_1, i_2, \ldots, i_M) \in [0, h-1]^M \setminus \{(0,0,\ldots,0)\}$, the polynomial $\prod_{t=1}^{M} (f_t(x))^{(q-1)i_t/h}$ cannot be written in the form $c \cdot (g(x))^{q-1}$, where $c \in \mathbb{F}_q$ and $g(x) \in \mathbb{F}_q[x]$. Then

$$\left| \sum_{\alpha \in \mathbb{F}_q^*} \Theta(\alpha) - \phi(q-1) \right| \leqslant A \cdot d(q-1) \cdot \sqrt{q},$$

where ϕ is the Euler function, d is the divisor function, and A is a real number that is independent of q.

Proof: From (10), if $f_t(\alpha) \neq 0$ for all $1 \leqslant t \leqslant M$, then let us write $\Theta(\alpha) = \psi(\alpha) + R(\alpha)$, where

$$R(\alpha) = \psi(\alpha) \sum_{\substack{(i_1,i_2,\ldots,i_M) \in [0,h-1]^M \\ (i_1,i_2,\ldots,i_M) \neq (0,0,\ldots,0)}} \chi_h^{i_1}(\alpha^{-\ell_1} f_1(\alpha)) \cdots \chi_h^{i_M}(\alpha^{-\ell_M} f_M(\alpha)). \tag{11}$$

Otherwise, if $f_t(\alpha) = 0$ for some $1 \leqslant t \leqslant M$, then $\Theta(\alpha) = 0 = R(\alpha)$. By Lemma 10,

$$\sum_{\alpha \in \mathbb{F}_q^*} \psi(\alpha) = \phi(q-1).$$

Thus, summing over all $\alpha \in \mathbb{F}_q^*$, we get

$$\begin{aligned} \phi(q-1) - \sum_{t=1}^{M} \deg(f_t) + \sum_{\alpha \in \mathbb{F}_q^*} R(\alpha) \\ \leqslant \sum_{\alpha \in \mathbb{F}_q^*} \Theta(\alpha) \leqslant \phi(q-1) + \sum_{\alpha \in \mathbb{F}_q^*} R(\alpha). \end{aligned} \tag{12}$$

Note that $\sum_{t=1}^{M} \deg(f_t)$ is independent of q. In the following, we shall give an upper bound on $\left| \sum_{\alpha \in \mathbb{F}_q^*} R(\alpha) \right|$.

Let us observe a typical term in the sum on the right-hand side of (11). From (9), we have

$$\psi(\alpha)\chi_h^{i_1}(\alpha^{-\ell_1} f_1(\alpha)) \cdots \chi_h^{i_M}(\alpha^{-\ell_M} f_M(\alpha)) = \sum_{k|q-1} \frac{\mu(k)}{k} \sum_{\chi^k = \chi_1} \chi(\alpha)\chi_h^{i_1}(\alpha^{-\ell_1} f_1(\alpha)) \cdots \chi_h^{i_M}(\alpha^{-\ell_M} f_M(\alpha)).$$

In the inner sum, $\chi = \chi_j$ for some $j|k$. Hence

$$\chi_j(\alpha)\chi_h^{i_1}(\alpha^{-\ell_1} f_1(\alpha)) \cdots \chi_h^{i_M}(\alpha^{-\ell_M} f_M(\alpha)) = \chi_{q-1}(\alpha^L w(\alpha))$$

where

$$L = (q-1)\left(\frac{1}{j} - \frac{1}{h}(i_1\ell_1 + \cdots + i_M\ell_M)\right)$$

and

$$w(x) = \prod_{t=1}^{M} (f_t(x))^{(q-1)i_t/h}.$$

We notice that $w(x)$ has at most $\sum_{t=1}^{M} \deg f_t$ distinct roots in its splitting field. Due to the assumption, we can apply

Lemma 12 to get

$$\left|\sum_{\alpha\in\mathbb{F}_q^*}\chi_j(\alpha)\chi_h^{i_1}(\alpha^{-\ell_1}f_1(\alpha))\cdots\chi_h^{i_M}(\alpha^{-\ell_M}f_M(\alpha))\right| \leqslant \sum_{t=1}^{M}(\deg f_t)\sqrt{q}.$$

Next, we observe that there are exactly k characters χ such that $\chi^k=\chi_1$. Hence,

$$\left|\sum_{\alpha\in\mathbb{F}_q^*}\psi(\alpha)\chi_h^{i_1}(\alpha^{-\ell_1}f_1(\alpha))\cdots\chi_h^{i_M}(\alpha^{-\ell_M}f_M(\alpha))\right| \leqslant \sum_{t=1}^{M}(\deg f_t)d(q-1)\sqrt{q}.$$

It follows that

$$\left|\sum_{\alpha\in\mathbb{F}_q^*}R(\alpha)\right| \leqslant \sum_{t=1}^{M}(h^M-1)(\deg f_t)d(q-1)\sqrt{q}.$$

Finally, using (12), we have

$$\left|\sum_{\alpha\in\mathbb{F}_q^*}\Theta(\alpha)-\phi(q-1)\right| \leqslant \left|\sum_{\alpha\in\mathbb{F}_q^*}R(\alpha)\right|+\sum_{t=1}^{M}\deg f_t \leqslant \sum_{t=1}^{M}h^M(\deg f_t)d(q-1)\sqrt{q}.$$

■

Now, we study the cases $(b,k_-,k_-)\in\{(2,1,1),(3,1,0),(3,1,1)\}$, and use Lemma 13 to show the existence of α which satisfies (7). It is worth noting that when we apply Lemma 13, the collection of polynomials under consideration is not necessarily the set $\mathcal{F}_b^{k_+,k_-}$. We first look at the case of $b=2$ and $(k_+,k_-)=(1,1)$.

Theorem 14: For all sufficiently large prime powers q such that $q\equiv 7 \pmod{12}$, there is a perfect lattice code of $\mathbb{Z}^n$ with $n=(q-1)/6$, which can correct a single cyclic 2-burst of $(1,1)$-limited-magnitude errors.

Proof: Recalling (3), (4), and (6), in this case we have $e=6$, $q\equiv 1 \pmod 6$, and

$$\mathcal{F}_2^{1,1}=\{1,1+x^6,1-x^6,-1,-1+x^6,-1-x^6\}.$$

We label the polynomials in $\mathcal{F}_2^{1,1}$ as $f_0,f_1,\ldots,f_5$, and then (7) becomes

$$\{\log_\alpha(f_i(\alpha)) \bmod 6 \mid 0\leqslant i\leqslant 5\}=\{0,1,\ldots,5\}.$$

Since $q\equiv 1 \pmod 6$, for any primitive α we have

$$\log_\alpha(-1)=(q-1)/2\equiv 0 \pmod 3.$$

Note that

$$\begin{aligned}\log_\alpha(1)&=0,\\ \log_\alpha(-1+\alpha^6)&\equiv\log_\alpha(-1)+\log_\alpha(1-\alpha^6) \pmod 6,\\ \log_\alpha(-1-\alpha^6)&\equiv\log_\alpha(-1)+\log_\alpha(1+\alpha^6) \pmod 6.\end{aligned}$$

Hence, in order to ensure (7), it suffices to require that $q\equiv 7 \pmod{12}$, i.e., $\log_\alpha(-1)\equiv 3 \pmod 6$, and

$$\{\log_\alpha(1+\alpha^6) \bmod 3,\ \log_\alpha(1-\alpha^6) \bmod 3\}=\{1,2\}. \tag{13}$$

We shall use Lemma 13 with $h=3$ to show the existence of α which satisfies (13). Then according to the discussion above and Proposition 7, the additive group of $\mathbb{F}_q$ can be split by $\mathcal{E}^\circ(n,2,1,1)$ with $\mathbf{s}_\alpha$, and so, the perfect 2-burst-correcting code exists.

Consider the collection of polynomials $\mathcal{F}=\{1+x^6,1-x^6\}$. Let $\ell_1=1,\ell_2=2$, and $h=3$. Let Θ be defined as in (10) for $\mathcal{F}$. For each $(i_1,i_2)\in\{0,1,2\}^2\setminus\{(0,0)\}$, let

$$f_{i_1,i_2}(x)\triangleq(1+x^6)^{\frac{(q-1)i_1}{3}}(1-x^6)^{\frac{(q-1)i_2}{3}}.$$

It can be checked that the polynomials $f_{i_1,i_2}(x)$ satisfy the condition in Lemma 13:

1) If $i_2\neq 0$, then $1-x$ is a factor of $f_{i_1,i_2}(x)$. Since $q\equiv 7 \pmod{12}$, we have that $1-x\nmid 1+x^6$, and $\gcd(1-x^6,-6x^5)=1$. Thus, in the factorization of $f_{i_1,i_2}(x)$ to irreducible polynomials, the multiplicity of $1-x$ is $\frac{(q-1)i_2}{3}$, which is not a multiple of $q-1$. It follows that $f_{i_1,i_2}(x)$ cannot be written in the form $c(g(x))^{q-1}$.
2) If $i_2=0$, then $i_1\neq 0$. Since $\gcd(1+x^6,6x^5)=1$, in the factorization of $1+x^6$ to irreducible polynomials, every irreducible factor has multiplicity 1. Thus, $f_{i_1,0}(x)$ cannot be written in the form $c(g(x))^{q-1}$.

Applying Lemma 13, we get

$$\left|\sum_{\alpha\in\mathbb{F}_q^*}\Theta(\alpha)-\phi(q-1)\right|\leqslant Ad(q-1)\sqrt{q},$$

which implies that

$$\sum_{\alpha\in\mathbb{F}_q^*}\Theta(\alpha)\geqslant\phi(q-1)-Ad(q-1)\sqrt{q}.$$

Note that A is independent of q, and for any given small $\varepsilon>0$ we have $\phi(q-1)>q^{1-\varepsilon}$ and $d(q-1)<q^\varepsilon$ for all sufficiently large q (see [13, Theorem 315 and Theorem 327]). Hence, $\sum_{\alpha\in\mathbb{F}_q^*}\Theta(\alpha)>0$, and so, there is an $\alpha\in\mathbb{F}_q^*$ such that $\Theta(\alpha)>0$. According to the definition of Θ, this α is the desired element to satisfy (13). ■

Now, we turn to the case of $b=3$ and $(k_+,k_-)=(1,0)$. This time, using (3), (4), and (6), we have $e=4$, $q\equiv 1 \pmod 4$, and

$$\mathcal{F}_3^{1,0}=\{1,1+x^4,1+x^8,1+x^4+x^8\}.$$

The idea is the same as before. We use Lemma 13 to find a primitive α such that the logarithm of the evaluations of the polynomials in $\mathcal{F}_3^{1,0}$ at α, are different modulo 4. However, here we need to consider two different collections of polynomials when applying Lemma 13, depending on whether q is divisible by 3 or not.

Theorem 15: For all sufficiently large prime powers q such that $q\equiv 1 \pmod 4$, there is a perfect lattice code of $\mathbb{Z}^n$ with

$n = (q-1)/4$, which can correct a single cyclic 3-burst of $(1,0)$-limited-magnitude errors.

Proof: If q is not divisible by 3, consider the collection of polynomials

$$\mathcal{F} = \mathcal{F}_3^{1,0} \setminus \{1\} = \{1+x^4, 1+x^8, 1+x^4+x^8\},$$

as $\log_\alpha(1) = 0$ for all primitive α. Let $h = e = 4$, $\ell_1 = 1$, $\ell_2 = 2$, $\ell_3 = 3$, and let Θ be defined as in (10). Consider $f_{i_1,i_2,i_3}(x) \triangleq (1+x^4)^{\frac{(q-1)i_1}{4}}(1+x^8)^{\frac{(q-1)i_2}{4}}(1+x^4+x^8)^{\frac{(q-1)i_3}{4}}$, where $(i_1,i_2,i_3) \in \{0,1,2,3\}^3 \setminus \{(0,0,0)\}$.

We verify that $f_{i_1,i_2,i_3}(x)$ cannot be written as $c\cdot(h(x))^{q-1}$ for any $c \in \mathbb{F}_q$ and $h(x) \in \mathbb{F}_q[x]$:

1) If $i_1 \neq 0$, let $p(x)$ be an irreducible factor of $1+x^4$ and a be a root of $p(x)$ in its splitting field. Since $\gcd(1+x^4, 4x^3) = 1$, the multiplicity of $p(x)$ in the factorization of $1+x^4$ is 1. Moreover, $p(x)$ does not divide $(1+x^8)(1+x^4+x^8)$ as $(1+a^8)(1+a^4+a^8) = 2 \neq 0$. Hence, in the factorization of $f_{i_1,i_2,i_3}(x)$, the multiplicity of $p(x)$ is $\frac{(q-1)i_1}{4}$, which is not a multiple of $q-1$.
2) If $i_1 = 0$ and $i_2 \neq 0$, let $p(x)$ be an irreducible factor of $1+x^8$. Using the same argument as above, we can show that in the factorization of $f_{0,i_2,i_3}(x)$, the multiplicity of $p(x)$ is $\frac{(q-1)i_2}{4}$, which is not a multiple of $q-1$.
3) If $i_1 = i_2 = 0$ and $i_3 \neq 0$, $f_{0,0,i_3}(x) = (1+x^4+x^8)^{\frac{(q-1)i_3}{4}}$. Note that $2(1+x^4+x^8) = (1+2x^4)(x^4-1) + 3(1+x^4)$. Since q is not divisible by 3 and $\gcd(1+x^4, 1+2x^4) = 1$, we have $\gcd(1+x^4+x^8, 1+2x^4) = 1$, and so, $\gcd(1+x^4+x^8, 4x^3+8x^7) = 1$. Hence, in the factorization of $f_{0,0,i_3}(x)$ every irreducible factor has multiplicity $\frac{(q-1)i_3}{4}$, which is not a multiple of $q-1$.

Then according to Lemma 13, when q is sufficiently large, there is a primitive element α such that the logarithm of the evaluations of the polynomials in $\mathcal{F}_3^{1,0}$ at α, are distinct modulo 4. The conclusion then follows from Proposition 7 and Theorem 3.

If q is divisible by 3, we have $(1+x^4+x^8) = (1-x^4)^2$. Then it suffices to find a primitive element α such that

$$\log_\alpha(1+\alpha^4) \equiv 1 \bmod 4, \log_\alpha(1+\alpha^8) \equiv 3 \bmod 4,$$
$$\log_\alpha(1-\alpha^4) \equiv 1 \bmod 4. \tag{14}$$

Let

$$g_{i_1,i_2,i_3}(x) \triangleq (1+x^4)^{\frac{(q-1)i_1}{4}}(1+x^8)^{\frac{(q-1)i_2}{4}}(1-x^4)^{\frac{(q-1)i_3}{4}},$$

where $(i_1,i_2,i_3) \in \{0,1,2,3\}^3 \setminus \{(0,0,0)\}$. If $i_3 = 0$, then $g_{i_1,i_2,0}(x) = f_{i_1,i_2,0}(x)$, and so, it cannot be written as $c\cdot(h(x))^{q-1}$. If $i_3 \neq 0$, since $1-x \nmid (1+x^4)(1+x^8)$ and $1-x^4 = (1-x)(1+x+x^2+x^3)$, in the factorization of $g_{i_1,i_2,i_3}(x)$ the factor $1-x$ has multiplicity $\frac{(q-1)i_3}{4}$, which is not a multiple of $q-1$. Hence, we can apply Lemma 13 with $\mathcal{F} = \{1+x^4, 1+x^8, 1-x^4\}$ to show the existence of α such that (14) holds, when q is sufficiently large, which completes our proof. ∎

For the case of $b = 3$ and $k_+ = k_- = 1$, we have $e = 18$ and $q \equiv 1 \pmod{18}$. Since $\log_\alpha(-1) = (q-1)/2$ for any primitive element α, we shall assume $q \equiv 19 \bmod 36$ such that $\log_\alpha(-1) \not\equiv \log_\alpha(1) \pmod{18}$.

Theorem 16: For all sufficiently large prime powers q such that $q \equiv 19 \pmod{36}$, there is a perfect lattice code of $\mathbb{Z}^n$ with $n = (q-1)/18$, which can correct a single cyclic 3-burst of $(1,1)$-limited-magnitude errors.

Proof: The proof repeats the same steps taken in the previous two proofs. We therefore briefly sketch its outline. We have $e = 18$ and let

$$f_1(x) = 1+x^e, \qquad f_2(x) = 1-x^e,$$
$$f_3(x) = 1+x^{2e}, \qquad f_4(x) = 1-x^{2e},$$
$$f_5(x) = 1+x^e+x^{2e}, \qquad f_6(x) = 1-x^e+x^{2e},$$
$$f_7(x) = 1+x^e-x^{2e}, \qquad f_8(x) = 1-x^e-x^{2e}.$$

Since $\log_\alpha(-1) \equiv 9 \pmod{18}$ and $f_4(x) = 1-x^{2e} = f_1(x)f_2(x)$, if we can find a primitive α such that

$$\log_\alpha(f_1(\alpha)) \equiv 1 \pmod 9, \quad \log_\alpha(f_2(\alpha)) \equiv 2 \pmod 9,$$
$$\log_\alpha(f_3(\alpha)) \equiv 6 \pmod 9, \quad \log_\alpha(f_5(\alpha)) \equiv 5 \pmod 9,$$
$$\log_\alpha(f_6(\alpha)) \equiv 7 \pmod 9, \quad \log_\alpha(f_7(\alpha)) \equiv 4 \pmod 9,$$
$$\log_\alpha(f_8(\alpha)) \equiv 8 \pmod 9,$$

then (7) holds.

We set $h = 9$. If q is not divisible by 5, it is verifiable that the set of polynomials $\{f_i \mid 1 \leqslant i \leqslant 8, i \neq 4\}$ satisfies the condition of Lemma 13. Thus, when q is large enough, such an α exists.

If q is divisible by 5, then

$$f_3(x) = 1+x^{2e} = (x^e+2)(x^e-2),$$
$$f_7(x) = 1+x^e-x^{2e} = -(x^e+2)^2,$$
$$f_8(x) = 1-x^e+x^2e = -(x^e-2)^2.$$

Let $f_9(x) = x^e+2$ and $f_{10}(x) = x^e-2$. Then the set of polynomials $\{f_1, f_2, f_5, f_6, f_9, f_{10}\}$ satisfies the condition of Lemma 13. Therefore, when q is large enough, there is a primitive element α such that

$$\log_\alpha(f_1(\alpha)) \equiv 1 \pmod 9, \quad \log_\alpha(f_2(\alpha)) \equiv 2 \pmod 9,$$
$$\log_\alpha(f_5(\alpha)) \equiv 5 \pmod 9, \quad \log_\alpha(f_6(\alpha)) \equiv 7 \pmod 9,$$
$$\log_\alpha(f_9(\alpha)) \equiv 2 \pmod 9, \quad \log_\alpha(f_{10}(\alpha)) \equiv 4 \pmod 9.$$

It then follows that

$$\log_\alpha(f_3(\alpha)) \equiv 6 \pmod 9, \quad \log_\alpha(f_4(\alpha)) \equiv 3 \pmod 9,$$
$$\log_\alpha(f_7(\alpha)) \equiv 4 \pmod 9, \quad \log_\alpha(f_8(\alpha)) \equiv 8 \pmod 9.$$

Hence, α is the desired primitive element. ∎

A. Modification of the Constructions

Theorem 14 shows the existence of lattice tilings of $\mathcal{E}^\circ(n,2,1,1)$ when $q \equiv 7 \pmod{12}$, whereas the necessary condition on q is only $q \equiv 1 \pmod 6$. Thus, the existence of such tilings when $q \equiv 1 \pmod{12}$ remains undecided. In the following, we solve half of the remaining cases. We assume that $q = 12m+1$ with m odd, and show that a different splitting sequence provides a tiling. The following proposition is the equivalent of Proposition 7.

Proposition 17: Assume $n \geqslant 3$, $q = 12m+1$, m odd, and define

$$\mathbf{r}_\alpha \triangleq (1, \alpha^3, \alpha^{12}, \alpha^{15}, \ldots, \alpha^{12(m-1)}, \alpha^{12(m-1)+3}),$$
$$\mathcal{F} \triangleq \{\pm 1, \pm x^3, \pm(1+x^3), \pm(1-x^3), \pm(x^3+x^{12}), \pm(x^3-x^{12})\}.$$

Let α be a primitive element of $\mathbb{F}_q^*$, and assume $f(\alpha) \neq 0$ for all $f(x) \in \mathcal{F}$. If

$$\{\log_\alpha(f(\alpha)) \bmod 12 \mid f(x) \in \mathcal{F}\} = \{0, 1, 2, \ldots, 11\}, \quad (15)$$

then $\mathcal{E}^\circ(n, 2, 1, 1)$ splits G (the additive group of $\mathbb{F}_q$) with the splitting sequence $\mathbf{r}_\alpha$.

Proof: For each pair $\mathbf{c} = (c_0, c_1) \in [-1, 1]^2$ with $c_0 \neq 0$, let

$$\mathcal{A}_\mathbf{c} \triangleq \{\mathbf{e} = (e_0, e_1, \ldots, e_{n-1}) \in \mathcal{E}^\circ(n, 2, 1, 1) \mid \text{ there is an } \textit{even} \text{ integer } i \text{ such that } \mathbf{e}[i, i+1] = \mathbf{c}\},$$
$$\mathcal{B}_\mathbf{c} \triangleq \{\mathbf{e} = (e_0, e_1, \ldots, e_{n-1}) \in \mathcal{E}^\circ(n, 2, 1, 1) \mid \text{ there is an } \textit{odd} \text{ integer } i \text{ such that } \mathbf{e}[i, i+1] = \mathbf{c}\},$$

where in both cases, $i+1$ is taken modulo n. Then

$$\{\mathbf{e} \cdot \mathbf{r}_\alpha \mid \mathbf{e} \in \mathcal{A}_\mathbf{c}\} = \{\alpha^{12\ell}(c_0 + c_1\alpha^3) \mid \ell \in [0, m-1]\},$$
$$\{\mathbf{e} \cdot \mathbf{r}_\alpha \mid \mathbf{e} \in \mathcal{B}_\mathbf{c}\} = \{\alpha^{12\ell}(c_0\alpha^3 + c_1\alpha^{12}) \mid \ell \in [0, m-1]\}.$$

Since (15) holds, we have that

$$\begin{aligned}
&\{\mathbf{e} \cdot \mathbf{r}_\alpha \mid \mathbf{e} \in \mathcal{E}^\circ(n, 2, 1, 1)\} \\
&= \{0\} \cup \left(\bigcup_{\substack{\mathbf{c} \in [-1,1]^2 \\ c_0 \neq 0}} (\{\mathbf{e} \cdot \mathbf{r}_\alpha \mid \mathbf{e} \in \mathcal{A}_\mathbf{c}\} \cup \{\mathbf{e} \cdot \mathbf{r}_\alpha \mid \mathbf{e} \in \mathcal{B}_\mathbf{c}\}) \right) \\
&= \mathbb{F}_q.
\end{aligned}$$

Hence $\mathcal{E}^\circ(n, 2, 1, 1)$ splits G with $\mathbf{r}_\alpha$. ∎

Theorem 18: For all sufficiently large prime powers q such that $q \equiv 13 \pmod{24}$, there is a perfect lattice code of $\mathbb{Z}^n$ with $n = (q-1)/6$, which can correct a single cyclic 2-burst of $(1, 1)$-limited-magnitude errors.

Proof: Since $q \equiv 13 \pmod{24}$, $\log_\alpha(-1) = (q-1)/2 \equiv 6 \pmod{12}$. Thus if the logarithms of $1, \alpha^3, 1+\alpha^3, 1-\alpha^3, \alpha^3+\alpha^{12}, \alpha^3-\alpha^{12}$ are distinct modulo 6, then (15) holds. To find such a primitive α, we let $h = 6$ and consider the following set of polynomials

$$\mathcal{F}' \triangleq \{1+x^3, 1-x^3, 1+x^3+x^6, 1-x^3+x^6\}.$$

It is verifiable that these polynomials satisfy the condition in Lemma 13. Hence, if q is large enough, there is a primitive α such that

$$\begin{aligned}
\log_\alpha(1+\alpha^3) &\equiv 1 \bmod 6 \\
\log_\alpha(1-\alpha^3) &\equiv 2 \bmod 6, \\
\log_\alpha(1-\alpha^3+\alpha^6) &\equiv 0 \bmod 6, \\
\log_\alpha(1+\alpha^3+\alpha^6) &\equiv 0 \bmod 6.
\end{aligned}$$

Then it follows that

$$\begin{aligned}
&\log_\alpha(\alpha^3+\alpha^{12}) \\
&\quad \equiv 3 + \log_\alpha(1+\alpha^3) + \log_\alpha(1-\alpha^3+\alpha^6) \equiv 4 \bmod 6, \\
&\log_\alpha(\alpha^3-\alpha^{12}) \\
&\quad \equiv 3 + \log_\alpha(1-\alpha^3) + \log_\alpha(1+\alpha^3+\alpha^6) \equiv 5 \bmod 6.
\end{aligned}$$

Noting that $\log_\alpha(1) = 0$ and $\log_\alpha(\alpha^3) = 3$, we have completed our proof. ∎

TABLE II
VALUES OF q, FROM $e(2b-1)+1$ UP TO 1000, THAT DO NOT ADMIT THE REQUIRED PRIMITIVE ELEMENT

	#Good	#Bad	Bad Prime Powers q
Theorem 14	41	3	$19, 43, 127$
Theorem 18	6	15	$37, 61, 109, 157, 181, 229, 277, 349, 373, 397, 421, 613, 661, 733, 829$
Theorem 15	76	14	$25, 37, 49, 61, 97, 101, 121, 157, 169, 289, 361, 449, 601, 729$
Theorem 16	2	13	$199, 271, 307, 343, 379, 487, 523, 631, 739, 811, 883, 919, 991$

V. DISCUSSION

In this paper we constructed perfect lattice codes that are capable of correcting a single burst of limited-magnitude errors. Our constructions span both the case of cyclic burst errors, as well as non-cyclic bursts. The parameters of the various constructions are summarized in Table I. We note that the first row in this table is obtained by using Theorem 1 to convert the code over $\mathbb{F}_p$ in [11] to a lattice code.

The approach in Section IV was inspired by [2]. This is in particular interesting, since [2] did not study perfect codes. Similar to [2], our constructions in Section IV call for finding a primitive element of $\mathbb{F}_q$ with certain properties. We note that a simple brute-force search can easily find such an element (if it exists) in time polynomial in q, which is also polynomial in n as $n = \Theta(q)$ in all of our constructions. The number-theoretic conditions required by our constructions seem to make it difficult to give an existence guarantee stronger than "sufficiently large q". We ran a computer search, whose results are summarized in Table II. The table count the number of good prime powers (i.e., those that admit a primitive α with the required properties), the number of bad prime powers, and the list of bad prime powers.

We would also like to comment on the prospect of extending our constructions, both for longer bursts, as well as for errors of larger magnitude.

A. Longer Bursts

In Section IV we presented a construction based on finite fields and used it to prove a few existence results for lattice tiling of $\mathcal{E}^\circ(n, t, k_+, k_-)$ with $b \leqslant 3$ and

TABLE III
SPLITTING OF G BY $\mathcal{E}^\circ(n,2,2,0)$ OR $\mathcal{E}(n,2,2,0)$

n	G	The shape	Splitting sequence
3	$\mathbb{Z}_{19}$	$\mathcal{E}^\circ(n,2,2,0)$	$\mathbf{s}=(1,7,11)$
4	$\mathbb{Z}_{25}$	$\mathcal{E}^\circ(n,2,2,0)$	$\mathbf{s}=(1,5,4,20)$
3	$\mathbb{Z}_{15}$	$\mathcal{E}(n,2,2,0)$	$\mathbf{s}=(1,5,4)$
4	$\mathbb{Z}_{21}$	$\mathcal{E}(n,2,2,0)$	$\mathbf{s}=(1,5,20,18)$

TABLE IV
SPLITTING OF $\mathbb{Z}_{6n+1}$ BY $\mathcal{E}^\circ(n,2,1,1)$

n	Splitting sequence
4	$\mathbf{s}=(1,5,2,10)$
5	$\mathbf{s}=(1,4,15,2,8)$
6	$\mathbf{s}=(1,8,10,6,11,14)$
8	$\mathbf{s}=(1,4,21,9,2,18,8,14)$
9	$\mathbf{s}=(1,3,12,25,6,20,27,17,22)$
10	$\mathbf{s}=(1,3,11,24,9,25,30,12,29,22)$
11	$\mathbf{s}=(1,3,9,27,14,25,8,24,5,15,22)$
12	$\mathbf{s}=(1,3,8,27,33,12,30,20,29,7,32,15)$
13	$\mathbf{s}=(1,3,8,14,37,17,10,26,38,9,39,21,34)$
14	$\mathbf{s}=(1,3,8,14,31,7,41,9,21,39,10,23,42,27)$

$(k_+,k_-)\in\{(1,0),(1,1)\}$. This approach may also work for the cases $b>3$. However, it would involve choosing a large number of factors of the polynomials in $\mathcal{F}_b^{k_-,k_-}$, checking whether they satisfy the condition in Lemma 13, and assigning each of them an integer such that (7) holds. Thus, a closed-form solution to all the cases $b>3$ still remains unsolved. We note that a similar problem was considered in [2] for polynomials that satisfy the Abramson-Elspus-Short (AES) conditions, and it was solved by showing that it suffices to consider only irreducible polynomials and assign all of them the same integer zero [2, Theorem 3]. Whether a similar solution exists here is still unknown.

B. Larger Error Magnitudes

In this paper, we studied only the case $k_+=1$. For $k_+\geqslant 2$, finding a lattice tiling becomes more difficult. If one wants to use the construction in Section IV to handle the case of $b=2$ and $(k_+,k_-)=(2,0)$, a primitive element α satisfying the following condition is required:

$$\{\log_\alpha(f_i(\alpha)) \bmod 6 \mid 1\leqslant i\leqslant 5\}=\{1,2,3,4,5\}, \quad (16)$$

where

$$f_1(x)=1+x^6, \quad f_2(x)=1+2x^6, \quad f_3(x)=2,$$
$$f_4(x)=2+x^6, \quad f_5(x)=2+2x^6.$$

Note that unlike $\log_\alpha(1)=0$ and $\log_\alpha(-1)=\frac{q-1}{2}$, the value of $\log_\alpha(2)$ modulo 6 depends on the choice of α. To complicate things further, $f_3(x)=2$ does not satisfy the condition in Lemma 13. Thus, we cannot use it, as is, to find the desired α. A computer search up to 1000 shows that the following field sizes, q,

$$19,79,103,163,181,199,229,349,373,397,421,487,499,$$
$$541,613,619,631,643,691,709,733,739,751,769,787,823,$$
$$853,859,907,967,997$$

admit a primitive α that satisfies (16).

TABLE V
SPLITTING OF $\mathbb{Z}_{6n-3}$ BY $\mathcal{E}(n,2,1,1)$

n	Splitting sequence
3	$\mathbf{s}=(1,5,2)$
4	$\mathbf{s}=(1,4,10,2)$
5	$\mathbf{s}=(1,4,10,2,9)$
6	$\mathbf{s}=(1,14,10,2,5,11)$
7	$\mathbf{s}=(1,3,12,19,6,16,5)$
8	$\mathbf{s}=(1,3,12,20,14,21,5,22)$
9	$\mathbf{s}=(1,3,9,16,5,24,10,23,8)$
10	$\mathbf{s}=(1,3,8,25,13,28,6,20,27,9)$
11	$\mathbf{s}=(1,3,8,29,7,25,15,28,16,30,24)$
12	$\mathbf{s}=(1,3,8,17,32,13,29,7,28,18,12,26)$
13	$\mathbf{s}=(1,3,8,14,32,19,31,16,26,9,30,7,27)$
14	$\mathbf{s}=(1,3,8,14,30,13,40,21,12,35,10,39,24,31)$

We also ran a computer search for splittings by $\mathcal{E}^\circ(n,2,2,0)$ and $\mathcal{E}(n,2,2,0)$. For $n\in\{3,4\}$, existence results are listed in Table III. Interestingly, for each $5\leqslant n\leqslant 11$, every Abelian group G of order $6n+1$ cannot be split by $\mathcal{E}^\circ(n,2,2,0)$, and every Abelian group of order $6n-3$ cannot be split by $\mathcal{E}(n,2,2,0)$. In contrast, for the case of $b=2$ and $(k_+,k_-)=(1,1)$, Table IV shows that $\mathbb{Z}_{6n+1}$ can be split by $\mathcal{E}^\circ(n,2,1,1)$ for each $n\in[4,14]\setminus\{7\}$, and Table V shows that $\mathbb{Z}_{6n-3}$ can be split by $\mathcal{E}(n,2,1,1)$ for each $n\in[3,14]$. Thus, it would be interesting to derive some constraints on the values of n for the existence of lattice tilings of $\mathcal{E}(n,2,2,0)$ and $\mathcal{E}^\circ(n,2,2,0)$.

REFERENCES

[1] K. A. S. Abdel-Ghaffar, "On the existence of optimum cyclic burst correcting codes over $GF(q)$," *IEEE Trans. Inf. Theory*, vol. IT-34, no. 2, pp. 329–332, Mar. 1988.

[2] K. Abdel-Ghaffar, R. McEliece, A. Odlyzko, and H. van Tilborg, "On the existence of optimum cyclic burst- correcting codes," *IEEE Trans. Inf. Theory*, vol. IT-32, no. 6, pp. 768–775, Nov. 1986.

[3] R. Bitar, S. K. Hanna, N. Polyanskii, and I. Vorobyev, "Optimal codes correcting localized deletions," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 1991–1996.

[4] A. R. Booker, S. D. Cohen, N. Sutherland, and T. Trudgian, "Primitive values of quadratic polynomials in a finite field," *Math. Comput.*, vol. 88, no. 318, pp. 1903–1912, Oct. 2018.

[5] B. Bose, N. Elarief, and L. G. Tallini, "On codes achieving zero error capacities in limited magnitude error channels," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 257–273, Jan. 2018.

[6] S. Buzaglo and T. Etzion, "Tilings with n-dimensional chairs and their applications to asymmetric codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 3, pp. 1573–1582, Mar. 2013.

[7] L. Carlitz, "Primitive roots in a finite field," *Trans. Amer. Math. Soc.*, vol. 73, no. 3, pp. 373–382, 1952.

[8] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for asymmetric limited-magnitude errors with applications to multilevel flash memories," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1582–1595, Apr. 2010.
[9] Y. M. Chee, S. Ling, T. T. Nguyen, V. K. Vu, H. Wei, and X. Zhang, "Burst-deletion-correcting codes for permutations and multipermutations," *IEEE Trans. Inf. Theory*, vol. 66, no. 2, pp. 957–969, Feb. 2020.
[10] B. Eitan and A. Roy, "Binary and multilevel flash cells," in *Flash Memories*, P. Cappelletti, C. Golla, P. Olivo, and E. Zanoni, Eds. Alphen aan den Rijn, The Netherlands: Kluwer, 1999, pp. 91–152.
[11] T. Etzion, "Constructions for perfect 2-burst-correcting codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2553–2555, Sep. 2001.
[12] W. Hamaker and S. Stein, "Combinatorial packing of R^3 by certain error spheres," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 2, pp. 364–368, Mar. 1984.
[13] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed. Oxford, U.K.: Oxford Univ. Press, 2008.
[14] D. Hickerson and S. Stein, "Abelian groups and packing by semicrosses," *Pacific J. Math.*, vol. 122, no. 1, pp. 95–109, 1986.
[15] S. Jain, F. Farnoud, M. Schwartz, and J. Bruck, "Coding for optimized writing rate in DNA storage," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 711–716.
[16] T. Kløve, J. Luo, I. Naydenova, and S. Yari, "Some codes correcting asymmetric errors of limited magnitude," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7459–7472, Nov. 2011.
[17] A. V. Kuznetsov and A. J. H. Vinck, "A coding scheme for single peak-shift correction in (d, k)-constrained channels," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1440–1450, Jul. 1993.
[18] A. Lenz and N. Polyanskii, "Optimal codes correcting a burst of deletions of variable length," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020.
[19] V. I. Levenshtein and A. J. H. Vinck, "Perfect (d, k)-codes capable of correcting single peak-shifts," *IEEE Trans. Inform. Theory*, vol. 39, no. 2, pp. 656–662, Mar. 1993.
[20] D. Lind and B. H. Marcus, *An Introduction to Symbolic Dynamics and Coding*. Cambridge, U.K.: Cambridge Univ. Press, 1985.
[21] C. Schoeny, A. Wachter-Zeh, R. Gabrys, and E. Yaakobi, "Codes correcting a burst of deletions or insertions," *IEEE Trans. Inf. Theory*, vol. 63, no. 4, pp. 1971–1985, Apr. 2017.
[22] M. Schwartz, "Quasi-cross lattice tilings with applications to flash memory," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.
[23] M. Schwartz, "On the non-existence of lattice tilings by quasi-crosses," *Eur. J. Combinat.*, vol. 36, pp. 130–142, Feb. 2014.
[24] S. K. Stein, "Factoring by subsets," *Pacific J. Math.*, vol. 22, no. 3, pp. 523–541, 1967.
[25] S. Stein, "Packings of R^n by certain error spheres," *IEEE Trans. Inform. Theory*, vol. IT-30, no. 2, pp. 356–363, Mar. 1984.
[26] S. Stein, "The notched cube tiles $\mathbb{R}^n$," *Discrete Math.*, vol. 80, no. 3, pp. 335–337, Mar. 1990.
[27] S. Stein and S. Szabó, *Algebra Tiling*. Washington, DC, USA: The Mathematical Association of America, 1994.
[28] H. Wei and M. Schwartz, "On tilings of asymmetric limited-magnitude balls," *Eur. J. Combin.*, vol. 100, pp. 1–21, Feb. 2022.
[29] H. Wei, X. Wang, and M. Schwartz, "On lattice packings and coverings of asymmetric limited-magnitude balls," *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5104–5115, Aug. 2021.
[30] S. Yari, T. Kløve, and B. Bose, "Some codes correcting unbalanced errors of limited magnitude for flash memories," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7278–7287, Nov. 2013.
[31] Z. Ye, T. Zhang, X. Zhang, and G. Ge, "Some new results on splitter sets," *IEEE Trans. Inf. Theory*, vol. 66, no. 5, pp. 2765–2776, May 2020.
[32] T. Zhang and G. Ge, "New results on codes correcting single error of limited magnitude for flash memory," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4494–4500, Aug. 2016.
[33] T. Zhang and G. Ge, "On the nonexistence of perfect splitter sets," *IEEE Trans. Inf. Theory*, vol. 64, no. 10, pp. 6561–6566, Oct. 2018.
[34] T. Zhang, X. Zhang, and G. Ge, "Splitter sets and k-radius sequences," *IEEE Trans. Inform. Theory*, vol. 63, no. 12, pp. 7633–7645, Dec. 2017.

Hengjia Wei received the Ph.D. degree in applied mathematics from Zhejiang University, Hangzhou, China, in 2014.

He was a Post-Doctoral Fellow with Capital Normal University, Beijing, China, from 2014 to 2016, a Research Fellow with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, from 2016 to 2019, and a Post-Doctoral Fellow with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel, from 2019 to 2022. He is currently an Associate Researcher with the Peng Cheng Laboratory, Shenzhen, China. His research interests include combinatorial design theory, coding theory, and their intersections. He received the 2017 Kirkman Medal from the Institute of Combinatorics and its Applications.

Moshe Schwartz (Senior Member, IEEE) received the B.A. *(summa cum laude)*, M.Sc., and Ph.D. degrees from the Computer Science Department, Technion—Israel Institute of Technology, Haifa, Israel, in 1997, 1998, and 2004, respectively.

He was a Fulbright Post-Doctoral Researcher with the Department of Electrical and Computer Engineering, University of California San Diego, and a Post-Doctoral Researcher with the Department of Electrical Engineering, California Institute of Technology. While on sabbatical (2012–2014), he was a Visiting Scientist at the Massachusetts Institute of Technology (MIT). He is currently a Professor with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel. His research interests include algebraic coding, combinatorial structures, and digital sequences.

Prof. Schwartz received the 2009 IEEE Communications Society Best Paper Award in Signal Processing and Coding for Data Storage and the 2020 NVMW Persistent Impact Prize. He served as an Associate Editor for Coding Techniques and Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2014 to 2021. Since 2021, he has been serving as an Area Editor for Coding and Decoding for the IEEE TRANSACTIONS ON INFORMATION THEORY. He has also been an Editorial Board Member for the *Journal of Combinatorial Theory Series—A* since 2021.