Perfect Codes Correcting a Single Burst of Limited-Magnitude Errors

Hengjia Wei
Peng Cheng Laboratory
Shenzhen 518000, China
Email: hjwei05@163.com

Moshe Schwartz
Electrical and Computer Engineering
Ben-Gurion University of the Negev,
Beer Sheva 8410501, Israel
schwartz@ee.bgu.ac.il

***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 for $(1,0)$-limited-magnitude errors, 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.**

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 [9] gave a construction for perfect binary 2-burst-correcting codes. As for deletions and insertions, it has been shown in [19] 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 [16], [19], 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 [7].

This paper focuses on the model of *limited-magnitude errors*, which could be found in several applications, including high-density magnetic recording channels [15], [17], flash memories [6], and some DNA-based storage systems [13], [28]. 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], [10], [12], [14], [21], [23]–[25], [28]–[33]. However, the applications which exhibit limited-magnitude errors are prone to errors occurring in a burst. The coding schemes for magnetic recording channels [15], [17], and the DNA-based storage system of [13], 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 [18, Section 5.5]). Similarly, flash memories suffer from inter-cell interference [8], 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], [9], we distinguish between *cyclic bursts* and *non-cyclic bursts*, of limited-magnitude errors. In the examples mentioned here, [1], [2] study cyclic bursts, whereas [9] studies non-cyclic bursts. We follow suit, and study both types of bursts. 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

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

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

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

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

This work was supported in part by the Israel Science Foundation (ISF) under Grant 270/18.

978-1-6654-2159-1/22/$31.00 ©2022 IEEE

which can correct a non-cyclic 2-burst of $(1,0)$-limited-magnitude errors.

2) For each $n \equiv 1,4 \pmod 6$, 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 a primitive element satisfying some conditions. 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 note that all the codes presented in this paper are lattice codes. Due to space limitations, most proofs are omitted. The full proofs, and additional results may be found in the full version [27].

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. It now follows that a perfect code capable of correcting a cyclic burst in our setting is equivalent to a tiling of $\mathbb{Z}^n$ by $\mathcal{E}^\circ(n,b,k_+,k_-)$ defined in (1), and a perfect code capable of correcting a non-cyclic burst in our setting is equivalent to a tiling of $\mathbb{Z}^n$ by $\mathcal{E}(n,b,k_+,k_-)$ 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, we have the notion of lattice tilings. Throughout the paper, we shall only consider lattice codes, since these are easier to analyze, construct, and encode, than non-lattice codes.

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 $\mathcal{E}(n,1,k_+,k_-)$. If we treat each point of $\mathbb{Z}^n$ as a unit cube centered at it, then the shape $\mathcal{E}(n,1,k_+,k_-)$ 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 with these shapes can be traced back to 1960's (e.g., see [22]), and is usually connected with group splitting (e.g., [10], [12], [20], [21], [23]). For an excellent treatment and history, the reader is referred to [25] and the many references therein. More recent results may be found in [30] and the references therein.

To construct codes that correct multiple errors, the notion of group splitting was generalized in [5]. 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 [5], [26]. 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 denote $g+g+\cdots+g$ (with m copies of g) when $m > 0$, which is extended in the natural way to $m \leqslant 0$. 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 1. 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 $\{\mathbf{a} \cdot \mathbf{s} \,|\, \mathbf{a} \in \mathcal{A}\}$ contains $|\mathcal{A}|$ distinct elements of G. This operation is called a *(generalized) splitting*.

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 $\mathcal{A} = \mathcal{E}^\circ(n,b,k_+,k_-)$. The following theorems show the equivalence of lattice tiling of $\mathbb{Z}^n$ and splitting.

Theorem 2 (Lemma 4 and Corollary 1 in [5])**.** *Let $\mathcal{S} \subset \mathbb{Z}^n$ be a finite subset, and G be an Abelian group of order $|\mathcal{S}|$. Assume that $\mathcal{S}$ splits G with a splitting sequence $\mathbf{s}$. Define $\phi : \mathbb{Z}^n \to G$ as $\phi(\mathbf{x}) \triangleq \mathbf{x} \cdot (s_1, \ldots, s_n)$ and let $\Lambda \triangleq \ker\phi$. Then Λ is a lattice tiling of $\mathbb{Z}^n$ with $\mathcal{S}$.*

Theorem 3 (Lemma 3 and Corollary 1 in [5])**.** *Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice tiling of $\mathbb{Z}^n$ with $\mathcal{S} \subset \mathbb{Z}^n$, and assume both $\mathcal{S}$ and G are finite. Define $G \triangleq \mathbb{Z}^n/\Lambda$. Let $\phi : \mathbb{Z}^n \to G$ be the natural homomorphism, namely the one that maps any $\mathbf{x} \in \mathbb{Z}^n$ to the coset of Λ in which it resides. Set $\mathbf{s} \triangleq (\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_n))$, where $\mathbf{e}_i$ is the i-th unit vector in $\mathbb{Z}^n$. Then $\mathcal{S}$ splits G with the splitting sequence $\mathbf{s}$.*

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 [9] 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 ([9]). *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 $\mathcal{E}^\circ(n, b, k_+, k_-)$. These tilings are equivalent to perfect b-burst-correcting codes with respect to limited-magnitude errors, by taking the kernel of the map $\phi(x)$ defined in Theorem 2.

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 $\mathbb{Z}_g$. Using these constructions, together with Theorem 2, 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 $n \equiv 1, 4 \pmod 6$.

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

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

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 the 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 four cases, depending on the residue of n modulo 4. Due to space limitations, we present the first case only.

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

$$\begin{aligned}\mathbf{s} &\triangleq ((m+1, 3m+3) \boxplus (0, 2, 4, \ldots, 2m))[1, n] \\ &= (m+1, 3m+3, m+3, 3m+5, \ldots, \\ &\quad m+1+2(m-1) = 3m-1, \\ &\quad 3m+3+2(m-1) = m-1, m+1+2m = 3m+1).\end{aligned}$$

Note that

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

and

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

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

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 $\mathbb{Z}_{2n+1}$. A similar approach gives the following construction.

Theorem 6. *Let $n \geqslant 4$ be a positive integer such that $n \equiv 1, 4 \pmod 6$. 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.*

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 of this section is defined as

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

We also define

$$\begin{aligned}\mathcal{F}_b^{k_+, k_-} \triangleq \Big\{&(1, x^e, x^{2e}, \ldots, x^{(b-1)e}) \cdot \mathbf{c} \;\Big| \\ &\mathbf{c} = (c_0, c_1, \ldots, c_{b-1}) \in [-k_-, k_+]^b \text{ and } c_0 \neq 0\Big\}.\end{aligned} \tag{6}$$

Hence, $\mathcal{F}_b^{k_+, k_-}$ is a set of e polynomials. The following result shows that by carefully choosing α, 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*

$$\left\{ \log_\alpha(f(\alpha)) \pmod e \;\middle|\; f(x) \in \mathcal{F}_b^{k_+,k_-} \right\} = [0, e-1], \quad (7)$$

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

According to Theorem 2, 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 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. 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:*

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

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 2, there is a lattice tiling of $\mathbb{Z}^3$ by $\mathcal{E}^\circ(3, 2, 1, 0)$. This specific case is in fact a standard 2-error-correcting code, and since $n = 3$, it is a perfect tiling with a chair [5].

For $q \geqslant 9$, let G be the additive group of $\mathbb{F}_q$. With the parameters 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. Since $\log_\alpha(1) = 0$, we need $\log(1 + \alpha^2) \equiv 1 \pmod 2$, namely, that $1 + \alpha^2$ is a quadratic non-residue. 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 for each such q 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 2 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 $\chi : \mathbb{F}_q^* \to \mathbb{C}$, such that for all $\beta, \gamma \in \mathbb{F}_q^*$ we have $\chi(\beta\gamma) = \chi(\beta)\chi(\gamma)$. 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

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

We now define

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

where the inner summation runs over all characters χ whose k-th power is the identity.

Lemma 10. *Assume the setting above. 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*

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

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

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

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

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

Lemma 11. *Consider the setting of Lemma 10. 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 $c \cdot (h(x))^{q-1}$, where $c \in \mathbb{F}_q$ and $h(x) \in \mathbb{F}_q[x]$. 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.

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	[9]	$r \geqslant 4$
2	1	0	$n \geqslant 2$	N	Theorem 5	
2	1	0	$4 \leqslant n \equiv 1, 4 \pmod 6$	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 12	$q \equiv 7 \pmod{12}$ sufficiently large
3	1	0	$n = \frac{q-1}{4}$	Y	Theorem 13	$q \equiv 1 \pmod 4$ sufficiently large
3	1	1	$n = \frac{q-1}{18}$	Y	Theorem 14	$q \equiv 19 \pmod{36}$ sufficiently large

Here is the first result obtained by this method:

Theorem 12. *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

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

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

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

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

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

Note that $\log_\alpha(1) = 0$, and

$$\log_\alpha(-1+\alpha^6) \equiv \log_\alpha(-1) + \log_\alpha(1-\alpha^6) \pmod 6,$$
$$\log_\alpha(-1-\alpha^6) \equiv \log_\alpha(-1) + \log_\alpha(1+\alpha^6) \pmod 6.$$

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

$$\{\log_\alpha(1+\alpha^6) \pmod 3,\ \log_\alpha(1-\alpha^6) \pmod 3\} = \{1, 2\}. \tag{11}$$

We shall use Lemma 11 to show the existence of α which satisfies (11). 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 $\mathcal{F} = \left\{1+x^6, 1-x^6\right\}$. 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 11:

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 canonical factorization of $f_{i_1,i_2}(x)$, the power 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 $c(h(x))^{q-1}$.
2) If $i_2 = 0$, then $i_1 \neq 0$. Since $\gcd(1+x^6, 6x^5) = 1$, in the factorization of $1+x^6$, every irreducible factor has power 1. Thus, $f_{i_1,0}(x)$ cannot be written in the form $c(h(x))^{q-1}$.

Applying Lemma 11, 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 [11, 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 (11). ∎

Using similar methods we obtain:

Theorem 13. *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.*

Theorem 14. *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.*

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 a standard argument that converts a code over $\mathbb{F}_p$, p a prime, to a lattice code.

REFERENCES

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

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

[3] R. Bitar, S. K. Hanna, N. Polyanskii, and I. Vorobyev, "Optimal codes correcting localized deletions," *arXiv:2105.02298*, May 2021.

[4] A. R. Booker, S. D. Cohen, N. Sutherland, and T. Trudgian, "Primitive values of quadratic polynomials in a finite field," *Math. Comp.*, vol. 88, pp. 1903–1912, Oct. 2019.

[5] S. Buzaglo and T. Etzion, "Tilings with n-dimensional chairs and their applications to asymmetric codes," *IEEE Trans. Inform. Theory*, vol. 59, pp. 1573–1582, Mar. 2013.

[6] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for asymmetric limited-magnitude errors with applications to multilevel flash memories," *IEEE Trans. Inform. Theory*, vol. 56, no. 4, pp. 1582–1595, Apr. 2010.

[7] 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. Inform. Theory*, vol. 66, no. 2, pp. 957–969, Feb. 2020.

[8] B. Eitan and A. Roy, "Binary and multilevel flash cells," in *Flash Memories*, P. Cappelletti, C. Golla, P. Olivo, and E. Zanoni, Eds. Kluwer, 1999, pp. 91–152.

[9] T. Etzion, "Constructions for perfect 2-burst-correcting codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 6, pp. 2553–2555, Sep. 2001.

[10] W. Hamaker and S. Stein, "Combinatorial packing of R^3 by certain error spheres," *IEEE Trans. Inform. Theory*, vol. 30, no. 2, pp. 364–368, Mar. 1984.

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers, 6th Edition*. Oxford University Press, 2008.

[12] D. Hickerson and S. Stein, "Abelian groups and packing by semicrosses," *Pacific J. Math.*, vol. 122, no. 1, pp. 95–109, 1986.

[13] S. Jain, F. Farnoud, M. Schwartz, and J. Bruck, "Coding for optimized writing rate in DNA storage," in *Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT2020), Los Angeles, CA, USA*, Jun. 2020.

[14] T. Kløve, J. Luo, I. Naydenova, and S. Yari, "Some codes correcting asymmetric errors of limited magnitude," *IEEE Trans. Inform. Theory*, vol. 57, no. 11, pp. 7459–7472, Nov. 2011.

[15] 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.

[16] A. Lenz and N. Polyanskii, "Optimal codes correcting a burst of deletions of variable length," in *Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT2020), Los Angeles, CA*, Jun. 2020.

[17] 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.

[18] D. Lind and B. H. Marcus, *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, 1985.

[19] C. Schoeny, A. Wachter-Zeh, R. Gabrys, and E. Yaakobi, "Codes correcting a burst of deletions or insertions," *IEEE Trans. Inform. Theory*, vol. 63, no. 4, pp. 1971–1985, Apr. 2017.

[20] M. Schwartz, "Quasi-cross lattice tilings with applications to flash memory," *IEEE Trans. Inform. Theory*, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.

[21] ——, "On the non-existence of lattice tilings by quasi-crosses," *European J. of Combin.*, vol. 36, pp. 130–142, Feb. 2014.

[22] S. Stein, "Factoring by subsets," *Pacific J. Math.*, vol. 22, no. 3, pp. 523–541, 1967.

[23] ——, "Packings of R^n by certain error spheres," *IEEE Trans. Inform. Theory*, vol. 30, no. 2, pp. 356–363, Mar. 1984.

[24] ——, "The notched cube tiles $\mathbb{R}^n$," *Discrete Math.*, vol. 80, no. 3, pp. 335–337, 1990.

[25] S. Stein and S. Szabó, *Algebra and Tiling*. The Mathematical Association of America, 1994.

[26] H. Wei and M. Schwartz, "On tilings of asymmetric limited-magnitude balls," *European J. of Combin.*, vol. 100, pp. 1–21, Feb. 2022.

[27] ——, "Perfect codes correcting a single burst of limited-magnitude errors," *arXiv:2201.01558*, Jan. 2022.

[28] H. Wei, X. Wang, and M. Schwartz, "On lattice packings and coverings of asymmetric limited-magnitude balls," *IEEE Trans. Inform. Theory*, vol. 67, no. 8, pp. 5104–5115, Aug. 2021.

[29] S. Yari, T. Kløve, and B. Bose, "Some codes correcting unbalanced errors of limited magnitude for flash memories," *IEEE Trans. Inform. Theory*, vol. 59, no. 11, pp. 7278–7287, Nov. 2013.

[30] Z. Ye, T. Zhang, X. Zhang, and G. Ge, "Some new results on splitter sets," *IEEE Trans. Inform. Theory*, vol. 66, no. 5, pp. 2765–2776, May 2020.

[31] T. Zhang and G. Ge, "New results on codes correcting single error of limited magnitude for flash memory," *IEEE Trans. Inform. Theory*, vol. 62, no. 8, pp. 4494–4500, Aug. 2016.

[32] ——, "On the nonexistence of perfect splitter sets," *IEEE Trans. Inform. Theory*, vol. 64, no. 10, pp. 6561–6566, Oct. 2018.

[33] 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.