On Lattice Packings and Coverings of Asymmetric Limited-Magnitude Balls

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

***Abstract*— We construct integer error-correcting codes and covering codes for the limited-magnitude error channel with more than one error. The codes are lattices that pack or cover the space with the appropriate error ball. Some of the constructions attain an asymptotic packing/covering density that is constant. The results are obtained via various methods, including the use of codes in the Hamming metric, modular B_t-sequences, 2-fold Sidon sets, and sets avoiding arithmetic progression.**

***Index Terms*— Integer coding, packing, covering, tiling, lattices, limited-magnitude errors.**

I. Introduction

Several applications use information that is encoded as vectors of integers, either directly or indirectly. Furthermore, these vectors are affected by noise that may increase or decrease entries of the vectors by a limited amount. We mention a few of these examples: In high-density magnetic recording channels, information is stored in the lengths of runs of 0's. Various phenomena may cause the reading process to shift the positions of 1's (peak-shift error), thereby changing the length of adjacent runs of 0's by a limited amount (e.g., see [19], [21]). In flash memories, information is stored in the charge levels of cells in an array. However, retention (slow charge leakage), and inter-cell interference, may cause charge levels to move, usually, by a limited amount (e.g., see [6]). More recently, in some DNA-storage applications, information is stored in the lengths of homopolymer runs. These however, may end up shorter or longer than planned, usually by a limited amount, due to variability in the molecule-synthesis process (see [14]).

In all of the applications mentioned above, an integer vector $\mathbf{v} \in \mathbb{Z}^n$ encodes information. If at most t of its entries suffer an increase by as much as k_+, or a decrease by as much as k_-, we can write the corrupted vector as $\mathbf{v} + \mathbf{e}$, where $\mathbf{e}$ resides within a shape we call the (n, t, k_+, k_-)-*error-ball*, and is defined as

$$\mathcal{B}(n, t, k_+, k_-) \triangleq \{\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{Z}^n \mid -k_- \leqslant x_i \leqslant k_+ \text{ and } \mathrm{wt}(\mathbf{x}) \leqslant t\}, \quad (1)$$

where $\mathrm{wt}(\mathbf{x})$ denotes the Hamming weight of $\mathbf{x}$.

It now follows that an error-correcting code in this setting is equivalent to a packing of $\mathbb{Z}^n$ by $\mathcal{B}(n, t, k_+, k_-)$, and a perfect code is equivalent to a tiling of $\mathbb{Z}^n$ by $\mathcal{B}(n, t, k_+, k_-)$. An example of $\mathcal{B}(3, 2, 2, 1)$ is shown in Fig. 1.

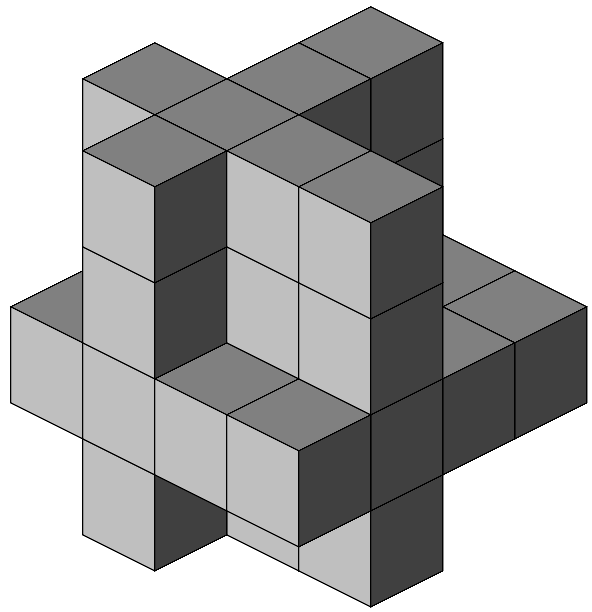

Fig. 1. A depiction of $\mathcal{B}(3, 2, 2, 1)$ where each point in $\mathcal{B}(3, 2, 2, 1)$ is shown as a unit cube.

Covering $\mathbb{Z}^n$ by $\mathcal{B}(n, t, k_+, k_-)$ is also of interest. Such coverings are useful in the context of non-volatile memories, most prominently flash memories. They have been used for rewriting scheme (e.g., see [15]), and write-once-memory (WOM) codes (e.g., see [12] and [8, Chapter 17], as well as the many references therein). As an example, the information stored in an array of flash memory cells may be thought of as a vector of integers. Due to an inherent asymmetry in these cells, increasing entries of this vector is easy, while decreasing is difficult and requires erasing the entire vector to an all-zero vector. The latter operation is physically harmful, and the lifetime of the memory is measured by it. Since cells have

Manuscript received May 29, 2020; revised November 30, 2020; accepted March 12, 2021. Date of publication April 2, 2021; date of current version July 14, 2021. The work of Hengjia Wei and Moshe Schwartz was supported in part by the Israel Science Foundation (ISF) under Grant 270/18. The work of Xin Wang was supported in part by the National Natural Science Foundation of China under Grant 11801392 and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20180833. *(Corresponding author: Hengjia Wei.)*

Hengjia Wei and Moshe Schwartz are with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer Sheva 8410501, Israel (e-mail: hjwei05@gmail.com; schwartz@ee.bgu.ac.il).

Xin Wang is with the Department of Mathematics, Soochow University, Suzhou 215006, China (e-mail: xinw@suda.edu.cn).

Communicated by L. Dolecek, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2021.3070462

0018-9448 © 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

an upper limit on their value, erasing the cells is inevitable, but WOM codes and rewriting schemes attempt to delay the inevitable in the following way: Assume the current stored vector is $\mathbf{x}$. Given a lattice covering of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,k_+,0)$, the user information is coset-encoded by choosing an arbitrary vector $\mathbf{x}'$ in the user-chosen lattice coset, such that $\mathbf{x}'$ is entry-wise no less than than $\mathbf{x}$. The covering property of the lattice ensures $\mathbf{x}'$ increases at most t entries by at most k_+ each, in comparison with $\mathbf{x}$. This slows the approach of the system to the cells' upper limit.

A significant amount of works has been devoted to lattice tiling/packing/covering of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,k_+,k_-)$, albeit, almost exclusively for the case of $t=1$. When packing and tiling are concerned, the *cross*, $\mathcal{B}(n,1,k,k)$, and semi-cross, $\mathcal{B}(n,1,k,0)$ have been extensively researched, e.g., see [11], [13], [17], [28], [30] and the many references therein. This was extended to *quasi-crosses*, $\mathcal{B}(n,1,k_+,k_-)$, in [25], creating a flurry of activity on the subject [26], [36]–[40]. To the best of our knowledge, [5], [17], [29], [35] are the only works to consider $t \geqslant 2$. [5], [29] considered tiling a notched cube (or a "chair"), which for certain parameters becomes $\mathcal{B}(n,n-1,k,0)$, while [17] considered packing the same ball $\mathcal{B}(n,n-1,k,0)$. Among others, [35] recently studied the tiling problem in the most general case, i.e., tiling $\mathcal{B}(n,t,k_+,k_-)$ for $t \geqslant 2$. Covering problems have also been studied, though only when $t=1$, [7], [16], [18].

The main goal of this paper is to study packing and covering of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,k_+,k_-)$ when $t \geqslant 2$. We would like to have packings of high density and covering of low density, as they imply error-correcting codes of large size and covering codes of small size, respectively. We provide explicit constructions for both packings and coverings, as well as some non-constructive existence results. In particular, we demonstrate the existence of packings with asymptotic packing density $\Omega(1)$ (as n tends to infinity) for some sets of (t,k_+,k_-), and the existence of coverings with density $O(1)$ for any given (t,k_+,k_-). Additionally, we generalize the concept of packing to λ-packing, which works in conjunction with the list-decoding framework and list size λ. We show the existence of λ-packings with density $O(n^{-\epsilon})$ for any (t,k_+,k_-) and arbitrarily small $\epsilon > 0$, while maintaining a list size $\lambda = O(\epsilon^{-t})$, which does not depend on n. Our results are summarized at the end of this paper, in Table I.

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 study of packings. This is generalized in Section IV to λ-packings. In Section V we construct coverings. Finally, we conclude in Section VI by giving a summary of the results as well as some open problems.

II. Preliminaries

For integers $a \leqslant b$ we define $[a,b] \triangleq \{a,a+1,\dots,b\}$ and $[a,b]^* \triangleq [a,b]\setminus\{0\}$. 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.

A *lattice* $\Lambda \subseteq \mathbb{Z}^n$ is an additive subgroup of $\mathbb{Z}^n$ (sometimes called an *integer lattice*). A lattice Λ may be represented by a matrix $\mathcal{G}(\Lambda) \in \mathbb{Z}^{n\times n}$, the span of whose rows (with integer coefficients) is Λ. From a geometric point of view, when viewing Λ inside $\mathbb{R}^n$, a *fundamental region* of Λ is defined as

$$\Pi(\Lambda) \triangleq \left\{ \sum_{i=1}^{n} c_i \mathbf{v}_i \;\middle|\; c_i \in \mathbb{R}, 0 \leqslant c_i < 1 \right\},$$

where $\mathbf{v}_i$ is the i-th row of $\mathcal{G}(\Lambda)$. It is well known that the volume of $\Pi(\Lambda)$ is $|\det(\mathcal{G}(\Lambda))|$, and is independent of the choice of $\mathcal{G}(\Lambda)$. We therefore denote

$$\mathrm{vol}(\Lambda) \triangleq \mathrm{vol}(\Pi(\Lambda)) = |\det(\mathcal{G}(\Lambda))|.$$

In addition, if $\mathrm{vol}(\Lambda) \neq 0$ then

$$\mathrm{vol}(\Lambda) = |\mathbb{Z}^n/\Lambda|.$$

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 $\mathcal{B}$ *tiles* $\mathbb{Z}^n$ by T. The *packing density* (or *covering density*, respectively) of $\mathcal{B}$ by T is defined as

$$\delta \triangleq \lim_{\ell\to\infty} \frac{|[-\ell,\ell]^n \cap T| \cdot |\mathcal{B}|}{|[-\ell,\ell]^n|}.$$

When $T=\Lambda$ is some lattice, we call these lattice packings and lattice coverings, respectively. The density then takes on a simpler form

$$\delta = \frac{|\mathcal{B}|}{\mathrm{vol}(\Lambda)}.$$

Throughout the paper, the object we pack and cover $\mathbb{Z}^n$ with, is the error ball, $\mathcal{B}(n,t,k_+,k_-)$, defined in (1). We conveniently observe that for all integers $n \geqslant 1$, $0 \leqslant t \leqslant n$, $0 \leqslant k_- \leqslant k_+$, we have

$$|\mathcal{B}(n,t,k_+,k_-)| = \sum_{i=0}^{t} \binom{n}{i} (k_+ + k_-)^i.$$

A. Lattice Packing/Covering/Tiling and Group Splitting

Lattice packing, covering, and tiling of $\mathbb{Z}^n$ with $\mathcal{B}(n,t,k_+,k_-)$, in connection with group splitting, has a long history when $t=1$ (e.g., see [27]), called lattice tiling by crosses if $k_+ = k_-$ (e.g., [28]), semi-crosses when $k_- = 0$ (e.g., [11], [13], [28]), and quasi-crosses when $k_+ \geqslant k_- \geqslant 0$ (e.g., [25], [26]). For an excellent treatment and history, the reader is referred to [30] and the many references therein. Other variations, keeping $t=1$ include [31], [32]. More recent results may be found in [37] and the references therein.

For $t \geqslant 2$, an extended definition of group splitting in connection with lattice tiling is provided in [35]. In the following, we modify this definition to distinguish between lattice packings, coverings, and tilings.

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

Definition 1: 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 $m \leqslant 0$. Let $M \subseteq \mathbb{Z} \setminus \{0\}$ be a finite set, and $S = \{s_1, s_2, \ldots, s_n\} \subseteq G$.

1) If the elements $\mathbf{e} \cdot (s_1, \ldots, s_n)$, where $\mathbf{e} \in (M \cup \{0\})^n$ and $1 \leqslant \mathrm{wt}(\mathbf{e}) \leqslant t$, are all distinct and non-zero in G, we say the set M partially t-splits G with splitter set S, denoted
$$G \geqslant M \diamond_t S.$$
2) If for every $g \in G$ there exists a vector $\mathbf{e} \in (M \cup \{0\})^n$, $\mathrm{wt}(\mathbf{e}) \leqslant t$, such that $g = \mathbf{e} \cdot (s_1, \ldots, s_n)$, we say the set M completely t-splits G with splitter set S, denoted
$$G \leqslant M \diamond_t S.$$
3) If $G \geqslant M \diamond_t S$ and $G \leqslant M \diamond_t S$ we say M t-splits G with splitter set S, and write
$$G = M \diamond_t S.$$

In our context, since we are interested in packing and covering with $\mathcal{B}(n, t, k_+, k_-)$, then in the previous definition, we need to take $M \triangleq [-k_-, k_+]^*$. Thus, the following two theorems show the equivalence of partial t-splittings with M and lattice packings of $\mathcal{B}(n, t, k_+, k_-)$, summarizing Lemma 3 and Lemma 4 in [5], and similarly for complete t-splittings and lattice coverings.

Theorem 2: Let G be a finite Abelian group, $M \triangleq [-k_-, k_+]^*$, and $S = \{s_1, \ldots, s_n\} \subseteq G$. Define $\phi : \mathbb{Z}^n \to G$ as $\phi(\mathbf{x}) \triangleq \mathbf{x} \cdot (s_1, \ldots, s_n)$ and let $\Lambda \triangleq \ker \phi$ be a lattice.

1) If $G \geqslant M \diamond_t S$, then $\mathcal{B}(n, t, k_+, k_-)$ packs $\mathbb{Z}^n$ by Λ.
2) If $G \leqslant M \diamond_t S$, then $\mathcal{B}(n, t, k_+, k_-)$ covers $\mathbb{Z}^n$ by Λ.

Proof: For packing, see Lemma 4 in [5]. For covering, denote $\mathcal{B} \triangleq \mathcal{B}(n, t, k_+, k_-)$. Assume $\mathbf{x} \in \mathbb{Z}^n$. Since $G \leqslant M \diamond_t S$, there exists a vector $\mathbf{e} \in \mathcal{B}$ such that $\phi(\mathbf{x}) = \phi(\mathbf{e})$. Then $\mathbf{v} \triangleq \mathbf{x} - \mathbf{e} \in \Lambda$, and $\mathbf{x} \in \mathbf{v} + \mathcal{B}$. ∎

In the theorem above, for $G \geqslant M \diamond_t S$, since the quotient group $\mathbb{Z}^n/\Lambda$ is isomorphic to the image of ϕ, which is a subgroup of G, we have $\mathrm{vol}(\Lambda) \leqslant |G|$. Then the packing density of Λ is
$$\delta = \frac{|\mathcal{B}(n, t, k_+, k_-)|}{\mathrm{vol}(\Lambda)} \geqslant \frac{|\mathcal{B}(n, t, k_+, k_-)|}{|G|}.$$
For $G \leqslant M \diamond_t S$, $\mathrm{vol}(\Lambda) = |G|$, and the covering density of Λ is
$$\delta = \frac{|\mathcal{B}(n, t, k_+, k_-)|}{\mathrm{vol}(\Lambda)} = \frac{|\mathcal{B}(n, t, k_+, k_-)|}{|G|}.$$

It is known that a lattice packing implies a partial splitting. While not of immediate use to us in this paper, we do mention that an analogous claim is also true for lattice coverings, as the following theorem shows.

Theorem 3: Let $\Lambda \subseteq \mathbb{Z}^n$ be a lattice. 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, and then $\Lambda = \ker \phi$. Finally, let $\mathbf{e}_i$ be the i-th unit vector in $\mathbb{Z}^n$ and set $s_i \triangleq \phi(\mathbf{e}_i)$ for all $1 \leqslant i \leqslant n$ and $S \triangleq \{s_1, s_2, \ldots, s_n\}$.

1) If $\mathcal{B}(n, t, k_+, k_-)$ packs $\mathbb{Z}^n$ by Λ, then $G \geqslant M \diamond_t S$;
2) if $\mathcal{B}(n, t, k_+, k_-)$ covers $\mathbb{Z}^n$ by Λ, then $G \leqslant M \diamond_t S$, where $M \triangleq [-k_-, k_+]^*$.

Proof: For the packing case, see Lemma 3 in [5]. Now we prove the claim for covering. Let $\Lambda + \mathbf{x} \in G$ be any element of G. Since $\mathcal{B}(n, t, k_+, k_-)$ covers $\mathbb{Z}^n$ by Λ, there exist $\mathbf{v} \in \Lambda$ and $\mathbf{e} \in \mathcal{B}(n, t, k_+, k_-)$ such that $\mathbf{x} = \mathbf{v} + \mathbf{e}$. This means
$$\Lambda + \mathbf{x} = \phi(\mathbf{x}) = \phi(\mathbf{v}) + \phi(\mathbf{e}) = \phi(\mathbf{e}) = \mathbf{e} \cdot (s_1, \ldots, s_n),$$
which completes the proof. ∎

Finally, a connection between perfect codes in the Hamming metric, and lattice tilings with $\mathcal{B}(n, t, k_+, k_-)$ was observed in [35]. We repeat a theorem that we shall generalize later.

Theorem 4 (Theorem 3 in [35]): In the Hamming metric space, let C be a perfect linear $[n, k, 2t+1]$ code over $\mathbb{F}_p$, with p a prime. If $k_+ + k_- + 1 = p$, then
$$\Lambda \triangleq \{\mathbf{x} \in \mathbb{Z}^n \mid (\mathbf{x} \bmod p) \in C\}$$
is a lattice, and $\mathcal{B}(n, t, k_+, k_-)$ tiles $\mathbb{Z}^n$ by Λ.

III. Constructions of Lattice Packings

In this section we describe several constructions for packings of $\mathcal{B}(n, t, k_+, k_-)$. We begin by showing how to translate codes in the Hamming metric into lattices that pack $\mathcal{B}(n, t, k_+, k_-)$. Apart from a single case, these have vanishing density. The motivation for showing these "off-the-shelf" constructions is to create a baseline against which we measure our tailor-made constructions that appear later. These use $B_t[N; 1]$ sets (see Subsection III-B), or take inspiration from constructions of sets with no arithmetic progression, to construct codes that improve upon the baseline.

A. Constructions Based on Error-Correcting Codes

Theorem 4 can be easily modified to yield the following construction, the proof of which is the same as that of [35, Theorem 3] and we omit here to avoid unnecessary repetition.

Theorem 5: In the Hamming metric space, let C be a linear $[n, k, 2t+1]$ code over $\mathbb{F}_p$, with p a prime. If $0 \leqslant k_+ + k_- < p$ are integers, then
$$\Lambda \triangleq \{\mathbf{x} \in \mathbb{Z}^n \mid (\mathbf{x} \bmod p) \in C\}$$
is a lattice, and $\mathcal{B}(n, t, k_+, k_-)$ packs $\mathbb{Z}^n$ by Λ.

Since $\mathcal{B}(n, t, k_+, k_-)$ packs $\mathbb{Z}^n$ by Λ, the lattice Λ is an error-correcting code over $\mathbb{Z}$ for asymmetric limited-magnitude errors. We note that a similar construction of error-correcting codes over a finite alphabet for asymmetric limited-magnitude errors was presented in [6] and the decoding scheme therein can be adapted here as follows. Let $\mathbf{x} \in \Lambda$ be a codeword, and $\mathbf{y} \in \mathbf{x} + \mathcal{B}(n, t, k_+, k_-)$ be the channel output. Denote $\boldsymbol{\psi} = \mathbf{y} \pmod p$. Run the decoding algorithm of the linear $[n, k, 2t+1]$ code on $\boldsymbol{\psi}$ and denote the output as $\boldsymbol{\phi}$. Then $\boldsymbol{\phi}$ is a codeword of the linear code over $\mathbb{F}_p$ and it is easy to see that $\boldsymbol{\phi} = \mathbf{x} \pmod p$. Thus $\mathbf{y} - \mathbf{x} \equiv \boldsymbol{\psi} - \boldsymbol{\phi} \pmod p$. Denote $\boldsymbol{\epsilon} = \boldsymbol{\psi} - \boldsymbol{\phi} \pmod p$ and let $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ where
$$e_i \triangleq \begin{cases} \epsilon_i, & \text{if } 0 \leqslant \epsilon_i \leqslant k_+; \\ \epsilon_i - p, & \text{otherwise.} \end{cases}$$
Then $\mathbf{x}$ can be decoded as $\mathbf{x} = \mathbf{y} - \mathbf{e}$.

Now let us look at the packing density.

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

Corollary 6: Let Λ be the lattice constructed in Theorem 5. Then $\mathrm{vol}(\Lambda) = p^{n-k}$ and the packing density is

$$\delta = \frac{\sum_{i=0}^{t} \binom{n}{i} (k_+ + k_-)^i}{p^{n-k}}.$$

Proof: In Theorem 5, the quotient group $\mathbb{Z}^n/\Lambda$ is isomorphic to the group $\mathbb{Z}_p^{n-k}$ (see Example 3 and Example 4 in [35]). The claim is then immediate. ■

When t is small, we may use BCH codes as the input to construct the lattice packing.

Theorem 7 (Primitive Narrow-Sense BCH Codes [1, Theorem 10]): Let p be a prime. Fix $m \geqslant 1$ and $2 \leqslant d \leqslant p^{\lceil m/2 \rceil} - 1$. Set $n = p^m - 1$. Then there exists an $[n, k, d]$-code over $\mathbb{F}_p$ with

$$k = n - \lceil (d-1)(1 - 1/p) \rceil m.$$

Corollary 8: Let $\psi(x)$ be the smallest prime not smaller than x [1] and denote $p \triangleq \psi(k_+ + k_- + 1)$. Let m, t be positive integers such that $2t \leqslant p^{\lceil m/2 \rceil} - 2$, and set $n = p^m - 1$. Then $\mathbb{Z}^n$ can be lattice packed by $\mathcal{B}(n, t, k_+, k_-)$ with density

$$\delta = \frac{\sum_{i=0}^{t} \binom{n}{i} (k_+ + k_-)^i}{(n+1)^{\lceil 2t(1-1/p) \rceil}}.$$

Proof: Simply combine Theorem 7 with Corollary 6. ■

Note that if $k_+ = 1$ and $k_- = 0$, then the packing density in Corollary 8 is $\delta = \frac{\sum_{i=0}^{t} \binom{n}{i}}{(n+1)^t} = \frac{1}{t!} + o(1)$ (when t is fixed and n tends to infinity). However, for all the other values of k_+ and k_-, namely $p \geqslant 3$, the density always vanishes when n tends to infinity, i.e., $\delta = \Theta(n^{t - \lceil 2t(1-1/p) \rceil})$. In the remainder of this section, we will present some constructions to provide lattice packings of higher density.

Perfect codes were used in [35] obtain lattice tilings, i.e., lattice packings with density 1. Similarly, it is possible to use quasi-perfect linear codes to obtain lattice packings with high densities.

Corollary 9: Assume that $1 \leqslant k_+ + k_- \leqslant 2$ are non-negative integers.

1) Let m be a positive integer and $n = (3^m + 1)/2$. Then $\mathbb{Z}^n$ can be lattice-packed by $\mathcal{B}(n, 2, k_+, k_-)$ with density

$$\delta = \frac{\binom{n}{2}(k_+ + k_-)^2 + n(k_+ + k_-) + 1}{(2n-1)^2}.$$

2) Let $m \geqslant 3$ be an odd integer and $n = (3^m - 1)/2$. Then $\mathbb{Z}^n$ can be lattice-packed by $\mathcal{B}(n, 2, k_+, k_-)$ with density

$$\delta = \frac{\binom{n}{2}(k_+ + k_-)^2 + n(k_+ + k_-) + 1}{(2n+1)^2}.$$

Proof: For the first case, we take a $[(3^m + 1)/2, (3^m + 1)/2 - 2m, 5]_3$ code from [10] as the input of Theorem 5 to obtain the lattice packing, while for the second, we take a $[(3^m - 1)/2, (3^m - 1)/2 - 2m, 5]_3$ code from [9] as the input. ■

We note that [22] presented some binary quasi-perfect linear codes with minimum distance 5, which can give rise to packings of $\mathcal{B}(n, 2, 1, 0)$. It has been checked out that the corresponding densities are asymptotically the same as that in Corollary 8, i.e., $\frac{1}{2} + o(1)$. [22] also studied p-ary quasi-perfect linear codes with $p \geqslant 3$. However, the minimum distances of those codes are no more that 4. So they cannot be used to obtain packings of $\mathcal{B}(n, t, k_+, k_-)$ with $t \geqslant 2$.

The following theorem uses non-linear codes to construct non-lattice packing, the proof of which is the same as that of [6, Theorem 5] and we omit here to avoid unnecessary repetition.

Theorem 10: In the Hamming metric space, let C be a q-ary $(n, M, 2t+1)$ code. Denote

$$V \triangleq \{\mathbf{v} \in \mathbb{Z}^n \mid (\mathbf{v} \bmod q) \in C\}.$$

If $k_+ + k_- < q$, then for any distinct $\mathbf{v}, \mathbf{v}' \in V$, we have $(\mathbf{v} + \mathcal{B}(n, t, k_+, k_-)) \cap (\mathbf{v}' + \mathcal{B}(n, t, k_+, k_-)) = \varnothing$, namely, $\mathcal{B}(n, t, k_+, k_-)$ can pack $\mathbb{Z}^n$ by V.

Corollary 11: The density of the packing of $\mathbb{Z}^n$ constructed in Theorem 10 is

$$\delta = \frac{M \cdot \sum_{i=0}^{t} \binom{n}{i} (k_+ + k_-)^i}{q^n}.$$

Proof: Note that the set V constructed in Theorem 10 has period q in each coordinate. Thus, the packing density of $\mathbb{Z}^n$ is equal to the packing density of $\mathbb{Z}_q^n$, which is $\frac{M}{q^n} \sum_{i=0}^{t} \binom{n}{i} (k_+ + k_-)^i$. ■

Corollary 12: Let $m \geqslant 4$ be an even integer and let $n = 2^m - 1$. Then $\mathbb{Z}^n$ can be packed by $\mathcal{B}(n, 2, 1, 0)$ with density

$$\delta = \frac{\binom{n}{2} + n + 1}{(n+1)^2/2} = 1 - \frac{n-1}{(n+1)^2}.$$

Proof: We take a binary $(2^m - 1, 2^{2^m - 2m}, 5)$ Preparata code [23] as the input of Theorem 10 to obtain the packing. ■

B. Construction Based on $B_t[N; 1]$ Sets for $(k_+, k_-) = (1, 0)$ or $(1, 1)$

A subset $A \subseteq \mathbb{Z}$ is called a $B_t[g]$ *set* if every integer can be written in at most g different ways as a sum of t (not necessary distinct) elements of A (e.g., see [33, Section 4.5] and the many references therein). In this section, however, we require $B_t[1]$ sets with a somewhat stronger property. Specifically, a subset A of $\mathbb{Z}_N$ is called a $B_t[N; 1]$ *set* if the sums of any t (not necessary distinct) elements of A are all different modulo N. Bose and Chowla [4] presented two classes of $B_t[N; 1]$ sets.

Theorem 13 ([4, Theorem 1 and Theorem 2]): Let q be a prime power and t be a positive integer. Let $\alpha_0 = 0, \alpha_1, \alpha_2, \dots, \alpha_{q-1}$ be all the different elements of $\mathbb{F}_q$.

1) Let ξ be a primitive element of the extended field $\mathbb{F}_{q^t}$. For each $0 \leqslant i \leqslant q-1$, let $d_i \in \mathbb{Z}_{q^t - 1}$ be such that

$$\xi^{d_i} = \xi + \alpha_i.$$

Then the set $S_1 \triangleq \{d_i \mid 0 \leqslant i \leqslant q-1\}$ is a $B_t[q^t - 1; 1]$ set of size q.

2) Let η be a primitive element of the extended field $\mathbb{F}_{q^{t+1}}$. For each $0 \leqslant i \leqslant q-1$, let $\beta_i \in \mathbb{F}_q$ and

[1]It is known that $\psi(x) \leqslant x + x^{21/40}$ [2], and conjectured that $\psi(x) = x + O(\log x)$.

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

$s_i \in \mathbb{Z}_{(q^{t+1}-1)/(q-1)}$ such that

$$\beta_i \eta^{s_i} = \eta + \alpha_i.$$

Then the set $S_2 \triangleq \{s_i \,|\, 0 \leqslant i \leqslant q-1\} \cup \{0\}$ is a $B_t[(q^{t+1}-1)/(q-1);1]$ set of size $q+1$.

Theorem 14: Let A be a $B_t[N;1]$ set which contains 0. Denote $S \triangleq A \setminus \{0\}$. Then $\mathbb{Z}_N \geqslant \{1\} \diamond_t S$.

Proof: Suppose to the contrary that $\{s_{i_1}, s_{i_2}, \ldots, s_{i_\ell}\}$ and $\{s_{j_1}, s_{j_2}, \ldots, s_{j_r}\}$ are two distinct subsets of S such that

$$s_{i_1} + s_{i_2} + \ldots + s_{i_\ell} \equiv s_{j_1} + s_{j_2} + \ldots + s_{j_r} \pmod N,$$

where $\ell, r \leqslant t$. Then we have

$$\underbrace{0+0+\cdots+0}_{t-\ell} + s_{i_1} + s_{i_2} + \ldots + s_{i_\ell}$$
$$\equiv \underbrace{0+0+\cdots+0}_{t-r} + s_{j_1} + s_{j_2} + \ldots + s_{j_r} \pmod N,$$

which contradicts that $S \cup \{0\}$ is a $B_t[N;1]$ set. ■

The following result slightly improves upon the density obtained in Corollary 8 for lattice packings of $\mathcal{B}(n,t,1,0)$.

Corollary 15: 1) Let $t \geqslant 2$ be a fixed integer. Assume that $n+1$ is a prime power tending to infinity, then there is a lattice packing of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,1,0)$ with density

$$\delta = \frac{\sum_{i=0}^{t}\binom{n}{i}}{(n+1)^t - 1} = \frac{1}{t!} + o(1).$$

2) Let $t \geqslant 2$ be a fixed integer. Assume that n is a prime power tending to infinity, then for any $2 \leqslant t \leqslant n$, there is a lattice packing of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,1,0)$ with density

$$\delta = \frac{\sum_{i=0}^{t}\binom{n}{i}}{(n^{t+1}-1)/(n-1)} = \frac{1}{t!} + o(1).$$

Proof: Note that if $\{s_1, s_2, \ldots, s_n\}$ is a $B_t[N;1]$ set, then $\{0, s_2 - s_1, s_3 - s_1, \ldots, s_n - s_1\}$ is also a $B_t[N;1]$ set, which contains 0. Hence, combining Theorem 13 and Theorem 14, together with Theorem 2, we prove the claim. ■

In general, we do not have an efficient decoding scheme for the lattice code obtained from Theorem 14. However, for the lattice code $\Lambda_{S_2\setminus\{0\}}$ obtained from the $B_t[(q^{t+1}-1)/(q-1);1]$ set S_2 in Theorem 13, we have the following decoding algorithm (summarized in Algorithm 1). Let $n = q$ and let $S_2 \setminus \{0\} = \{s_0, \ldots, s_{n-1}\}$ be defined as in Theorem 13. Let $\mathbf{x} \in \Lambda_{S_2\setminus\{0\}}$ be a codeword and $\mathbf{y} \in \mathbf{x} + \mathcal{B}(n,t,1,0)$ be the channel output. Then $\mathbf{x} \cdot (s_0, s_1, \ldots, s_{n-1}) = 0$, and $\mathbf{y} - \mathbf{x}$ is a binary vector over $\{0,1\}$ of weight at most t. Let $i_1, i_2, \ldots, i_r$ be the indices of the nonzero bits of $\mathbf{y} - \mathbf{x}$, and denote $s = \mathbf{y} \cdot (s_0, s_1, \ldots, s_{n-1})$. We aim to recover $i_1, i_2, \ldots, i_r$ from s. Since

$$\begin{aligned} s &= \mathbf{y} \cdot (s_0, s_1, \ldots, s_{n-1}) = \mathbf{y} \cdot (s_0, s_1, \ldots, s_{n-1}) - 0 \\ &= \mathbf{y} \cdot (s_0, s_1, \ldots, s_{n-1}) - \mathbf{x} \cdot (s_0, s_1, \ldots, s_{n-1}) \\ &= (\mathbf{y} - \mathbf{x}) \cdot (s_0, s_1, \ldots, s_{n-1}) = \sum_{\ell=1}^{r} s_{i_\ell}, \end{aligned}$$

we have that

$$\left(\prod_{\ell=1}^{r} \beta_{i_\ell}\right)\eta^s = \prod_{\ell=1}^{r}(\beta_{i_\ell}\eta^{s_{i_\ell}}) = \prod_{\ell=1}^{r}(\eta + \alpha_{i_\ell}). \tag{2}$$

Let $p(x)$ be the primitive polynomial of η and $r(x) = x^s \bmod p(x)$. Then $r(\eta) = \eta^s$, and we substitute this in (2) to obtain

$$\left(\prod_{\ell=1}^{r} \beta_\ell\right) r(\eta) = \prod_{\ell=1}^{r}(\eta + \alpha_{i_\ell}).$$

Since both the polynomials $(\prod_{\ell=1}^{r} \beta_{i_\ell}) r(x)$ and $\prod_{\ell=1}^{r}(x + \alpha_{i_\ell})$ are over $\mathbb{F}_q$ and have degrees at most t, they should be the same; otherwise, η is a root of a nonzero polynomial of degree at most t, which contradicts the fact that η is a primitive element of $\mathbb{F}_{q^{t+1}}$. Thus, we may solve $(\prod_{\ell=1}^{r} \beta_\ell) r(x)$ to find out $\alpha_{i_1}, \alpha_{i_1}, \ldots, \alpha_{i_r}$. Finally, we can subtract $\sum_{\ell=1}^{r} \mathbf{e}_{i_\ell}$ from $\mathbf{y}$ to obtain $\mathbf{x}$.

Algorithm 1 Decoding Algorithm for $\Lambda_{S_2\setminus\{0\}}$ From Theorem 13

Input: received vector $\mathbf{y} \in \mathbb{Z}^n$ suffering at most t errors
$S_2 \setminus \{0\} = \{s_0, \ldots, s_{n-1}\}$ from Theorem 13
where η is a root of a primitive polynomial $p(x)$ of degree $t+1$
and where $\mathbb{F}_q \setminus \{0\} = \{\alpha_1, \ldots, \alpha_{q-1}\}$.
Output: codeword $\mathbf{x} \in \Lambda_{S_2\setminus\{0\}}$ such that $\mathbf{y} \in \mathbf{x} + \mathcal{B}(n,t,1,0)$

1: $s \leftarrow \mathbf{y} \cdot (s_0, s_1, \ldots, s_{n-1})$
2: $r(x) \leftarrow x^s \bmod p(x)$
3: **for** $1 \leqslant i \leqslant q-1$ **do**
4:     **if** $r(\alpha_i) = 0$ **then**
5:         $\mathbf{y} \leftarrow \mathbf{y} - \mathbf{e}_i$
6:     **end if**
7: **end for**
8: **return y**

Let us analyze the time complexity of Algorithm 1, where we count the number of field operations in $\mathbb{F}_q$. The inner product in Step 1 takes $O(n)$ operations. Step 2 is possible to compute in $O(t^2 \log s)$ field operations (by using successive squaring and multiplication by x as necessary, taking a modulo $p(x)$ after each iteration). Since $s \in \mathbb{Z}_{(q^{t+1}-1)/(q-1)}$ and $n = q$, it is $O(t^3 \log n)$. Finally, the root search loop starting in Step 3 takes $O(tn)$ operations. Thus, in total, the time complexity $O(tn + t^3 \log n)$ field operations. If t is constant, then this is linear in the code length. As a final comment, we point out that $q = O(n)$, and thus the basic field operations of addition and multiplication may be realized in $O(\text{polylog}(n))$ time.

We now move from packing $\mathcal{B}(n,t,1,0)$ to packing $\mathcal{B}(n,t,1,1)$. In general, we note that one can use a $B_h[N;1]$ set with $h = t(k_+ + k_-)$ to obtain a lattice packing of $\mathcal{B}(n,t,k_+,k_-)$ in $\mathbb{Z}_n$ for $k_+ + k_- \geqslant 2$. However, in this case, the density is $O(n^{t(1-k_+ + k_-)})$, which vanishes when n tends to infinity. Similarly, the lattice packing from Corollary 8 also has vanishing density $O(n^{t - \lceil 2t(1-1/p) \rceil})$. In the following, we give a modified construction which uses a $B_t[N;1]$ set to obtain a lattice packing of $\mathcal{B}(n,t,1,1)$ with density $\Omega(1)$.

Theorem 16: Let $A = \{a_1, a_2, \ldots, a_n\}$ be a $B_t[N;1]$ set. In the group $\mathbb{Z}_N \times \mathbb{Z}_{2t+1}$, construct a set

$$S \triangleq \{(a_i, 1) \,|\, a_i \in A\}.$$

Then $\mathbb{Z}_N \times \mathbb{Z}_{2t+1} \geqslant \{-1, 1\} \diamond_t S$.

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

Proof: Suppose to the contrary that there are $(a_{i_1},1),(a_{i_1},1),\dots,(a_{i_\ell},1)$ and $(a_{j_1},1),(a_{j_2},1),\dots,(a_{j_r},1)$ in S such that

$$\sum_{m=1}^{\ell'}(a_{i_m},1)-\sum_{m=\ell'+1}^{\ell}(a_{i_m},1)=\sum_{m=1}^{r'}(a_{j_m},1)-\sum_{m=r'+1}^{r}(a_{j_m},1), \tag{3}$$

where $0\leqslant \ell'\leqslant \ell\leqslant t$ and $0\leqslant r'\leqslant r\leqslant t$, and the addition is over the group $\mathbb{Z}_N\times\mathbb{Z}_{2t+1}$.

The second coordinate of the equation above implies that

$$\ell-2\ell'\equiv r-2r' \pmod{2t+1}.$$

Since $0\leqslant \ell'\leqslant \ell\leqslant t$ and $0\leqslant r'\leqslant r\leqslant t$, we have $\ell-2\ell'$, $r-2r'\in[-t,t]$. It follows that $\ell-2\ell'=r-2r'$, and so, $\ell'+r-r'=r'+\ell-\ell'$. Let $\tau\triangleq \ell'+r-r'$. Then

$$\tau=\frac{\ell'+r-r'+r'+\ell-\ell'}{2}=\frac{\ell+r}{2}\leqslant t.$$

Rearranging the terms in the first coordinate of the equation (3), we have

$$\begin{aligned}&a_{i_1}+a_{i_2}+\cdots+a_{i_{\ell'}}+a_{j_{r'+1}}+\cdots+a_{j_r}\\ \equiv&a_{j_1}+a_{j_2}+\cdots+a_{j_{r'}}+a_{i_{\ell'+1}}+\cdots+a_{i_\ell} \pmod N.\end{aligned}$$

On both side of the equation above, there are τ terms. This contradicts the fact that A is a $B_t[N;1]$ (and hence a $B_\tau[N;1]$ set for any $\tau\leqslant t$). ■

Combining Theorem 13 and Theorem 16, together with Theorem 2, we have the following result.

Corollary 17: Let $t\geqslant 2$ be a fixed integer. If n is a prime power tending to infinity, then there is a lattice packing of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,1,1)$ with density

$$\delta=\frac{\sum_{i=0}^{t}\binom{n}{i}2^i}{(2t+1)(n^t-1)}=\frac{2^t}{t!(2t+1)}+o(1).$$

If $n-1$ is a prime power tending to infinity, then there is a lattice packing of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,1,1)$ with density

$$\delta=\frac{\sum_{i=0}^{t}\binom{n}{i}2^i}{(2t+1)((n-1)^{t+1}-1)/(n-2)}=\frac{2^t}{t!(2t+1)}+o(1).$$

C. Constructions for $t=2$

Whereas in the previous section we considered unconstrained t but only small values of k_+,k_-, in this section we focus on the case of $t=2$ but unconstrained k_+,k_-.

We first present a construction based on k-fold Sidon sets. Such sets were first defined in [20] as a generalization of Sidon sets. We repeat the definition here. Let k be a positive integer and let N be relatively prime to all elements of $[1,k]$, i.e., $\gcd(N,k!)=1$. Fix integers $c_1,c_2,c_3,c_4\in[-k,k]$ such that $c_1+c_2+c_3+c_4=0$, and let $\mathcal{S}$ be the collection of sets $S\subseteq\{1,2,3,4\}$ such that $\sum_{i\in S}c_i=0$ and $c_i\neq 0$ for $i\in S$. We note that $\mathcal{S}$ always contains the empty set. Consider the following equation over $x_1,x_2,x_3,x_4\in\mathbb{Z}_N$:

$$c_1x_1+c_2x_2+c_3x_3+c_4x_4\equiv 0 \pmod N. \tag{4}$$

A solution of (4) is *trivial* if there exists a partition of the set $\{i\,|\,c_i\neq 0\}$ into sets $S,T\in\mathcal{S}$ such that $x_i=x_j$ for all $i,j\in S$ and all $i,j\in T$. We now define a *k-fold Sidon set* to be a set $A\subseteq\mathbb{Z}_N$ such that for any $c_1,c_2,c_3,c_4\in[-k,k]$ with $c_1+c_2+c_3+c_4=0$, equation (4) has only trivial solutions in A. In the special case of $k=1$, a 1-fold Sidon set coincides with the usual definition of a *Sidon set*, which is also a $B_2[N;1]$ set.

Theorem 18: Let $A\subseteq\mathbb{Z}_N$ be a k-fold Sidon set. Assume that $0\leqslant k_-\leqslant k_+\leqslant k$ and $k_++k_-\geqslant 1$. In the group $G\triangleq\mathbb{Z}_{2(k_++k_-)+1}\times\mathbb{Z}_N$, construct a set

$$S\triangleq\{(1,x)\,|\,x\in A\}.$$

Then $G\geqslant[-k_-,k_+]^*\diamond_2\ S$.

Proof: Suppose to the contrary that G is not partially 2-split by S. Then there are $x_1,x_2,x_3,x_4\in A$ and $c_1,c_2,c_3,c_4\in[-k_-,k_+]$ such that

$$c_1+c_2\equiv c_3+c_4 \pmod{2(k_++k_-)+1},$$

and

$$c_1x_1+c_2x_2\equiv c_3x_3+c_4x_4 \pmod N, \tag{5}$$

where all the following hold:

1) $x_1\neq x_2$
2) $x_3\neq x_4$
3) $x_1\neq x_3$ if $c_1=c_3$ and $c_2=c_4=0$
4) $x_2\neq x_4$ if $c_2=c_4$ and $c_1=c_3=0$
5) $(x_1,x_2)\neq(x_3,x_4)$ if $(c_1,c_2)=(c_3,c_4)$.
6) $(x_1,x_2)\neq(x_4,x_3)$ if $(c_1,c_2)=(c_4,c_3)$.

Since $-(k_++k_-)\leqslant a+b,c+d\leqslant k_++k_-$, it follows that $c_1+c_2=c_3+c_4$, or equivalently, $c_1+c_2-c_3-c_4=0$. To avoid contradicting the assumption that A is a k-fold Sidon set, (x_1,x_2,x_3,x_4) should be a trivial solution of (5). We consider the following cases:

Case 1. If none of c_1,c_2,c_3,c_4 are 0, we consider the possible partitions of $\{1,2,3,4\}$. Since $x_1\neq x_2$ and $x_3\neq x_4$, 1 and 2, respectively 3 and 4, cannot be placed in the same set in the partition. Then the possible partitions are $\{\{1,3\},\{2,4\}\}$, and $\{\{1,4\},\{2,3\}\}$. If the partition is $\{\{1,3\},\{2,4\}\}$, then $c_1-c_3=0$ and $c_2-c_4=0$. It follows that $x_1=x_3$ and $x_2=x_4$, which contradicts that $(x_1,x_2)\neq(x_3,x_4)$ when $(c_1,c_2)=(c_3,c_4)$. The case of $\{\{1,4\},\{2,3\}\}$ is proved symmetrically.

Case 2. If there is exactly one element of c_1,c_2,c_3,c_4 that is equal to 0, say w.l.o.g., $c_1=0$, then the only possible partition of $\{2,3,4\}$ is $\{\emptyset,\{2,3,4\}\}$, which contradicts $x_3\neq x_4$.

Case 3. If there are exactly two elements of c_1,c_2,c_3,c_4 that are equal to 0, w.l.o.g., we may consider the two cases where $c_1=c_2=0$, and $c_1=c_3=0$. If $c_1=c_2=0$, the only possible partition of $\{3,4\}$ is $\{\emptyset,\{3,4\}\}$, which contradicts $x_3\neq x_4$. If $c_1=c_3=0$, the only possible partition of $\{2,4\}$ is $\{\emptyset,\{2,4\}\}$. Then we have $x_2=x_4$. Note that $c_1=c_3=0$ and $c_2=c_4$, and we get a contradiction.

Case 4. If there are exactly three elements of c_1,c_2,c_3,c_4 that are equal to 0, assume w.l.o.g., that $c_2=c_3=c_4=0$ and $c_1\neq 0$. Then we need to partition $\{1\}$. However, such

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

a partition does not exist as $c_1 \neq 0$. Thus, there is no solution to (5). ∎

When $k = 2$, a family of 2-fold Sidon sets is constructed in [20] by removing some elements from Singer difference sets with multiplier 2.

Theorem 19 (Theorem 2.5 in [20]): Let m be a positive integer and $N = 2^{2^{m+1}} + 2^{2^m} + 1$. Then there exists a 2-fold Sidon set $A \subseteq \mathbb{Z}_N$ such that

$$|A| \geqslant \frac{1}{2} N^{1/2} - 3.$$

We immediately get the following corollary.

Corollary 20: Let $0 \leqslant k_- \leqslant k_+ \leqslant 2$ be integers with $k_+ + k_- \geqslant 1$. There is an infinite family of integers n such that $\mathbb{Z}^n$ can be lattice packed by $\mathcal{B}(n, 2, k_+, k_-)$ with density

$$\delta = \frac{\binom{n}{2}(k_+ + k_-)^2 + n(k_+ + k_-) + 1}{(2(k_+ + k_-) + 1)(2n + 6)^2} = \frac{1}{8(2(k_+ + k_-) + 1)} + o(1).$$

Proof: Simply combine Theorem 18 and Theorem 19. ∎

Now, we present a construction for $t = 2$ and $0 \leqslant k_- \leqslant k_+ \leqslant 3$, which combines Behrend's method [3] and Ruzsa's method [24] to forbid some specified linear equations.

Theorem 21: Let $0 \leqslant k_- \leqslant k_+ \leqslant 3$ be integers such that $k_+ + k_- \geqslant 1$. Set $\alpha \triangleq \max\{2k_+^2, 3\}$. Let $D \geqslant 2$ and $K \geqslant 1$ be integers, and $p \equiv \pm 5 \pmod{12}$ be a prime such that $(\alpha K + 1)^D \leqslant p$. For each $0 \leqslant m < DK^2$, define

$$C_m \triangleq \left\{ x = \sum_{i=0}^{D-1} x_i (\alpha K + 1)^i \;\middle|\; 0 \leqslant x_i \leqslant K, \sum_{i=0}^{D-1} x_i^2 = m \right\}.$$

Let $G \triangleq \mathbb{Z}_{3k_+ + 2k_- + 1} \times \mathbb{Z}_p \times \mathbb{Z}_p$, and construct a subset

$$S_m \triangleq \{ s_x \mid x \in C_m \}, \text{ where } s_x \triangleq (1, x, x^2) \in G.$$

If $k_+ \leqslant 3$, then $G \geqslant M \diamond_2 S_m$ for every $0 \leqslant m < DK^2$, and where $M \triangleq [-k_-, k_+]^*$.

Proof: Suppose to the contrary that G is not partially 2-split by S_m. We consider the following cases.

Case 1. $as_x = \mathbf{0}$ for some $a \in M$ and $x \in C_m$. The first coordinate of this equation is $a \equiv 0 \pmod{3k_+ + 2k_- + 1}$. Since $-k_- \leqslant a \leqslant k_+$, necessarily $a = 0$, a contradiction.

Case 2. $as_x = bs_y$ for some $a, b \in M$, $x, y \in C_m$ and $(a, x) \neq (b, y)$. Similarly to Case 1, the first coordinate implies that $a = b$. From the second coordinate, we have $ax \equiv by \pmod{p}$, and so, $x \equiv y \pmod{p}$. It follows that $x = y$ as $0 \leqslant x, y < p$, which contradicts $(a, x) \neq (b, y)$.

Case 3. $as_x + bs_y = \mathbf{0}$ for some $a, b \in M$, $x, y \in C_m$ and $x \neq y$. The first coordinate implies $a + b = 0$ as $-2k_- \leqslant a + b \leqslant 2k_+$. W.l.o.g., we assume $a > 0$. Then $as_x = (-b)s_y$, where $0 < a, -b \leqslant k_-$, which was ruled out in Case 2.

Case 4. $as_x + bs_y = cs_u$ for some $a, b, c \in M$ and $x, y, u \in C_m$ with $x \neq y$. From the first coordinate, we have $a+b = c$ as $-2k_- \leqslant a+b \leqslant 2k_+$ and $-k_- \leqslant c \leqslant k_+$. If $x = u$ or $y = u$, then $bs_y = bs_u$ or $as_x = as_u$, respectively, both of which were ruled out in Case 2. Thus, in the following, we assume x, y, u are pairwise distinct. Furthermore, using the condition $a + b = c$ and rearranging the terms, we may assume that $a, b, c > 0$.

From the second coordinate, we have that $ax + by \equiv cu \pmod{p}$, or equivalently,

$$\sum_{i=0}^{D-1} (ax_i + by_i)(\alpha K + 1)^i \equiv \sum_{i=0}^{D-1} cu_i (\alpha K + 1)^i \pmod{p}.$$

Note that $0 \leqslant ax_i + by_i, cu_i \leqslant 2k_+ K < \alpha K + 1$ and $p \geqslant (\alpha K + 1)^D$. It follows that $ax_i + by_i = cu_i$ for all $0 \leqslant i \leqslant D - 1$. Thus, the three distinct points $(x_0, x_1, \ldots, x_{D-1})$, $(y_0, y_1, \ldots, y_{D-1})$, and $(u_0, u_1, \ldots, u_{D-1})$, are collinear in $\mathbb{Z}^D$ where $D \geqslant 2$, which contradicts the fact that they are on the same sphere, i.e., $\sum_i x_i^2 = \sum_i y_i^2 = \sum_i u_i^2 = m$.

Case 5. $as_x + bs_y = cs_u + ds_v$ for some $a, b, c, d \in M$, $x, y, u, v \in C_m$, $x \neq y$ and $u \neq v$, where $abcd$ is negative. By rearranging the terms, we may assume w.l.o.g. that

$$as_x + bs_y + cs_z = ds_u$$

for some $0 < a, b, c, d \leqslant k_+$ and $x, y, z, u \in C_m$ where x, y, z, u are not all the same.

Note that $0 < a + b + c \leqslant 3k_+$ and $0 < d \leqslant k_+$. From the first coordinate of the equation above we have $a + b + c = d$. The second coordinate of the equation implies that

$$\sum_{i=0}^{D-1} (ax_i + by_i + cz_i)(\alpha K + 1)^i \equiv \sum_{i=0}^{D-1} du_i (\alpha K + 1)^i \pmod{p}.$$

Since $0 \leqslant ax_i + by_i + cz_i \leqslant 3k_+ K < \alpha K + 1$ and $0 \leqslant du_i \leqslant k_+ K < \alpha K + 1$, necessarily $ax_i + by_i + cz_i = du_i$ for all $0 \leqslant i \leqslant D - 1$. Then

$$\begin{aligned}
&ax_i^2 + by_i^2 + cz_i^2 \\
&= a(x_i - u_i + u_i)^2 + b(y_i - u_i + u_i)^2 + c(z_i - u_i + u_i)^2 \\
&= a(x_i - u_i)^2 + 2a(x_i - u_i)u_i + au_i^2 + b(y_i - u_i)^2 \\
&\quad + 2b(y_i - u_i)u_i + bu_i^2 + c(z_i - u_i)^2 + 2c(z_i - u_i)u_i + cu_i^2 \\
&= a(x_i - u_i)^2 + b(y_i - u_i)^2 + c(z_i - u_i)^2 \\
&\quad + 2(ax_i + by_i + cz_i)u_i - (a + b + c)u_i^2 \\
&= a(x_i - u_i)^2 + b(y_i - u_i)^2 + c(z_i - u_i)^2 + (a + b + c)u_i^2.
\end{aligned}$$

Note that $x, y, z, u \in C_m$, i.e., $\sum_{i=0}^{D-1} x_i^2 = \sum_{i=0}^{D-1} y_i^2 = \sum_{i=0}^{D-1} z_i^2 = \sum_{i=0}^{D-1} u_i^2$. It follows that

$$\begin{aligned}
&(a + b + c) \sum_{i=0}^{D-1} u_i^2 \\
&= a \sum_{i=0}^{D-1} x_i^2 + b \sum_{i=0}^{D-1} y_i^2 + c \sum_{i=0}^{D-1} z_i^2 \\
&= a \sum_{i=0}^{D-1} (x_i - u_i)^2 + b \sum_{i=0}^{D-1} (y_i - u_i)^2 \\
&\quad + c \sum_{i=0}^{D-1} (z_i - u_i)^2 + (a + b + c) \sum_{i=0}^{D-1} u_i^2,
\end{aligned}$$

which in turn implies that $x_i = y_i = z_i = u_i$ for all $0 \leqslant i \leqslant D - 1$, and so, $x = y = z = u$, a contradiction.

Case 6. $as_x + bs_y = cs_u + ds_v$ for some $a, b, c, d \in M$, $x, y, u, v \in C_m$, $x \neq y$ and $u \neq v$, where $abcd$ is positive. Note that from the first coordinate, we have $a + b = c + d$.

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

By rearranging the terms, we may assume that

$$as_x + bs_y = cs_u + ds_v$$

for some $0 < a, b, c, d \leqslant k_+$, $a + b = c + d$, $x, y, u, v \in C_m$ and x, y, u, v are not all the same. The second coordinate and the third coordinate of the equation above imply that

$$ax + by \equiv cu + dv \pmod p \tag{6}$$

and

$$ax^2 + by^2 \equiv cu^2 + dv^2 \pmod p. \tag{7}$$

We multiply (7) by $a + b$, and then subtract the square of (6). Noting that $a + b = c + d$, the result is

$$ab(x - y)^2 \equiv cd(u - v)^2 \pmod p. \tag{8}$$

If $x = y$, using (6) and (8), it is easy to see that x, y, u, v are all the same, a contradiction; if $x = u$, then (6) was ruled out in Case 4. Thus, we may assume that x, y, u, v are pairwise distinct, and so,

$$abcd \equiv c^2d^2(u - v)^2/(x - y)^2 \pmod p, \tag{9}$$

i.e., $abcd$ should be a quadratic residue modulo p.

Check all the possible $abcd$, where $0 < a, b, c, d \leqslant k_+ \leqslant 3$ and $a+b = c+d$. We have $abcd \in \{1, 2^2, 3^2, 4^2, 6^2, 9^2, 3 \cdot 2^2\}$. Since $p \equiv \pm 5 \pmod{12}$, 3 is not a quadratic residue modulo p, and so, $abcd \in \{1, 2^2, 3^2, 4^2, 6^2, 9^2\}$. In all of these cases, $abcd$ is a square in $\mathbb{Z}$. Denote $t = \sqrt{abcd}$. Since $0 < a, b, c, d \leqslant k_+$, we have $0 < t \leqslant k_+^2$. Substituting $abcd = t^2$ in (9) yields

$$\pm t(x - y) \equiv cd(u - v) \pmod p. \tag{10}$$

Solving the system of equations (6) and (10), we get

$$(c^2 + cd)u \equiv (\pm t + ac)x + (bc \mp t)y \pmod p.$$

Note that $a + b = c + d$. Hence,

$$\begin{aligned}&\sum_{i=0}^{D-1}(ac + bc)u_i(\alpha K + 1)^i\\ \equiv &\sum_{i=0}^{D-1}((\pm t + ac)x_i + (bc \mp t)y_i)(\alpha K + 1)^i \pmod p.\end{aligned} \tag{11}$$

Since $(\pm t + ac) + (bc \mp t) = ac + bc > 0$, at least one of $\pm t + ac$ and $bc \mp t$ is positive. We proceed in the following subcases.

1) If $\pm t + ac = 0$, we have $t = ac$, and so,

$$\begin{aligned}&\sum_{i=0}^{D-1}(ac + bc)u_i(\alpha K + 1)^i\\ \equiv &\sum_{i=0}^{D-1}(bc + ac)y_i(\alpha K + 1)^i \pmod p,\end{aligned}$$

which in turn implies $u = y$, a contradiction.
Similarly, if $bc \mp t = 0$, we can get $u = x$, again, a contradiction.

2) If both $\pm t + ac$ and $bc \mp t$ are positive, then $0 \leqslant (\pm t + ac)x_i + (bc \mp t)y_i \leqslant (ac+bc)K \leqslant 2k_+^2\ K \leqslant \alpha K$. On the other hand, $0 \leqslant (ac + bc)u_i \leqslant 2k_+^2\ K \leqslant \alpha K$. Thus it follows from (11) that

$$(ac+bc)u_i = (\pm t+ac)x_i+(bc\mp t)y_i \text{ for all } 0\leqslant i\leqslant D-1.$$

That is, the three distinct points $(x_0, x_1, \ldots, x_{D-1})$, $(y_0, y_1, \ldots, y_{D-1})$ and $(u_0, u_1, \ldots, u_{D-1})$ of $\mathbb{F}_p^D$ are collinear, which contradicts the fact that they are on the same sphere.

3) If $\pm t + ac$ is negative, then $bc \mp t$ is positive. Rearranging the terms in (11), we have that

$$\begin{aligned}&\sum_{i=0}^{D-1}((ac + bc)u_i - (\pm t + ac)x_i)(\alpha K + 1)^i\\ \equiv &\sum_{i=0}^{D-1}(bc \mp t)y_i(\alpha K + 1)^i \pmod p.\end{aligned}$$

Since

$$\begin{aligned}0 &\leqslant (ac + bc)u_i - (\pm t + ac)x_i\\ &= (ac + bc)u_i + (\mp t - ac)x_i\\ &\leqslant (ac + bc)K + (\mp t - ac)K\\ &= (bc \mp t)K \leqslant 2k_+^2\ K \leqslant \alpha K,\end{aligned}$$

then

$$(ac + bc)u_i - (\pm t + ac)x_i = (bc \mp t)y_i$$

for all $0 \leqslant i \leqslant D - 1$. Again we get three distinct points on the same sphere which are collinear, a contradiction.

4) If $bc \mp t$ is negative, then $\pm t + ac$ is positive. Using the same argument as above, we can get the contradiction.

Thus we complete our proof. ■

Remark: In the proof above, the product $abcd$ is required to be either a square of $\mathbb{Z}$ or a non quadratic residue modulo p. This requirement comes from Ruzsa's method, in the proof of Theorem of 7.3 of [24]. However, for $k_+ \geqslant 4$, this requirement cannot be satisfied: we may choose (a, b, c, d) to be $(1, 4, 2, 3), (1, 3, 2, 2)$ or $(2, 4, 3, 3)$, the products $24, 12$ and 72 are not squares and they cannot simultaneously be non quadratic residues modulo p for any prime p as, using the Legendre symbol,

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right).$$

Corollary 22: Let $t = 2$ and $0\leqslant k_-\leqslant k_+ \leqslant 3$, $k_++k_-\geqslant 1$. There is an infinite family of n such that $\mathbb{Z}^n$ can be lattice packed by $\mathcal{B}(n, t, k_+, k_-)$ with density $\delta = \Omega(c^{-\sqrt{\ln n}})$ for some real number $c > 0$.

Proof: Let $p \equiv \pm 5 \pmod{12}$ be a sufficiently large prime. Set $D \triangleq \lfloor\sqrt{\ln p}\rfloor$ and $K \triangleq \lfloor(e^D - 1)/\alpha\rfloor$. Then we have $(\alpha K + 1)^D \leqslant p$. Consider the group G and the splitting sets S_m, $m \in [0, DK^2 - 1]$, in Theorem 21. According to the pigeonhole principle, there exists one set S_m of size $\geqslant \frac{(K+1)^D}{DK^2}$. Then

$$\begin{aligned}n &\geqslant \frac{(K + 1)^D}{DK^2} = \frac{\left(\left\lfloor\frac{e^D-1}{\alpha}\right\rfloor + 1\right)^D}{D\left\lfloor\frac{e^D-1}{\alpha}\right\rfloor^2} \geqslant \frac{\left(\frac{e^D-\alpha}{\alpha} + 1\right)^D}{D\left(\frac{e^D-1}{\alpha}\right)^2}\\ &\geqslant \frac{\alpha^2\ e^{D^2}}{\alpha^D De^{2D}} \geqslant \frac{\alpha^2\ e^{\lfloor\sqrt{\ln p}\rfloor^2}}{\alpha^{\sqrt{\ln p}}\sqrt{\ln p}e^{2\sqrt{\ln p}}}\end{aligned}$$

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

$$\geqslant \frac{\alpha^2\ e^{\left(\sqrt{\ln p}-1\right)^2}}{\alpha^{\sqrt{\ln p}}\sqrt{\ln p}e^{2\sqrt{\ln p}}} = \frac{e\alpha^2\ p}{\alpha^{\sqrt{\ln p}}\sqrt{\ln p}e^{4\sqrt{\ln p}}}$$
$$\geqslant \frac{p}{c_1^{\sqrt{\ln p}}},$$

for some real number $c_1 > 0$. Taking logarithm of both side, we have $\ln n \geqslant \ln p - \sqrt{\ln p}\ln c_1$, or equivalently,

$$\ln p - \ln c_1 \sqrt{\ln p} - \ln n \leqslant 0.$$

Solving for $\sqrt{\ln p}$, we get

$$\sqrt{\ln p} \leqslant \frac{\ln c_1 + \sqrt{(\ln c_1)^2 + 4\ln n}}{2},$$

and so

$$\ln p \leqslant \frac{4\ln n + 2(\ln c_1)^2 + 2\ln c_1\sqrt{(\ln c_1)^2 + 4\ln n}}{4}$$
$$\leqslant \ln n + c_2\sqrt{\ln n},$$

for some real number $c_2 > 0$. It follows that

$$n \geqslant \frac{p}{e^{c_2\sqrt{\ln n}}},$$

and

$$\delta \geqslant \frac{\binom{n}{2}(k_+ + k_-)^2 + n(k_+ + k_-) + 1}{|G|} = \Omega(c^{-\sqrt{\ln n}}),$$

for some real number $c > 0$. ■

IV. Generalized Packings

It is a common practice in coding theory to also consider list decoding instead of unique decoding. In such scenarios, the channel output is decoded to produce a list of up to λ possible distinct codewords, where the channel output is within the error balls centered at each of these codewords. In this section, we therefore generalize the concept of packing to work in conjunction with list decoding. The trade-off we present here is that at the price of a constant-sized list, λ, we can find lattice arrangements of $\mathcal{B}(n,t,k_+,k_-)$ with density almost constant, $\Omega(n^{-\epsilon})$, for any $\epsilon > 0$. The proof method, however, is non-constructive, and relies on the probabilistic method. We note that for sufficiently small $k'_+ \leqslant k_+$ and $k'_- \leqslant k_-$, any lattice arrangement of $\mathcal{B}(n,t,k_+,k_-)$ that induces a list size of λ, is also a lattice packing of $\mathcal{B}(n,t,k'_+,k'_-)$ (namely, with unique decoding, or list size $\lambda = 1$). Thus, we may think of list decoding as allowing us to "decode beyond half the minimum distance", as it does in the Hamming metric. Unfortunately, since our result is based on the probabilistic method, it is hard to determine the best k'_+ and k'_-. Nevertheless, this approach, with almost constant density $\Omega(n^{-\epsilon})$ for any $\epsilon > 0$, improves upon the general construction with unique decoding that was presented in Corollary 8, whose density approaches 0 faster.

Given a shape $\mathcal{B} \subseteq \mathbb{Z}^n$ and a lattice $\Lambda \subseteq \mathbb{Z}^n$, we say $\mathcal{B}$ *λ-packs* $\mathbb{Z}^n$ *by* Λ if for every element $\mathbf{z} \in \mathbb{Z}^n$, there are at most λ distinct elements $\mathbf{v}_i \in \Lambda$ such that $\mathbf{z} \in \mathbf{v}_i + \mathcal{B}$. Obviously, if $\lambda = 1$, this definition coincides with the packing defined in Section II.

Let G be a finite Abelian group, $M \triangleq [-k_-, k_+]^*$, and $S \subseteq G$. If each element of G can be written in at most λ ways as a linear combination of t elements of S with coefficients from $M \cup \{0\}$, then we say $G \overset{\lambda}{\geqslant} M \diamond_t S$.

The following result is an analogue of Theorem 2, which relates lattice packings to Abelian groups. The proof is exactly analogous, and we omit it.

Theorem 23: Let G be a finite Abelian group and $M \triangleq [-k_-, k_+]^*$. Suppose that there is a subset $S = \{s_1, s_2, \dots, s_n\} \subseteq G$ such that $G \overset{\lambda}{\geqslant} M \diamond_t S$. Define $\phi : \mathbb{Z}^n \to G$ as $\phi(\mathbf{x}) \triangleq \mathbf{x} \cdot (s_1, \dots, s_n)$ and let $\Lambda \triangleq \ker\phi$ be a lattice. Then $\mathcal{B}(n,t,k_+,k_-)$ λ-packs $\mathbb{Z}^n$ by Λ.

We use the probabilistic approach detailed in [34], and follow some of the notation there. Let $x_1, x_2, \dots, x_N$ be independent $\{0,1\}$ random variables. Let $Y = Y(x_1, x_2, \dots, x_N)$ be a polynomial of $x_1, x_2, \dots, x_N$. Y is *normal* if its coefficients are between 0 and 1. A polynomial Y is *simplified* if every monomial is a product of different variables. Since we are dealing with $\{0,1\}$ random variables, every Y has a unique simplification. Given a set A, let $\partial_A(Y)$ denote the partial derivative of Y with respect to A, and let ∂^*_A be the polynomial obtained from the partial derivative $\partial_A(Y)$ by subtracting its constant coefficient. Define $\mathbb{E}^*_j(Y) \triangleq \max_{|A|\geqslant j}\mathbb{E}(\partial^*_A Y)$.

Theorem 24 ([34, Corollary 4.9]): For any positive constants α and β and a positive integer d, there is a positive constant $C = C(d,\alpha,\beta)$ such that if Y is a simplified normal polynomial of degree at most d and $\mathbb{E}^*_0(Y) \leqslant N^{-\alpha}$, then $\Pr(Y \geqslant C) \leqslant N^{-\beta}$.

We now use Theorem 24 to show the existence of generalized lattice packings with the desired parameters.

Theorem 25: Let $0 \leqslant k_- \leqslant k_+$ with $k_+ + k_- \geqslant 1$, and $t > 0$, be integers. Let N be a sufficiently large integer such that $\gcd(N, k_+!) = 1$, and fix $G \triangleq \mathbb{Z}_N$. Then for any $0 < \epsilon < 1/t$, there is a number λ which only depends on t and ϵ, and a subset $S = \{s_1, s_2, \dots, s_n\} \subseteq G$ with $\frac{1}{2}N^{1/t-\epsilon} \leqslant n \leqslant \frac{3}{2}N^{1/t-\epsilon}$, such that $G \overset{\lambda}{\geqslant} M \diamond_t S$, where $M \triangleq [-k_-, k_+]^*$.

Proof: Set $\alpha = \epsilon t$, $\beta = 2$, and $d = t$. Denote

$$p \triangleq N^{\frac{1}{t}-1-\epsilon}.$$

We construct S randomly. For each $0 \leqslant i < N$, let the event $i \in S$ be independent with probability p. Let x_i be the indicator variable of the event $i \in S$. Then $|S| = \sum_{i=0}^{N-1} x_i$, and

$$\mathbb{E}(|S|) = Np = N^{\frac{1}{t}-\epsilon}.$$

Using Chernoff's inequality, one can show that

$$\Pr\left(\frac{1}{2}\mathbb{E}(|S|) \leqslant |S| \leqslant \frac{3}{2}\mathbb{E}(|S|)\right) \geqslant 1 - 2e^{-\mathbb{E}(|S|)/16}. \quad (12)$$

For every $g \in G$ and $0 \leqslant i_1 < i_1 < \dots < i_\ell < N$, denote

$$c(g; i_1, i_2, \dots, i_\ell)$$
$$\triangleq \left|\left\{(a_1, a_2, \dots, a_\ell) \in M^\ell \mid g = a_1 i_1 + a_2 i_2 + \cdots a_\ell i_\ell\right\}\right|,$$

where addition and multiplication are in $G = \mathbb{Z}_N$. Consider the following random variables (which are polynomials in the indicator random variables $x_0, \dots, x_{N-1}$),

$$Y_g \triangleq \sum_{0\leqslant i_1<\cdots<i_t<N} \frac{c(g; i_1, i_2, \dots, i_t)}{(k_+ + k_-)^t} x_{i_1} x_{i_2} \cdots x_{i_t},$$

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

and

$$Z_g \triangleq \sum_{\substack{1\leqslant \ell\leqslant t-1\\ 0\leqslant i_1<\cdots<i_\ell<N}} \frac{c(g;i_1,i_2,\dots,i_\ell)}{(k_++k_-)^{t-1}} x_{i_1}x_{i_2}\cdots x_{i_\ell}.$$

Both of them are positive, and as polynomials, they are simplified, and normal. To show that $G \overset{\lambda}{\geqslant} M \diamond_t S$, it suffices to show that $(k_++k_-)^t Y_g + (k_++k_-)^{t-1} Z_g \leqslant \lambda - 1$ for every $g \in G$.

We first look at Y_g. Since $\gcd(N, k_+!) = 1$, if we fix $a_1, a_2, \dots, a_t \in M^t$ and $i_1, i_2, \dots, i_{t-1}$, then there is a unique $i_t \in [0, N-1]$ such that $a_1 i_1 + a_2 i_2 + \cdots + a_t i_t = g$. Hence,

$$\mathbb{E}(Y_g) \leqslant ((k_++k_-)^t N^{t-1} p^t)/(k_++k_-)^t = N^{-\epsilon t} = N^{-\alpha}.$$

For the partial derivative $\partial_A(Y_g)$ with $A = \{j_1, j_2, \dots, j_k\} \subseteq [0, N-1]$ and $k \leqslant t-1$,

$$\partial_A(Y_g) = \sum_{\substack{0\leqslant i_1<\cdots<i_{t-k}<N\\ \{i_1,\dots,i_{t-k}\}\cap A=\varnothing}} \frac{c_A(g;i_1,\dots,i_{t-k})}{(k_++k_-)^t} x_{i_1}\cdots x_{i_{t-k}},$$

where

$$c_A(g;i_1,\dots,i_{t-k}) = \sum_{c_1,c_2,\dots,c_k\in M} c(g - c_1 j_1 - \cdots - c_k j_k; i_1,\dots,i_{t-k}).$$

Hence,

$$\mathbb{E}(\partial_A(Y_g)) \leqslant (k_++k_-)^k \frac{(k_++k_-)^{t-k} N^{t-k-1} p^{t-k}}{(k_++k_-)^t} = N^{-\epsilon t + k\epsilon - k/t} < N^{-\alpha}.$$

Applying Theorem 24, there is a number C, depending on t and ϵ, such that

$$\Pr(Y_g \geqslant C) \leqslant N^{-2}. \tag{13}$$

As for Z_g, a similar computation to the above shows that

$$\mathbb{E}(\partial_A^*(Z_g)) = O(N^{t-1-k-1} p^{t-1-k}).$$

Since

$$N^{t-1-k-1} p^{t-1-k} = N^{-\epsilon t - (\frac{1}{t}-\epsilon)(k+1)} < N^{-\alpha},$$

we have $\mathbb{E}(\partial_A^*(Z_g)) < N^{-\alpha}$ when N is sufficiently large. Applying Theorem 24 again, there is a C' such that

$$\Pr(Z_g \geqslant C') \leqslant N^{-2}. \tag{14}$$

Denote $\lambda = C(k_++k_-)^t + C'(k_++k_-)^{t-1} + 1$. Then (13) and (14) imply, via a union bound, that the probability that there exists $g \in G$ such that $(k_++k_-)^t Y_g + (k_++k_-)^{t-1} Z_g > \lambda - 1$ is at most $2N^{-1}$. From this, together with (12), we can see that the random set S satisfies the conditions with probability at least $1 - 2N^{-1} - 2e^{-\mathbb{E}(|S|)/16}$, which is positive for large enough N. Thus, such a set exists. ∎

Corollary 26: Let $0 \leqslant k_- \leqslant k_+$ with $k_+ + k_- \geqslant 1$, and $t > 0$, be integers. Then for any real number $\epsilon > 0$, there is an integer λ and infinitely many values of n such that $\mathbb{Z}^n$ can be λ-lattice-packed by $\mathcal{B}(n,t,k_+,k_-)$ with density $\delta = \Omega(n^{-\epsilon})$.

Proof: Fix $\epsilon' \triangleq \frac{\epsilon}{\epsilon t + t^2}$, and observe that $\epsilon' < 1/t$. Use Theorem 25 with ϵ', noting that $N = \Theta(n^{\epsilon + t})$, to obtain a lattice λ-packing of $\mathcal{B}(n,t,k_+,k_-)$ with density

$$\delta \geqslant \frac{|\mathcal{B}(n,t,k_+,k_-)|}{|G|} = \frac{\sum_{i=0}^t \binom{n}{i}(k_++k_-)^i}{N} = \Omega(n^{-\epsilon}).$$

∎

As a final comment on the matter, we observe that a tedious calculation shows that in the above corollary $\lambda = O(\epsilon^{-t})$ – a calculation which we omit.

V. Constructions of Lattice Coverings

We switch gears in this section, and focus on covering instead of packing. We first argue that using known techniques from the theory of covering codes in the Hamming metric, we can show the existence of non-lattice coverings of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,k_+,k_-)$. However, these have a high density of $\Omega(n)$. We then provide a product construction to obtain a lattice covering by $\mathcal{B}(n,t,k_+,k_-)$ with density $O(1)$.

Fixing an integer $\ell \in \mathbb{N}$, we use the same argument as the one given in [8, Section 12.1] to construct a covering code $C \subseteq \mathbb{Z}_\ell^n$, of size

$$|C| = \left\lceil \frac{n\ell^n \ln \ell}{|\mathcal{B}(n,t,k_+,k_-)|} \right\rceil.$$

We can then translate this covering of $\mathbb{Z}_\ell^n$ by $\mathcal{B}(n,t,k_+,k_-)$ to a covering of $\mathbb{Z}^n$ by using the same idea as Theorem 5, and defining $C' \triangleq \{\mathbf{x} \in \mathbb{Z}^n \mid (\mathbf{x} \bmod \ell) \in C\}$. However, the density of the resulting covering is

$$\delta = \frac{|C| \cdot |\mathcal{B}(n,t,k_+,k_-)|}{\ell^n} = \Omega(n).$$

We therefore proceed to consider more efficient coverings using the product construction whose details follow.

Theorem 27: Suppose that there exist a finite Abelian group G and a subset $S \subseteq G$ such that $G \leqslant M \diamond_1 S$. Let $t > 0$ be an integer, and denote

$$S^{(t)} \triangleq \{(s,0,0,\dots,0) \mid s \in S\} \cup \{(0,s,0,\dots,0) \mid s \in S\} \cup \cdots \cup \{(0,0,0,\dots,s) \mid s \in S\}.$$

Then $G^t \leqslant M \diamond_t S^{(t)}$.

Proof: For any element $g = (g_1, g_2, \dots, g_t) \in G^t$, since $G \leqslant M \diamond_1 S$, for each $1 \leqslant i \leqslant t$, there are $s_i \in S$ and $c_i \in M \cup \{0\}$ such that $g_i = c_i \cdot s_i$. Hence,

$$g = c_1(s_1,0,0,\dots,0) + c_2(0,s_2,0,\dots,0) + \cdots + c_t(0,0,0,\dots,s_t).$$

That is, g can be written as a linear combination of t elements of S with coefficients from $M \cup \{0\}$, and so, $G^t \leqslant M \diamond_t S^{(t)}$. ∎

We can now construct a lattice covering, using the previous theorem.

Corollary 28: Let $\overline{\psi}(x)$ be the largest prime not larger than x, and denote $p \triangleq \overline{\psi}(k_+ + k_- + 1)$. Let $0 \leqslant k_- \leqslant k_+$, with $k_+ + k_- \geqslant 1$, and $t > 0$, be integers. Define $M \triangleq [-k_-, k_+]^*$. Then for any integer $m > 0$, there exists $S \subseteq (\mathbb{Z}_{p^m})^t$, $|S| = t \cdot \frac{p^m - 1}{p-1}$, such that $(\mathbb{Z}_{p^m})^t \leqslant M \diamond_t S$, and thereby, a lattice covering of $\mathbb{Z}^n$, $n = |S|$, with density

$$\delta = \frac{\sum_{i=0}^t \binom{n}{i}(k_++k_-)^i}{(n(p-1)/t+1)^t} = \frac{(t(k_++k_-))^t}{t!(p-1)^t} + o(1).$$

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

TABLE I

A SUMMARY OF THE RESULTS

Type	t	k_+	k_-	density	Location	Comment
Packing	any	1	0	$\frac{1}{t!}+o(1)$	Corollary 8	via BCH codes
Packing	any	any	any	$\Theta(n^{t-\lceil 2t(1-1/p)\rceil})$	Corollary 8	via BCH codes, $p \geqslant k_+ + k_- + 1$ prime
Packing	any	1	0	$\frac{1}{t!}+o(1)$	Corollary 15	via $B_t[N;1]$ sets
Packing	any	1	1	$\frac{2^t}{t!(2t+1)}+o(1)$	Corollary 17	via $B_t[N;1]$ sets
Packing	2	1	0	$1-o(1)$	Corollary 12	via Preparata codes, non-lattice packing
Packing	2	1	1	$\frac{1}{2}+o(1)$	Corollary 9	via quasi-perfect linear codes
Packing	2	2	0	$\frac{1}{2}+o(1)$	Corollary 9	via quasi-perfect linear codes
Packing	2	$\leqslant 2$	$\leqslant 2$	$\frac{1}{8(2(k_++k_-)+1)}+o(1)$	Corollary 20	via 2-fold Sidon sets
Packing	2	$\leqslant 3$	$\leqslant 3$	$\Omega(c^{-\sqrt{\ln n}})$	Corollary 22	via Behrend's and Ruzsa's methods
λ-Packing	any	any	any	$\Omega(n^{-\epsilon})$	Corollary 26	$\lambda = O(\epsilon^{-t})$
Covering	any	any	any	$\frac{(t(k_++k_-))^t}{t!(p-1)^t}+o(1)$	Corollary 28	$p \leqslant k_+ + k_- + 1$ prime

Proof: According to [25, Construction 1], there is a subset $A \subseteq \mathbb{Z}_{p^m}$ of size $\frac{p^m-1}{p-1}$ such that $\mathbb{Z}_{p^m} = [-k_-, p-1-k_-]^* \diamond_1 A$. We may apply Theorem 27 to obtain a subset $S = A^{(t)} \subseteq (\mathbb{Z}_{p^m})^t$ of size $t \cdot \frac{p^m-1}{p-1}$ such that $(\mathbb{Z}_{p^m})^t \leqslant M \diamond_t S$. The calculation of the density of the resulting lattice covering is straightforward. ■

VI. CONCLUSION

Motivated by coding for integer vectors with limited-magnitude errors, we provided several constructions of packings of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,k_+,k_-)$ for various parameters. These are summarized in Table I. While the parameter ranges of the constructions sometimes overlap, and perhaps result in equal or inferior asymptotic density, having more constructions allows for more choices for fixed values of the parameters.

One main goal was to construct lattice packings, analogous to linear codes, as these are generally easier to analyze, encode, and decode. Thus, except for one case, all constructions we provide are lattices. The main tool in constructing these is the connection between lattice packings of $\mathcal{B}(n,t,k_+,k_-)$ and t-splittings of Abelian groups. The other important goal was to have asymptotic packing density that is non-vanishing. This is achieved in many of the cases.

We also discussed λ-packing, which allows for a small overlap between the translates of $\mathcal{B}(n,t,k_+,k_-)$ centered at the lattice points. This is useful for list-decoding setting with a list size of λ. The result we obtain is non-constructive, and it provides a trade-off between the list size and the packing density. Finally, we also addressed the problem of lattice-covering of $\mathbb{Z}^n$ by $\mathcal{B}(n,t,k_+,k_-)$, showing using the product construction, that there exist such coverings with asymptotic constant density.

The results still leave numerous open questions, of which we mention but a few:

1) Constructions for packings of $\mathcal{B}(n,t,k_+,k_-)$ with $t \geqslant 3$, $k_+ \geqslant 2$, and non-vanishing asymptotic density are still unknown.
2) Whether asymptotic density of 1 is attainable for all parameters is still an open questions. Such lattice packings would be analogous to asymptotically perfect codes.
3) In the asymptotic regime of $t = \Theta(n)$, all of the constructions in this paper produce packings with vanishing asymptotic rates. Such families of packings are analogous to good codes in the Hamming metric, and their existence and constructions would be most welcome.
4) Efficient decoding algorithms are missing for most of the cases. In the asymptotic regime of constant t, $|\mathcal{B}(n,t,k_+,k_-)| = \Theta(n^t)$. Thus, we are looking for non-trivial decoding algorithms, whose run-time is $o(n^t)$.
5) We would also like to find constructive versions of the non-constructive proofs for λ-packings, and covering lattices.

REFERENCES

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1183–1188, Mar. 2007.

[2] R. C. Baker, G. Harman, and J. Pintz, "The difference between consecutive primes, II," *Proc. London Math. Soc.*, vol. 83, no. 3, pp. 532–562, Nov. 2001.

[3] F. A. Behrend, "On sets of integers which contain no three terms in arithmetical progression," *Proc. Nat. Acad. Sci. USA*, vol. 32, no. 12, p. 331, 1946.

[4] R. C. Bose and S. Chowla, "Theorems in the additive theory of numbers," *Commentarii Math. Helvetici*, vol. 37, no. 1, pp. 141–147, Dec. 1962.

[5] S. Buzaglo and T. Etzion, "Tilings with N-dimensional chairs and their applications to asymmetric codes," *IEEE Trans. Inf. 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 application to multilevel flash memories," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1582–1595, Apr. 2010.

[7] Z. Chen, I. E. Shparlinski, and A. Winterhof, "Covering sets for limited-magnitude errors," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5315–5321, Sep. 2014.

[8] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.

[9] D. Danev and S. Dodunekov, "A family of ternary quasi-perfect BCH codes," *Designs, Codes Cryptogr.*, vol. 49, nos. 1–3, pp. 265–271, Dec. 2008.

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.

[10] I. Gashkov and V. Sidel'nikov, "Linear ternary quasiperfect codes that correct double errors," *Problemy Peredachi Inf.*, vol. 22, no. 4, pp. 43–48, 1986.
[11] W. Hamaker and S. Stein, "Combinatorial packing of R^3 by certain error spheres," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 2, pp. 364–368, Mar. 1984.
[12] K. Haymaker and C. A. Kelley, "Covering codes for multilevel flash memories," in *Proc. 6th Asilomar Conf. Signals, Syst. Comput. (ASILOMAR)*, Pacific Grove, CA, USA, Nov. 2012, pp. 942–949.
[13] D. Hickerson and S. Stein, "Abelian groups and packing by semicrosses," *Pacific J. Math.*, vol. 122, no. 1, pp. 95–109, Mar. 1986.
[14] 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.
[15] A. Jiang, V. Bohossian, and J. Bruck, "Rewriting codes for joint information storage in flash memories," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 5300–5313, Oct. 2010.
[16] T. Klove, "Two constructions of covering sets for limited-magnitude errors," *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1177–1182, Mar. 2016.
[17] T. Klove, 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.
[18] T. Kløve and M. Schwartz, "Linear covering codes and error-correcting codes for limited-magnitude errors," *Des., Codes Cryptogr.*, vol. 73, no. 2, pp. 329–354, Nov. 2014.
[19] A. V. Kuznetsov and A. J. H. Vinck, "A coding scheme for single peak-shift correction in (d,k)-constrained channels," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1440–1450, Jul. 1993.
[20] F. Lazebnik and J. Verstraëte, "On hypergraphs of girth five," *Electron. J. Combinatorics*, vol. 10, no. 1, p. 25, May 2003.
[21] V. I. Levenshtein and A. J. H. Vinck, "Perfect (d,k)-codes capable of correcting single peak-shifts," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 656–662, Mar. 1993.
[22] C. Li and T. Helleseth, "Quasi-perfect linear codes from planar and APN functions," *Cryptogr. Commun.*, vol. 8, no. 2, pp. 215–227, Apr. 2016.
[23] F. P. Preparata, "A class of optimum nonlinear double-error-correcting codes," *Inf. Control*, vol. 13, no. 4, pp. 378–400, Oct. 1968.
[24] I. Ruzsa, "Solving a linear equation in a set of integers I," *Acta Arithmetica*, vol. 65, no. 3, pp. 259–282, 1993.
[25] M. Schwartz, "Quasi-cross lattice tilings with applications to flash memory," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.
[26] M. Schwartz, "On the non-existence of lattice tilings by quasi-crosses," *Eur. J. Combinatorics*, vol. 36, pp. 130–142, Feb. 2014.
[27] S. Stein, "Factoring by subsets," *Pacific J. Math.*, vol. 22, no. 3, pp. 523–541, Sep. 1967.
[28] S. Stein, "Packings of R^n by certain error spheres," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 2, pp. 356–363, Mar. 1984.
[29] S. Stein, "The notched cube tiles R^n," *Discrete Math.*, vol. 80, no. 3, pp. 335–337, Mar. 1990.
[30] S. Stein and S. Szabó, *Algebra Tiling*. Washington, DC, USA: The Mathematical Association of America, 1994.
[31] U. Tamm, "Splittings of cyclic groups and perfect shift codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 2003–2009, Sep. 1998.
[32] U. Tamm, "On perfect integer codes," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Adelaide, SA, Australia, Sep. 2005, pp. 117–120.
[33] T. Tao and V. Vu, *Additive Combinatorics*. Cambridge, U.K.: Cambridge Univ. Press, 2006.
[34] V. H. Vu, "Concentration of non-lipschitz functions and applications," *Random Struct. Algorithms*, vol. 20, no. 3, pp. 262–316, May 2002.
[35] H. Wei and M. Schwartz, "On tilings of asymmetric limited-magnitude balls," 2020, *arXiv:2006.00198*. [Online]. Available: http://arxiv.org/abs/2006.00198
[36] 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.
[37] 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.
[38] 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.
[39] 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.
[40] T. Zhang, X. Zhang, and G. Ge, "Splitter sets and K-radius sequences," *IEEE Trans. Inf. Theory*, vol. 63, no. 12, pp. 7633–7645, Dec. 2017.

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

He was a Post-Doctoral Fellow with the Capital Normal University, Beijing, China, from 2014 to 2016, and a Research Fellow with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, from 2016 to 2019. He is currently a Post-Doctoral Fellow with the School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Israel. 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.

Xin Wang received the Ph.D. degree in mathematics from Zhejiang University, Hangzhou, Zhejiang, China, in 2017. He is currently an Associate Professor with the Department of Mathematics, Soochow University. His research interests include extremal combinatorics, coding theory, and their interactions.

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 at San Diego, and a Post-Doctoral Researcher with the Department of Electrical Engineering, California Institute of Technology. While on sabbatical from 2012 to 2014, he was the Visiting Scientist with 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 has also been serving as an Associate Editor for Coding Techniques for the IEEE TRANSACTIONS ON INFORMATION THEORY since 2014, and an Editorial Board Member for the *Journal of Combinatorial Theory Series A* since 2021.

Authorized licensed use limited to: Moshe Schwartz. Downloaded on July 17,2021 at 10:22:57 UTC from IEEE Xplore. Restrictions apply.