Covering Sets for Limited-Magnitude Errors*

Torleiv Kløve and Moshe Schwartz

[1] T. Kløve, Department of Informatics, University of Bergen, N-5020 Bergen, Norway. Torleiv.Klove@ii.uib.no
[2] M. Schwartz, Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer Sheva 84105 Israel. schwartz@ee.bgu.ac.il

Abstract. The concept of a covering set for the limited-magnitude error channel is introduced. A number of covering-set constructions, as well as some bounds, are given. In particular, optimal constructions are given for some cases involving small-magnitude errors.

1 Introduction

For integers a, b, where $a \le b$, we let

$$[a, b] = \{a, a+1, a+2, \dots, b\}, \qquad [a, b]^* = \{a, a+1, a+2, \dots, b\} \setminus \{0\}.$$

Throughout this paper, let μ, λ be integers such that $0 \le \mu \le \lambda$, and let q be a positive integer. In the $(\lambda, \mu; q)$ limited-magnitude error channel an element $a \in \mathbb{Z}_q$ can be changed into any element in the set $\{(a+e) \bmod q \mid e \in [-\mu, \lambda]\}$. For convenience we shall also set $M = [-\mu, \lambda]^*$.

For any $S \subseteq \mathbb{Z}_q$ we define $MS = \{xs \in \mathbb{Z}_q \mid x \in M, s \in S\}$, where multiplication is done modulo q. If $|MS| = (\mu + \lambda)|S|$, then S is *packing set.* A packing set S where $MS \subseteq \mathbb{Z}_q \setminus \{0\}$ is a $B[-\mu, \lambda](q)$ set in the terminology of [8].

If $\mathbf{s} = (s_1, s_2, \dots, s_n)$, where $\{s_1, s_2, \dots, s_n\}$ is a $B[-\mu, \lambda](q)$ set, then

$$\left\{\mathbf{x} \in \mathbb{Z}_q^n \mid \mathbf{x} \cdot \mathbf{s} \equiv 0 \pmod{q}\right\}$$

is a code that can correct a single limited-magnitude error from the set $[-\mu, \lambda]$. Such codes have been studied in, e.g., [1]-[6], and [8].

Similar to packing sets, we can consider covering sets, where a set S is called a $(\lambda, \mu; q)$ *covering set* if $|MS| = q$. Thus, covering sets are to packing sets as covering codes are to error-correcting codes. Instead of trying to pack many disjoint translates Ms, $s \in S$, into $\mathbb{Z}_q$, in the covering set scenario we are interested in having the union of Ms, $s \in S$, cover $\mathbb{Z}_q$ entirely with S being as small as possible. Some results where $\mu = 0$ or $\mu = \lambda$ are described in [7]. Apart from its independent intellectual merit, solving this problem for $\mu = 0$ has immediate applications, such as rewriting schemes for non-volatile memories, a simplified version of which we now describe. For a more detailed description the reader is referred to [2] and references therein.

* Supported by The Norwegian Research Council and by ISF grant 134/10.

Consider a set of n flash memory cells, each capable of storing an integer from $\mathbb{Z}$. Let G be some finite abelian group, say $G = \mathbb{Z}_q$, and some subset $S = \{s_1, s_2, \dots, s_n\} \subseteq G$, where we denote $\mathbf{s} = (s_1, s_2, \dots, s_n)$. Define the *decoding* mapping $\mathcal{D} : \mathbb{Z}^n \to \mathbb{Z}_q$ as $\mathcal{D}(\mathbf{x}) = \mathbf{x} \cdot \mathbf{s}$.

If we want to store the value $v \in \mathbb{Z}_q$ in the n memory cells, we choose a vector $\mathbf{x} \in \mathbb{Z}^n$ such that $\mathcal{D}(\mathbf{x}) = v$, and store the i-th component of $\mathbf{x}$ in the i-th cell. If we then want to *rewrite* this value with $v' \in \mathbb{Z}_q$, we can choose a different vector $\mathbf{x'} \in \mathbb{Z}^n$ that decodes to v'. Due to the limitations of flash memory, we would like x'_i to be in the range $[x_i - \mu, x_i + \lambda]$, and to leave as many cells as possible unchanged. In the extreme case, we allow only a single cell to change. To be able to allow any value v to be rewritten with v' while changing the stored integer in a single cell as above, S can be taken to be a $(\lambda, \mu; q)$ covering set. This is because we can write $v' - v = ms_i$ with $m \in [-\mu, \lambda]$, $s_i \in S$, and then choose $\mathbf{x'} = \mathbf{x} + m\mathbf{e_i}$, where $\mathbf{e_i}$ is the i-th standard unit vector. For maximum efficiency, we would like S to be as small as possible.

We say S is a $(\lambda, \mu; q)$ *perfect* covering set if $MS = \mathbb{Z}_q$, $|M|(|S| - 1) = q - 1$, and $0 \in S$. In other words, S is a perfect covering set if, apart from $0 \in S$, the products ms in $\mathbb{Z}_q$, where $m \in M$, $s \in S$, are all distinct, non-zero, and cover all the non-zero elements of $\mathbb{Z}_q$. These are also called abelian group splittings in the terminology of [7].

Similarly, S is a perfect packing set if the products ms in $\mathbb{Z}_q$, where $m \in M$, $s \in S$, are all distinct, non-zero, and cover all the non-zero elements of $\mathbb{Z}_q$. We note that S is a perfect covering if and only if $S \setminus \{0\}$ is a perfect packing set.

The following functions shall be of interest to us:

$$\begin{aligned}
\nu(q, r) = \nu_{\lambda,\mu}(q, r) &= \max_{S \subseteq \mathbb{Z}_q} \{|MS| \mid |S| = r\}, \\
\theta(q) = \theta_{\lambda,\mu}(q) &= \max_{r \in \mathbb{N}} \{r \mid \nu(q, r) = (\mu + \lambda)r\}, \\
\omega(q) = \omega_{\lambda,\mu}(q) &= \min_{r \in \mathbb{N}} \{r \mid \nu(q, r) = q\}.
\end{aligned}$$

Intuitively speaking, $\nu(q, r)$ expresses the maximum coverage of sets of size r, $\theta(q)$ is the maximum size of a packing set, and $\omega(q)$ is the minimum size of a covering set. If S is a $(\lambda, \mu; q)$ covering set of minimal size $\omega_{\lambda,\mu}(q)$, we call S optimal. We first prove some basic monotonicity properties.

Theorem 1. *Let μ' and λ' be integers such that $-\mu \le -\mu' \le 0 \le \lambda' \le \lambda$. Then*

$$\nu_{\lambda',\mu'}(q, r) \le \nu_{\lambda,\mu}(q, r), \quad \theta_{\lambda',\mu'}(q) \ge \theta_{\lambda,\mu}(q), \quad \omega_{\lambda',\mu'}(q) \ge \omega_{\lambda,\mu}(q).$$

Proof. If we denote $M' = [-\mu', \lambda']^*$ then obviously $M' \subseteq M$ and therefore $M'S \subseteq MS$. The claims follow immediately. □

We now give a simple lower bound.

Theorem 2. *We have $\omega_{\lambda,\mu}(q) \ge \left\lceil \frac{q}{\lambda+\mu} \right\rceil$.*

Proof. By definition, there exists an optimal covering set S. Therefore,

$$q = |MS| \le (\lambda+\mu)|S| = (\lambda+\mu)\,\omega_{\lambda,\mu}(q),$$

and the theorem follows. □

Example 1. For $\mu = 0$ and $\lambda = 1$ we clearly have $MS = S$ for all sets S. Hence, $\nu_{1,0}(q,r) = r$ and $\theta_{1,0}(q) = \omega_{1,0}(q) = q$.

Example 2. Let $\mu = \lambda = 1$. For $1 \le r \le \lfloor q/2 \rfloor$ we have $|M[1,r]| = 2r$. Hence, $\nu(q,r) = 2r$. For $\lfloor q/2\rfloor + 1 \le r \le q$ we have $|M[0,r-1]| = q$. Hence, $\nu(q,r) = q$. We can conclude that $\theta_{1,1}(q) = \lfloor q/2 \rfloor$ and $\omega_{1,1}(q) = \lceil q/2 \rceil$.

For $\lambda \ge 2$, it seems to be quite complicated to determine θ and ω in many cases. For $\lambda = 2$, $\theta_{2,0}(q)$ was determined in [4], $\theta_{2,1}(q)$ in [8], and $\theta_{2,2}(q)$ in [5]. In the next sections we consider $\omega_{2,0}(q)$ and $\omega_{2,1}(q)$. Because of the page limitations, our results on $\omega_{2,2}(q)$ is are not given here.

We first give a general BCH-like upper bound.

Theorem 3. *Let p be a prime, and let g be a primitive element in $\mathbb{Z}_p$. If $[-\mu,\lambda]^*$ contains δ consecutive powers of g then $\omega_{\lambda,\mu}(p) \le \lceil \frac{p-1}{\delta} \rceil + 1$.*

Proof. One can easily verify that the set

$$S = \{0\} \cup \left\{ g^{\delta i} \;\middle|\; 0 \le i \le \left\lceil \frac{p-1}{\delta} \right\rceil - 1 \right\}$$

is indeed a $(\lambda,\mu;q)$ covering set. □

Another upper bound is the following.

Theorem 4. *If q and r are odd, then $\omega_{2,\mu}(qr) \le r(\omega_{2,\mu}(q) - 1) + \omega_{2,\mu}(r)$.*

Proof. Let S be an optimal $(2,\mu;q)$ covering set and D an optimal $(2,\mu;r)$ covering set. We remind that $\mu \le \lambda = 2$. Since q is odd, $ac \equiv 0 \pmod q$ for some $a \in [-\mu,2]^*$, only if $c = 0$. Therefore, we must have $0 \in S$. Similarly, $0 \in D$. Let

$$E = \{cq + s \in \mathbb{Z}_{qr} \mid c \in [0, r-1],\, s \in S \setminus \{0\}\} \cup \{qd \in \mathbb{Z}_{qr} \mid d \in D\}\,.$$

Then $|E| = r(\omega_{2,\mu}(q) - 1) + \omega_{2,\mu}(r)$. We will show that E is a $(2,\mu;qr)$ covering set.

First, consider the case $b \in \mathbb{Z}_{qr}$, $b \not\equiv 0 \pmod q$. Let $b_1 \equiv b \pmod q$, $b_1 \in [1, q-1]$, that is $b = mq + b_1$ for some integer m. Furthermore, $b_1 \equiv as \pmod q$ for some $a \in [-\mu,2]^*$ and $s \in S \setminus \{0\}$. That is, $as = m_1 q + b_1$ for some integer m_1. Hence

$$b = mq + (as - m_1 q) = (m - m_1)q + as.$$

Since qr is odd, we note that all the elements of $[-\mu, 2]$ are invertible in $\mathbb{Z}_{qr}$. Thus,

$$b = (m - m_1)q + as \equiv a[a^{-1}(m - m_1)q + s] \pmod{qr}.$$

This shows that $b \in [-\mu,2]^* E$.

Next, consider the case $b \in \mathbb{Z}_{qr}$, $b \equiv 0 \pmod q$. Then $b = qb_2$. There exist $a \in [-\mu,2]^*$ and $d \in D$ such that $b_2 \equiv ad \pmod r$. Hence $b = qb_2 \equiv a(qd) \pmod{qr}$, that is $b \in [-\mu,2]^* E$ also in this case. □

2 Determination of $\omega_{2,0}(q)$

For $S \subseteq \mathbb{Z}_q$ and $(\lambda, \mu) = (2, 0)$, we have $M = [0, 2]^* = \{1, 2\}$ and

$$MS = \bigcup_{s \in S} \{s, 2s\} .$$

First, we consider $q = 2m+1$. For an integer $a \in \mathbb{Z}_{2m+1} \setminus \{0\}$, the corresponding cyclotomic coset is

$$\sigma(a) = \left\{ a2^j \bmod (2m+1) \mid j \geq 0 \right\} .$$

If $2m+1$ is a prime, then all the cosets have the same size. We see that a packing set can contain at most $\lfloor |\sigma(a)| /2 \rfloor$ of the elements in $\sigma(a)$, and we can find a packing set with this many elements. Let $\varsigma(2m+1)$ be the number of cyclotomic cosets of odd size. Then we get

$$\theta_{2,0}(2m+1) = m - \varsigma(2m+1)/2.$$

This is Theorem 7 in [3], where a more detailed proof is given.

Similarly, a covering set must contain at least $\lceil |\sigma(a)| /2 \rceil$ of the elements in $\sigma(a)$, and we can find a covering set with this many elements. Moreover, a covering set must contain 0. Hence

$$\omega_{2,0}(2m+1) = m + 1 + \varsigma(2m+1)/2. \tag{1}$$

An explicit expression for $\varsigma(2m + 1)$ is given as Theorem 2 in [4]. Combining this with (1), we get the following theorem where $\varphi(d)$ is Euler's function and $\mathrm{ord}_p(2)$ is the multiplicative order of 2 modulo p.

Theorem 5. *If $2m+1 = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$ is the prime factorization of $2m+1$, let $q_o = \prod_{\substack{1 \leq i \leq s \\ p_i \in P_o}} p_i^{t_i}$, where P_o is the set of odd primes p such that $\mathrm{ord}_p(2)$ is odd. Then*

$$\omega_{2,0}(2m+1) = m + 1 + \sum_{d \mid q_o, d > 1} \frac{\varphi(d)}{2 \ \mathrm{ord}_d(2)} .$$

In particular, a perfect $(2, 0; 2m + 1)$ set exists if and only if none of the primes dividing $2m + 1$ belongs to P_o.

Theorem 6. *For $m \geq 0$ we have $\omega_{2,0}(4m + 2) = 2m + 1$.*

Proof. By Theorem 2, $\omega_{2,0}(4m+2) \geq 2m+1$. On the other hand, $\{1, 3, \ldots, 4m + 1\}$ is a covering set of size $2m + 1$. □

Theorem 7. *For all $m \geq 1$ we have $\omega_{2,0}(4m) = 2m + \omega_{2,0}(m)$.*

Proof. Let D be an optimal $(2,0;m)$ covering set. The set

$$\{2a+1 \mid a \in [0,2m-1]\} \cup \{4d \mid d \in D\}$$

is easily seen to be a $(2,0;4m)$ set of size $2m + \omega_{2,1}(m)$. Hence,

$$\omega_{2,0}(4m) \le 2m + \omega_{2,0}(m). \tag{2}$$

On the other hand, let S be an $(2,0;4m)$ covering set. Clearly, S must contain $E = \{2a+1 \mid a \in [0,2m-1]\}$. Let X be the set of even elements in S. Let $s \in X$. If $s \equiv 2 \pmod 4$, then $s \in ME$, where $M = [1,2]$. Hence we can replace s by $2s$ in S and still have a covering set. Therefore, we may assume that all the elements of X are divisible by 4. Define

$$D = \{s/4 \mid s \in X\}.$$

We will show that D is a covering $(2,0;m)$ set. Let $a \in \mathbb{Z}_m$. Then $4a \in \mathbb{Z}_{4m}$. Hence, we have two possibilities:

- $4a \in X$. Then $a \in D$.
- $4a \notin X$. Then $4a = 2 \cdot 4b$, where $4b \in X$, and so $a = 2b$ where $b \in D$.

Hence $MD = \mathbb{Z}_m$. Therefore we get

$$\omega_{2,0}(4m) = |X| + 2m = |D| + 2m \ge \omega_{2,0}(m) + 2m.$$

Combined with (2), this proves the theorem. □

3 Some results on $\omega_{2,1}(q)$

For $S \subseteq \mathbb{Z}_q$ and $(\lambda, \mu) = (2,1)$, we have $M = [-1,2]^* = \{-1,1,2\}$ and

$$MS = \bigcup_{s \in S} \{s, -s, 2s\}.$$

Theorem 8. *For all $m \ge 1$ we have $\omega_{2,1}(2m+1) = m+1$.*

Proof. The set $[0,m]$ is clearly a $(2,1;2m+1)$ covering set. Hence

$$\omega_{2,1}(2m+1) \le m+1. \tag{3}$$

Now, let S be a set of minimal size covering $\mathbb{Z}_{2m+1}$. We note that for $x \in [-1,2]^*$ we have $xs \equiv 0 \pmod{2m+1}$ if and only if $s = 0$. Hence $0 \in S$. Since $0 \in S$ covers only $0 \in \mathbb{Z}_{2m+1}$ we shall, for the rest of the proof, only consider non-zero elements in S and the covering of non-zero elements in $\mathbb{Z}_{2m+1}$. We partition the elements of $\mathbb{Z}^*_{2m+1}$ into the “positive” and “negative” elements,

$$P = \{1, 2, \ldots, m\} \quad \text{and} \quad N = \{-1, -2, \ldots, -m\}.$$

We will determine a particular ordering $s_0 = 0, s_1, s_2, \ldots$ of the elements of S. We use the notation $S_i = \{s_1, s_2, \ldots, s_i\}$. We shall say MS_i is of configuration (j, k) if

$$|P \cap MS_i| = j \quad \text{and} \quad |N \cap MS_i| = k.$$

We shall further say that a configuration (j, k) is balanced if $j = k$, almost balanced if $|j - k| = 1$, and imbalanced otherwise. We will show by induction that there is an ordering with the following properties:

1. If MS_i is balanced then:
   (a) $a \in MS_i$ iff $-a \in MS_i$.
   (b) $|MS_i| \leq 2i$
2. If MS_i is almost balanced then:
   (a) $a \in MS_i$ iff $-a \in MS_i$, except for exactly one element in MS_i.
   (b) $-2s_i \notin MS_i$.
   (c) $|MS_i| \leq 2i + 1$.
3. MS_i is never imbalanced.

If $2m+1$ is divisible by 3, then we must have $(2m+1)/3 \in S$ or $-(2m+1)/3 \in S$ (but not both since S has minimal size). In this case, we choose this as s_1. Then

$$MS_1 = \left\{ \frac{2m+1}{3}, 2\frac{2m+1}{3} \right\}$$

which is a balanced set of size 2. Otherwise, $2m + 1$ is not divisible by 3, and we choose any non-zero element of S as s_1 and we get $MS_1 = \{s_1, -s_1, 2s_1\}$, an imbalanced set of size 3. Moreover, $-2s_1 \notin MS_1$. Thus, the induction basis is proved.

For the induction step, let us assume the hypothesis holds for i, and we show how to pick s_{i+1}. We consider the following cases:

1. MS_i is balanced: If we choose as s_{i+1} an element that is already covered, i.e., $s_{i+1} \in MS_i$, then by the induction hypothesis $-s_{i+1}$ is also covered. Now, if $2s_{i+1}$ is covered, then again, $-2s_{i+1}$ is covered and so $MS_i = MS_{i+1}$ and is balanced. If, on the other hand, $2s_{i+1}$ is not covered then so is $-2s_{i+1}$, but then $2s_{i+1} \in MS_{i+1}$ and $-2s_{i+1} \notin MS_{i+1}$ and so MS_{i+1} is almost balanced. If we choose s_{i+1} that is not covered, then $-s_{i+1}$ is also not covered. As before, if $2s_{i+1}$ is covered, then so is $-2s_{i+1}$ and MS_{i+1} is balanced. Otherwise, $2s_{i+1}$ is not covered and MS_{i+1} is almost balanced since $-2s_{i+1} \notin MS_{i+1}$.
2. MS_i is almost balanced: By the induction hypothesis $-2s_i \notin MS_i$. We must have $-2s_i \in \{s, -s, 2s\}$ for some $s \in S$. We choose s_{i+1} to be one such s. We therefore have three subcases here to consider:
   (a) $s_{i+1} = -2s_i$. In that case $-s_{i+1}$ is already covered. We note that $2s_{i+1}$ and $-2s_{i+1}$ are both covered or both not covered, which results in MS_{i+1} being balanced or almost balanced (with $-2s_{i+1} \notin MS_{i+1}$) respectively.
   (b) $-s_{i+1} = -2s_i$, that is, $s_{i+1} = 2s_i$. This is exactly like the previous case only s_{i+1} is already covered.

(c) $2s_{i+1} = -2s_i$, that is, $s_{i+1} = -s_i$. In this case both s_{i+1} and $-s_{i+1}$ are already covered, as well as $-2s_{i+1} = 2s_i$ being covered. We now have $2s_{i+1} = -2s_i \in MS_{i+1}$ and MS_{i+1} is balanced.

We note that in all cases we never reach an imbalanced state, and it is a matter of simple bookkeeping to verify the size of MS_{i+1} does not exceed the claim.

Having proved the claims by induction, assume $MS_i = \mathbb{Z}^*_{2m+1}$, i.e., a covering of the non-zero elements of $\mathbb{Z}_{2m+1}$. Since MS_i is obviously balanced, by the claims above $i \geq m$. Since we need to add 0 to S_i to get a covering of $\mathbb{Z}_{2m+1}$ we get $\omega_{2,1}(2m+1) \geq m+1$. Combining this with (3), the theorem follows. □

Theorem 9. *For all $m \geq 1$ we have $\omega_{2,1}(4m) = m + \omega_{2,1}(m)$.*

Proof. Let $E = \{2a+1 \mid a \in [0, m-1]\}$. Then

$$ME = \{a \in \mathbb{Z}_{4m} \mid a \not\equiv 0 \pmod 4\}.$$

Let D be an optimal $(2,1;m)$ set. Then the set $E \cup \{4d \mid d \in D\}$ is easily seen to be a $(2,1;4m)$ set of size $m + \omega_{2,1}(m)$. Hence,

$$\omega_{2,1}(4m) \leq m + \omega_{2,1}(m). \tag{4}$$

On the other hand, let S be an optimal $(2,1;4m)$ covering set. Let S_0 be the set of even elements in S and S_1 be the set of odd elements in S. First, we see that for an odd integer $a \in \mathbb{Z}_{4m}$, we must have $a \in S_1$ or $-a \in S_1$. Hence, S_1 contains at least m elements. Let $S' = S_0 \cup E$. Then $MS_1 \subseteq ME$ and so $MS' = \mathbb{Z}_{4m}$. Also

$$\omega_{2,1}(4m) \leq |S'| = m + |S_0| \leq |S_1| + |S_0| = \omega_{2,1}(4m),$$

and so S' is an optimal covering set.

Next, if S_0 contains an element $s \equiv 2 \pmod 4$, this covers s, $4m - s$, and $s' = (2s \bmod 4m)$. The first two are also covered by E. Therefore, if we replace s by s', the set is still a covering set for $\mathbb{Z}_{4m}$. Repeating the process with for all elements in S_0 that er congruent to 2 modulo $4m$, we get a set S'_0 where all elements are divisible by 4, and such that $E \cup S'_0$ is a covering set, of size $\omega_{2,1}(4m)$. Let $D = \{s/4 \mid s \in S'_0\}$. Then it is easy to see that D is a set covering $\mathbb{Z}_m$. Hence, $|S'_0| \geq \omega_{2,1}(m)$ and so

$$\omega_{2,1}(4m) = |S| = |E| + |S'_0| \geq m + \omega_{2,1}(m).$$

Combined with (4), the theorem follows. □

The determination of $\omega_{2,1}(4m+2)$ seems to be more tricky. We start with a lower bound.

Theorem 10. *For all $m \geq 1$ we have $\omega_{2,1}(4m+2) \geq 3m/2 + 1$.*

Proof. Let S be an optimal $(2,1;4m+2)$ covering set. We first note that the only way to cover $2m+1 \in \mathbb{Z}_{4m+2}$ is by having $2m+1 \in S$. Thus, 0 is also covered since $2(2m+1) \equiv 0 \pmod{4m+2}$. We now use an argument similar to that used in the proof of Theorem 9. The odd elements of $\mathbb{Z}_{4m+2}$ can only be covered by odd elements in S. Since $s \in S$ covers both s and $-s$, in order to cover the $2m$ remaining odd elements of $\mathbb{Z}_{4m+2}$ we need at least m odd elements in S in addition to our initial choice of $2m+1 \in S$. Furthermore, this implies that of the $2m$ even non-zero elements of $\mathbb{Z}_{4m+2}$, m are already covered. We are therefore left with m even non-zero elements in $\mathbb{Z}_{4m+2}$ which we still need to cover. Adding an odd element to S can cover at most another single even element in $\mathbb{Z}_{4m+2}$. In contrast, adding an even element s to S can cover at most two more elements of $\mathbb{Z}_{4m+2}$ since at least one of s and $-s$ is already covered. Thus, we need to add at least $\frac{m}{2}$ more elements to S. ◻

We turn to prove upper bounds on $\omega_{2,1}(4m+2)$. Let v_2 denote the 2-ary evaluation, that is $n = 2^{v_2(n)}n_1$, where n_1 is odd. By an explicit construction, we can find an upper bound on $\omega_{2,1}(4m+2)$.

Construction 1. For $m \geq 0$, let $S = X \cup Y \cup Z$, where

$$X = \{2a+1 \mid a \in [0,m]\},$$
$$Y = \left\{c \in \left[1, 4\left\lfloor \frac{m}{3} \right\rfloor + 2\right] \;\middle|\; v_2(c) = 1\right\},$$
$$Z = \left\{c \in \left[1, 8\left\lfloor \frac{m}{3} \right\rfloor\right] \;\middle|\; v_2(c) \text{ is odd and } v_2(c) \geq 3\right\}.$$

Proposition 1. *For all $m \geq 0$, S of Construction 1 is a $(2,1;4m+2)$ covering set.*

Proof. Let $b \in [0, 4m+1]$.

- Case $b = 0$. We have $0 \equiv 4m+2 = 2(2m+1) \pmod{4m+2}$.
- Case $b \in [1, 4m+1]$ and $v_2(b) = 0$. If $b \leq 2m+1$, then $b \in X$. If $b \geq 2m+3$, then $q - b \in X$.
- Case $b \in [1, 4m+1]$ and $v_2(b) = 1$. In this case, $b = 2c$, where $c \in X$.
- Case $b \in \left[1, 8\left\lfloor \frac{m}{3} \right\rfloor + 4\right]$ and $v_2(b) = 2$. In this case, $b = 2c$, where $c \in Y$.
- Case $b \in \left[1, 8\left\lfloor \frac{m}{3} \right\rfloor + 4\right]$, $v_2(b) \geq 3$, and $v_2(b)$ is odd. In this case, $b \in Z$.
- Case $b \in \left[1, 8\left\lfloor \frac{m}{3} \right\rfloor + 4\right]$, $v_2(b) \geq 4$, and $v_2(b)$ is even. In this case, $b = 2c$, where $c \in Z$.
- Case $b \in \left[8\left\lfloor \frac{m}{3} \right\rfloor + 8, 4m\right]$ and $v_2(b) \geq 2$. Let $b = 4\beta$, where now β is an integer. Then
$$4m+2-b = 4(m-\beta)+2.$$
In particular, $v_2(4m+2-b) = 1$. Furthermore,
$$4m+2-b \leq 4m+2-8\left\lfloor \frac{m}{3} \right\rfloor - 8 \leq 4\left\lfloor \frac{m}{3} \right\rfloor + 2,$$
and so $4m+2-b \in Y$.

□

Corollary 1. *For all $m \geq 0$ we have*

$$\frac{3m+2}{2} \leq \omega_{2,1}(4m+2) < \frac{14m+18}{9} + \left\lceil \frac{1}{2}\log_2\left(\left\lfloor \frac{m}{3}\right\rfloor + 1\right)\right\rceil .$$

Proof. The lower bound is from Theorem 9. We will show that the upper bound follows from Proposition 1. We have

$$\begin{aligned}
|X| &= m+1,\\
|Y| &= \left\lfloor \frac{m}{3}\right\rfloor + 1,\\
|Z| &= \sum_{j\geq 1}\left\lfloor 2^{1-2j}\left\lfloor \frac{m}{3}\right\rfloor + \frac{1}{2}\right\rfloor < \frac{2}{3}\left\lfloor \frac{m}{3}\right\rfloor + \left\lceil \frac{1}{2}\log_2\left(\left\lfloor \frac{m}{3}\right\rfloor + 1\right)\right\rceil .
\end{aligned}$$

The first two of these are immediate.

For $|Z|$, we see that $b \in Z$ if $b = 2^{2j+1}(2\delta+1)$ where $\delta \geq 0$, $j \geq 1$, and

$$2\delta + 1 \leq 2^{3-2j-1}\left\lfloor \frac{m}{3}\right\rfloor .$$

Hence, we must have $2^{2-2j}\left\lfloor \frac{m}{3}\right\rfloor \geq 1$, that is $2^{2j-2} \leq \left\lfloor \frac{m}{3}\right\rfloor$ and s $2j-2 \leq \log_2\left(\left\lfloor \frac{m}{3}\right\rfloor\right)$, that is $j \leq 1 + \frac{\log_2(\lfloor m/3\rfloor)}{2}$. Further, for a given j,

$$0 \leq \delta \leq -2^{-1} + 2^{1-2j}\left\lfloor \frac{m}{3}\right\rfloor ,$$

that is, the number of δ is $\left\lfloor 2^{1-2j}\left\lfloor \frac{m}{3}\right\rfloor + \frac{1}{2}\right\rfloor$. By Proposition 1,

$$\begin{aligned}
\omega_{2,1}(4m+2) &< |X| + |Y| + |Z|\\
&\leq m + 1 + \left\lfloor \frac{m}{3}\right\rfloor + 1 + \frac{2}{3}\left\lfloor \frac{m}{3}\right\rfloor + \left\lceil \frac{1}{2}\log_2\left(\left\lfloor \frac{m}{3}\right\rfloor + 1\right)\right\rceil\\
&\leq \frac{14m+18}{9} + \left\lceil \frac{1}{2}\log_2\left(\left\lfloor \frac{m}{3}\right\rfloor + 1\right)\right\rceil .
\end{aligned}$$

□

Another recursive construction is described next.

Construction 2. Let $S' \subseteq \mathbb{Z}_{2m+1}$ be a $(2,2;2m+1)$ covering set such that $S' \subseteq [0,m]$. Let $S = X \cup Y$, where the sets $X, Y \subseteq \mathbb{Z}_{4m+2}$ are defined by

$$X = \{2a+1 \mid a \in [0,m]\}, \qquad Y = \{2s' \mid s' \in S'\} \setminus \{0\} .$$

Proposition 2. *For all $m \geq 0$, S of Construction 2 is a $(2,1;4m+2)$ covering set.*

Proof. First, we see that X covers 0 and all the odd elements of $\mathbb{Z}_{4m+2}$. Next, we note that the even elements of $\mathbb{Z}_{4m+2}$ are isomorphic to $\mathbb{Z}_{2m+1}$. Thus, the elements of Y cover all the even non-zero elements of $\mathbb{Z}_{4m+2}$ except perhaps elements of the form $-4s'$ for $s' \in S'$. However

$$-4s' \equiv 2\big(2(m-s')+1\big) \pmod{4m+2},$$

and so $-4s'$ is covered by X since $2(m-s')+1 \in X$. □

Corollary 2. *For all* $m \geq 0$, $\omega_{2,1}(4m+2) \leq m + \omega_{2,2}(2m+1)$.

Proof. Let $S' \subseteq \mathbb{Z}_{2m+1}$ be a $(2,2;2m+1)$ optimal covering set. Without loss of generality, we may assume that $S' \subseteq [0,m]$, since s and $-s \equiv 2m+1-s \pmod{2m+1}$ cover the same elements of $\mathbb{Z}_{2m+1}$. From Construction 2 we get

$$\omega_{2,1}(4m+2) \leq |S| = |X| + |Y| = (m+1) + (\omega_{2,2}(2m+1) - 1).$$

□

Corollary 3 in [5] states that a $(2,2;2m+1)$ perfect packing set exists if and only if $v_2(\mathrm{ord}_p(2)) \geq 2$ for any prime p dividing $2m+1$.

Corollary 3. *If* $v_2(\mathrm{ord}_p(2)) \geq 2$ *for any prime* p *dividing* $2m+1$*, then* $\omega_{2,1}(4m+2) = 3m/2+1$*, and Construction 2 produces an optimal* $(2,1;4m+2)$ *covering set.*

Proof. A simple counting argument shows that if a $(2,2;2m+1)$ perfect covering set exists, then $\omega_{2,2}(2m+1) = m/2+1$. We then combine Theorem 10 with Corollary 2 to obtain the desired result. □

Example 3. Of the first 1000 even m, 390 satisfy the condition of Corollary 3, the first ten are 2, 6, 8, 12, 14, 18, 20, 26, 30, 32. Of the 5000 even m below 10000, 1745 satisfy the condition of Corollary 3.

References

1. Cassuto, Y., Schwartz, M., Bohossian, V., Bruck, J.: Codes for asymmetric limited-magnitude errors with applications to multilevel flash memories. IEEE Trans. Inform. Theory **56**(4), 1582–1595 (2010)
2. Jiang, A., Langberg, M., Schwartz, M., Bruck, J.: Trajectory codes for flash memory. Accepted to IEEE Trans. on Inform. Theory
3. Kløve, T., Bose, B., Elarief, N.: Systematic, single limited magnitude error correcting codes for flash memories. IEEE Trans. Inform. Theory **57**(7), 4477–4487 (2011)
4. Kløve, T., Luo, J., Naydenova, I., Yari, S.: Some codes correcting asymmetric errors of limited magnitude. IEEE Trans. Inform. Theory **57**(11), 7459–7472 (2011)
5. Kløve, T., Luo, J., Yari, S.: Codes correcting single errors of limited magnitude. IEEE Trans. Inform. Theory **58**(4), 2206–2219 (2012)
6. Schwartz, M.: Quasi-cross lattice tilings with applications to flash memory. IEEE Trans. Inform. Theory **58**(4), 2397–2405 (2012)
7. Stein, S., Szabó, S.: Algebra and Tiling. The Mathematical Association of America (1994)
8. Yari, S., Kløve, T., Bose, B.: Some codes correcting unbalanced errors of limited magnitude for flash memories. Submitted to IEEE Trans. on Inform. Theory