Des. Codes Cryptogr. (2014) 73:329–354
DOI 10.1007/s10623-013-9917-1

Linear covering codes and error-correcting codes for limited-magnitude errors

Torleiv Kløve · Moshe Schwartz

Received: 27 June 2013 / Revised: 28 December 2013 / Accepted: 29 December 2013 /
Published online: 18 January 2014

Abstract The concepts of a linear covering code and a covering set for the limited-magnitude-error channel are 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. A problem of Stein is partially solved for these cases. Optimal packing sets and the corresponding error-correcting codes are also considered for some small-magnitude errors.

Keywords Covering codes · Covering sets · Packing sets · Error-correcting codes · Limited-magnitude errors

Mathematics Subject Classification 11H31 · 52C17 · 94B05

1 Introduction

For integers a and b, where $a \leq b$, we let

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

Moshe Schwartz—on sabbatical leave at the Research Laboratory of Electronics, MIT.

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Coding and Cryptography".

T. Kløve (✉)
Department of Informatics, University of Bergen, 5020 Bergen, Norway
e-mail: Torleiv.Klove@ii.uib.no

M. Schwartz
Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, 8410501 Beersheba, Israel
e-mail: schwartz@ee.bgu.ac.il

Throughout this paper, let k_-, k_+ be integers such that $0 \le k_- \le k_+$, and let q be a positive integer. The ring of integers modulo q is denoted by $\mathbb{Z}_q$. Usually, but not always, we represent the elements of $\mathbb{Z}_q$ by $\{0, 1, \ldots, q-1\}$.

In the $(k_+, k_-; q)$limited-magnitude-error channel, an element $a \in \mathbb{Z}_q$ may be changed into any element in the set

$$\{(a+e) \bmod q \mid e \in [-k_-, k_+]\}.$$

For convenience we shall also set $M = [-k_-, k_+]^*$.

For a set $S \subset \mathbb{Z}_q^r$ we can define a corresponding linear code C_S by using the vectors in S as columns of a parity-check matrix, that is, if $S = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n\}$, then

$$C_S = \left\{ (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_q^n \;\middle|\; \sum_{i=1}^{n} x_i \mathbf{s}_i \equiv \mathbf{0} \pmod{q} \right\}.$$

If an error e occurs in position j, that is, $(x_1, x_2, \ldots, x_n)$ is changed into $(y_1, y_2, \ldots, y_n)$ where $y_j = x_j + e$ and $y_i = x_i$ for $i \ne j$, then

$$\sum_{i=1}^{n} y_i \mathbf{s}_i \equiv e\mathbf{s}_j + \sum_{i=1}^{n} x_i \mathbf{s}_i \equiv e\mathbf{s}_j \pmod{q}.$$

This sum is called the syndrome of the error. The set of syndromes for single errors, limited to M, is therefore

$$MS = \left\{ e\mathbf{s} \in \mathbb{Z}_q^r \mid e \in M, \mathbf{s} \in S \right\}.$$

If all these syndromes are distinct and non-zero, that is, $MS \subseteq \mathbb{Z}_q^r \setminus \{\mathbf{0}\}$ and $|MS| = (k_- + k_+)\,|S|$, then C_S can correct any single limited-magnitude error and we call S a $(k_+, k_-, r; q)$-*packing set*. In the terminology of [15], S is a $B[r, -k_-, k_+](q)$ set. Such codes have been studied in, e.g., [2–11,15].

Similar to packing sets, we can consider covering codes and covering sets. The code C_S is a *covering code* if any vector in $\mathbb{Z}_q^n$ can be obtained from a codeword by a single limited-magnitude error from M. If this is the case, that is, if $MS \supseteq \mathbb{Z}_q^r \setminus \{\mathbf{0}\}$, we call the set S a $(k_+, k_-, r; q)$-*covering set*. Instead of trying to pack many disjoint translates $M\mathbf{s}$, $\mathbf{s} \in S$, into $\mathbb{Z}_q^r \setminus \{\mathbf{0}\}$, in the covering-set scenario we are interested in having the union of $M\mathbf{s}$, $\mathbf{s} \in S$, cover $\mathbb{Z}_q^r \setminus \{\mathbf{0}\}$ entirely with S being as small as possible. Apart from its independent intellectual merit, solving this problem for certain parameters has applications, such as rewriting schemes for non-volatile memories. For a more detailed description the reader is referred to [5] and references therein.

We say that a $(k_+, k_-, r; q)$-covering set, S, is *perfect* if the products $m\mathbf{s} \in \mathbb{Z}_q^r$, where $m \in M$, $\mathbf{s} \in S$, are all distinct and non-zero. These are also called abelian-group splittings in the terminology of [13]. Similarly, a packing set, S, is *perfect* if the products $m\mathbf{s} \in \mathbb{Z}_q^r$, where $m \in M$, $\mathbf{s} \in S$, cover all the non-zero elements of $\mathbb{Z}_q^r$. We note that S is a perfect covering set if and only if it is a perfect packing set.

The following functions shall be of interest to us:

$$\theta(q) = \theta_{k_+,k_-,r}(q) = \text{size of a maximal } (k_+, k_-, r; q)\text{-packing set},$$
$$\omega(q) = \omega_{k_+,k_-,r}(q) = \text{ size of a minimal } (k_+, k_-, r; q)\text{-covering set}.$$

If S is a $(k_+, k_-, r; q)$-covering set of minimal size $\omega_{k_+,k_-,r}(q)$, we call S an optimal covering set. Similarly, if S is a $(k_+, k_-, r; q)$-packing set of maximal size $\theta_{k_+,k_-,r}(q)$, we call S an optimal packing set.

Table 1 The elements of MX

s	(1,1)	(1,3)	(1,5)	(2,1)	(2,3)	(2,5)	(3,1)	(3,2)
$-\mathbf{s}$	(5,5)	(5,3)	(5,1)	(4,5)	(4,3)	(4,1)	(3,5)	(3,4)
$2\mathbf{s}$	(2,2)	(2,0)	(2,4)	(4,2)	(4,0)	(4,4)	(0,2)	(0,4)

Table 2 The elements of MY

s	(0,1)	(0,3)	(1,0)	(1,2)	(1,4)	(3,0)	(3,3)
$-\mathbf{s}$	(0,5)	(0,3)	(5,0)	(5,4)	(5,2)	(0,2)	(0,0)
$2\mathbf{s}$	(0,2)	(0,0)	(2,0)	(2,4)	(2,2)	(0,0)	(0,0)

Example 1 Let $q = 6$, $k_+ = 2$, $k_- = 1$, and $r = 2$. Furthermore, let

$$X = \{(1,1), (1,3), (1,5), (2,1), (2,3), (2,5), (3,1), (3,2)\} \subseteq \mathbb{Z}_6^2,$$
$$Y = \{(0,1), (0,3), (1,0), (1,2), (1,4), (3,0), (3,3)\} \subseteq \mathbb{Z}_6^2.$$

We have $M = \{-1, 1, 2\}$. In Table 1 we list all the elements of MX and in Table 2 all the elements of MY. We see that all the elements of MX are distinct and non-zero. Hence X is a $(2, 1, 2; 6)$-packing set. In particular, $\theta_{2,1,2}(6) \geq 8$. Theorem 17 below implies that we have equality, i.e., $\theta_{2,1,2}(6) = 8$.

We further see that $M(X \cup Y) = \mathbb{Z}_6^2$. In particular, $X \cup Y$ is a $(2, 1, 2; 6)$-covering set. Hence $\omega_{2,1,2}(6) \leq 15$. Theorem 11 below implies that we have equality, i.e., $\omega_{2,1,2}(6) = 15$.

The code C_X consists of all $(x_1, x_2, \ldots, x_8) \in \mathbb{Z}_6^8$ such that

$$x_1 + x_2 + x_3 + 2x_4 + 2x_5 + 2x_6 + 3x_7 + 3x_8 \equiv 0 \pmod 6, \tag{1}$$

and

$$x_1 + 3x_2 + 5x_3 + x_4 + 3x_5 + 5x_6 + x_7 + 2x_8 \equiv 0 \pmod 6. \tag{2}$$

Since $\mathbb{Z}_6$ is not a field, C_X is not a vector space, and so we have to do the counting to determine $|C_X|$ a little carefully. Subtracting (2) from (1) we get

$$4x_2 + 2x_3 + x_4 + 5x_5 + 3x_6 + 2x_7 + x_8 \equiv 0 \pmod 6. \tag{3}$$

In particular,

$$x_4 \equiv x_5 + x_6 + x_8 \pmod 2. \tag{4}$$

Solving (3) for x_3 we get

$$x_3 \equiv x_2 + x_4 + 2x_5 + 2x_7 + x_8 \pmod 3. \tag{5}$$

We can now make the count of $|C_X|$ as follows: x_2, x_5, x_6, x_7, x_8 can be any elements in $\mathbb{Z}_6$. This gives 6^5 choices. By (4), there are now three possible values for x_4. For each of these, by (5), there are now two possible values for x_3. Finally, x_1 is now fixed by (1). Hence $|C_X| = 6^5 \cdot 3 \cdot 2 = 6^6 = 46{,}656$. For an example, consider the codewords with $x_2 = x_5 = x_6 = x_7 = 0$ and $x_8 = 1$. First, by (4), we see that x_4 must be odd, that is $x_4 \in \{1, 3, 5\}$. If $x_4 = 1$, (5) shows that $x_3 = 2$ or $x_3 = 5$. For $x_3 = 2$, we must have $x_1 = 5$, that is $(5, 0, 2, 1, 0, 0, 0, 1) \in C_X$. Considering the other choices of x_4 and x_3 in this case, we get the following additional five codewords:

$$(2, 0, 5, 1, 0, 0, 0, 1), (2, 0, 1, 3, 0, 0, 0, 1), (5, 0, 4, 3, 0, 0, 0, 1),$$
$$(5, 0, 0, 5, 0, 0, 0, 1), (2, 0, 3, 5, 0, 0, 0, 1).$$

In the next section, we prove some simple general bounds. In the rest of the paper, we determine $\omega_{2,k_-,r}(q)$ and $\theta_{2,k_-,r}(q)$ for $k_- = 0, 1, 2$ and all q and r. Section 3 lists some notations that will be used in the rest of the paper. In Sect. 4 we determine $\omega_{2,0,r}(q)$ and in Sects. 5–7 we determine $\omega_{2,1,r}(q)$ and $\omega_{2,2,r}(q)$. In Sect. 8 we consider a problem by Stein. In Sect. 9 we determine $\theta_{2,k_-,r}(q)$ when $k_- = 0, 1, 2$. Finally, in Sect. 10 we summarize our results. Some proofs are collected in Appendix.

2 Some basic general results

We first prove some basic monotonicity properties.

Theorem 1 *Let k'_- and k'_+ be integers such that $0 \le k'_+ \le k_+$ and $0 \le k'_- \le k_-$. Then*

$$\theta_{k'_+,k'_-,r}(q) \ge \theta_{k_+,k_-,r}(q), \quad \omega_{k'_+,k'_-,r}(q) \ge \omega_{k_+,k_-,r}(q).$$

Proof If we let $M' = [-k'_-, k'_+]^*$, then obviously $M' \subseteq M$ and therefore $M'S \subseteq MS$. The claims follow immediately. □

We now give two simple bounds.

Theorem 2 *We have*

$$\omega_{k_+,k_-,r}(q) \ge \left\lceil \frac{q^r - 1}{k_+ + k_-} \right\rceil \quad \text{and} \quad \theta_{k_+,k_-,r}(q) \le \left\lfloor \frac{q^r - 1}{k_+ + k_-} \right\rfloor.$$

Proof By definition, there exists a covering set S of size $\omega_{k_+,k_-,r}(q)$. Therefore,

$$q^r - 1 \le |MS| \le (k_+ + k_-)\,|S| = (k_+ + k_-)\omega_{k_+,k_-,r}(q),$$

and the first inequality follows.

Similarly, there exists a packing set S of size $\theta_{k_+,k_-,r}(q)$. Therefore,

$$q^r - 1 \ge |MS| = (k_+ + k_-)\,|S| = (k_+ + k_-)\theta_{k_+,k_-,r}(q),$$

and the second inequality follows. □

The following theorem shows a connection between covering codes and covering sets. A similar connection between error-correcting codes and packing sets is already known (see, for example, [10]).

Theorem 3 *Let H be an $r \times n$ parity-check matrix for C, a 1-covering linear code over $\mathbb{Z}_q$, q a prime. Then S, the set of columns of H, considered as vectors from $\mathbb{Z}_q^r$, forms a $(k_+, k_-, r; q)$-covering set for all $k_+ + k_- = q - 1$, $0 \le k_- \le k_+$. In particular, if C is perfect, so is S.*

Proof Denote the columns of H by $\mathbf{s}_1, \ldots, \mathbf{s}_n \in \mathbb{Z}_q^r$. Since the code defined by H is a 1-covering code, the syndromes $c\mathbf{s}_i$, $c \in \mathbb{Z}_q$, $c \ne 0$, cover all possible non-zero vectors in $\mathbb{Z}_q^r$. Since $\{m \bmod q \mid m \in [-k_-, k_+]^*\} = \mathbb{Z}_q \setminus \{0\}$, the set $S = \{\mathbf{s}_1, \ldots, \mathbf{s}_n\}$ forms a $(k_+, k_-, r; q)$-covering set.

Finally, if C is perfect, every non-zero column vector in $\mathbb{Z}_q^r \setminus \{\mathbf{0}\}$ has a unique factorization as $c\,\mathbf{s}_i$ for some $c \in \mathbb{Z}_q \setminus \{0\}$. Thus, S is perfect by definition. □

Finally, we present a simple recursion on the parameter r, while fixing all other parameters. Given k_+ and k_-, let

$$\mathcal{M}_q(k_+, k_-) = \left\{\alpha^{-1}\beta \;\middle|\; \alpha, \beta \in [-k_-, k_+]^*\right\},$$

where α^{-1} is the multiplicative inverse of α in $\mathbb{Z}_q$. For this to be well defined, we shall require $\gcd(q, k_+!) = 1$.

Theorem 4 *When* $0 \le k_- \le k_+$ *and* $\gcd(q, k_+!) = 1$ *we have*

$$\omega_{k_+,k_-,r_1+r_2}(q) \le \omega_{k_+,k_-,r_1}(q) + \omega_{k_+,k_-,r_2}(q) + \left|\mathcal{M}_q(k_+, k_-)\right| \omega_{k_+,k_-,r_1}(q)\omega_{k_+,k_-,r_2}(q).$$

Proof For $i \in \{1, 2\}$, let S_i be a $(k_+, k_-, r_i; q)$-covering set of optimal size $\omega_{k_+,k_-,r_i}(q)$. We construct the set $S \subseteq \mathbb{Z}_q^{r_1+r_2}$ defined by

$$S = \{\mathbf{s}_1 \| \mathbf{0} \mid \mathbf{s}_1 \in S_1\} \cup \{\mathbf{0} \| \mathbf{s}_2 \mid \mathbf{s}_2 \in S_2\} \cup \left\{\mathbf{s}_1 \| \gamma\mathbf{s}_2 \mid \mathbf{s}_1 \in S_1, \mathbf{s}_2 \in S_2, \gamma \in \mathcal{M}_q(k_+, k_-)\right\},$$

where $\|$ denotes vector concatenation.

It is easily verifiable that S is indeed a $(k_+, k_-, r_1 + r_2; q)$-covering set: let $\mathbf{x} \in \mathbb{Z}_q^{r_1}$ and $\mathbf{y} \in \mathbb{Z}_q^{r_2}$, $(\mathbf{x}, \mathbf{y}) \neq (\mathbf{0}, \mathbf{0})$. Then $\mathbf{x} = m_1\mathbf{s}_1$ for some $m_1 \in [-k_-, k_+]$ and $\mathbf{s}_1 \in S_1$, and $\mathbf{y} = m_2\mathbf{s}_2$ for some $m_2 \in [-k_-, k_+]$ and $\mathbf{s}_2 \in S_2$. If $\mathbf{y} = \mathbf{0}$, then

$$(\mathbf{x}, \mathbf{y}) = m_1(\mathbf{s}_1, \mathbf{0}) \in [-k_-, k_+]^* S.$$

Similarly if $\mathbf{x} = \mathbf{0}$. Finally, consider the case when $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{y} \neq \mathbf{0}$. In that case, $m_1 \neq 0$ and $m_2 \neq 0$, and so $\gamma = m_1^{-1}m_2 \in \mathcal{M}_q(k_+, k_-)$, as well as $\mathbf{s} = \mathbf{s}_1||\gamma\mathbf{s}_2 \in S$. Since $m_1\mathbf{s} = (\mathbf{x}, \mathbf{y})$, the proof is complete. □

There is no simple explicit expression for $\left|\mathcal{M}_q(k_+, k_-)\right|$, but we can estimate its size. We first note that

$$\left|\mathcal{M}_q(k_+, k_-)\right| \le \left((k_+ + k_-)^2 - 2k_-^2\right),$$

since

$$\left\{\alpha^{-1}\beta \;\middle|\; \alpha \in [-k_-, k_-]^*, \beta \in [-k_-, -1]\right\} = \left\{\alpha^{-1}\beta \;\middle|\; \alpha \in [-k_-, k_-]^*, \beta \in [1, k_-]\right\}.$$

We also observe that in counting the number of elements of $\mathcal{M}_q(k_+, k_-)$, we can skip pairs α, β such that $\gcd(|\alpha|, |\beta|) \neq 1$. It is well known that the size of $\{(\alpha, \beta) \mid \alpha, \beta \in [1, k], \gcd(\alpha, \beta) = 1\}$ is approximately $6\pi^{-2}k^2$, see e.g. [4, Theorem 324]. Using the same argument, we find that

$$\left|\mathcal{M}_q(k_+, k_-)\right| \approx 6\pi^{-2}\left((k_+ + k_-)^2 - 2k_-^2\right) \approx 0.6\left((k_+ + k_-)^2 - 2k_-^2\right).$$

In Table 3 we give some examples for $k_+ = 500$.

Some general upper bounds on $\omega_{k_+,k_-,1}(q)$ were recently given in [3]: If q is a prime, then

$$\omega_{k_+,k_-,1}(q) \le 2\left\lceil \frac{q}{k_+} \right\rceil - 1.$$

It was further shown in [3] that for general q,

$$\omega_{k_+,k_-,1}(q) \le \frac{q^{1+o(q)}}{\sqrt{k_+}}.$$

It is an open question whether these can be generalized to bounds on $\omega_{k_+,k_-,r}(q)$ for $r > 1$.

Table 3 Values and approximations of $|\mathcal{M}_q(500, k_-)|$ in some cases

k_-	$\lvert\mathcal{M}_q(500,k_-)\rvert$	$6\pi^{-2}\big((500+k_-)^2-2k_-^2\big)$
0	152,232	151,981
100	207,020	206,695
00	249,818	249,250
300	280,104	279,646
400	298,360	297,884
500	304,462	303,963

3 Some further notation

An integer is called *doubly even* if it is twice an even number, that is, divisible by 4. It is called *singly even* if it is twice an odd number, that is, congruent to 2 modulo 4.

If q is even, then a vector $\mathbf{a} \in \mathbb{Z}_q^r$ is called even if all the elements are even, otherwise it is called odd. We note that this is well defined; $(a_1, a_2, \ldots, a_r)$ can also be represented by $(b_1, b_2, \ldots, b_r)$ where $b_i \equiv a_i \pmod 2$, but all the b_i are even if and only all the a_i are even. We let $\mathbb{Z}_{q;\mathrm{e}}^r$ denote the set of even vectors in $\mathbb{Z}_q^r$ and $\mathbb{Z}_{q;\mathrm{o}}^r$ denote the set of odd vectors in $\mathbb{Z}_q^r$.

If q is doubly even, then an even vector $\mathbf{a} \in \mathbb{Z}_q^r$ is called doubly even if all the elements are doubly even, otherwise it is called singly even. Again this is well defined. We let $\mathbb{Z}_{q;\mathrm{de}}^r$ denote the set of doubly-even vectors in $\mathbb{Z}_q^r$ and $\mathbb{Z}_{q;\mathrm{se}}^r$ denote the set of singly-even vectors in $\mathbb{Z}_q^r$.

However, note that if $q = 2t$ is singly even, and $2b$ is even, then $2b \equiv 2(b+t) \pmod q$. If $2b$ is singly even, then $2(b+t)$ is doubly even and vice versa. Hence it is not well defined to talk about a singly-even (or a doubly-even) vector in $\mathbb{Z}_q^r$. But if $\mathbf{a} \in \mathbb{Z}_q^r$ is even and non-zero, then the argument shows that there is vector $\mathbf{b} \in \mathbb{Z}_q^r$ with only odd elements such that $\mathbf{a} = 2\mathbf{b}$.

For any positive integer q, a vector $\mathbf{a} \in \{0, 1, \ldots, q-1\}^r \setminus \{\mathbf{0}\}$ whose first non-zero element satisfies $a_i \in [1, \lfloor q/2 \rfloor]$ is called *positive*. The other vectors are called *negative*. This extends in a natural way to vectors in $\mathbf{a} \in \mathbb{Z}_q^r \setminus \{\mathbf{0}\}$. For example, $(6, 3, 7) \equiv (2, 3, 3) \pmod 4$ and so $(6, 3, 7)$ is a positive vector in $\mathbb{Z}_4^3$, $(7, 3, 7) \equiv (3, 3, 3) \pmod 4$ is a negative vector. We let $\mathbb{Z}_{q;\mathrm{p}}^r$ denote the set of positive vectors in $\mathbb{Z}_q^r$. Similarly, we define $\mathbb{Z}_{q;\mathrm{se,p}}^r$, etc.

For any positive integer n and prime p, the p-adic exponent valuation of n, denoted by $v_p(n)$, is the exact power of p dividing n, that is, $n = p^{v_p(n)}n'$ with $\gcd(n', p) = 1$. Let $\mathcal{P}$ be the set all primes. Then

$$n = \prod_{p \in \mathcal{P}, p \mid n} p^{v_p(n)}.$$

If q is odd and d is a divisor of q, we let ℓ_d be the order of 2 modulo d, that is,

$$\ell_d = \min\left\{n \mid 2^n \equiv 1 \pmod d, n > 0\right\}.$$

Let $\mathcal{P}_i$ be the set of primes p for which $v_2(\ell_p) = i$. In particular

$$\mathcal{P}_0 = \{7, 23, 31, 47, 71, 73, 79, 89, \ldots\}$$

is the set of primes dividing $2^m - 1$ for some odd integer m, and

$$\mathcal{P}_1 = \{3, 11, 19, 43, 59, 67, 83, \ldots\}$$

is the set of primes dividing $2^m + 1$ for some odd integer m.

Table 4 The ℓ_p and $v_2(\ell_p)$ for the primes p dividing q

p	3	5	7	11	13	17
ℓ_p	2	4	3	10	12	8
$v_2(\ell_p)$	1	2	0	1	2	3

If q is an odd integer and $i \geq 0$, we write

$$q_i = \prod_{p \in \mathcal{P}_i, p|q} p^{v_p(q)}. \tag{6}$$

We see that $q = q_0 \cdot q_1 \cdot q_1 \cdot q_2 \ldots$.

Example 2 Let $q = 3 \cdot 5^2 \cdot 7^3 \cdot 11^3 \cdot 13 \cdot 17$. In Table 4 we list ℓ_p and $v_2(\ell_p)$ for the primes p dividing q.

We see that $v_2(\ell_p) = 0$ only for $p = 7$. Hence, $q_0 = 7^3$. Next, we see that $v_2(\ell_p) = 1$ for $p = 3$ and $p = 11$. Hence $q_1 = 3 \cdot 11^3$. Furthermore, $v_2(\ell_p) = 2$ for $p = 5$ and $p = 13$. Hence, $q_2 = 5^2 \cdot 13$. Finally, $v_2(\ell_p) = 3$ for $p = 17$. Hence, $q_3 = 17$. We see that $q = q_0 \cdot q_1 \cdot q_2 \cdot q_3$.

Also, for q odd, we define

$$\vartheta_r(q) = \sum_{d|q} \frac{1}{\ell_d} \sum_{c|d} \mu\left(\frac{d}{c}\right) c^r. \tag{7}$$

Here, $\mu(\cdot)$ denotes the Möbius function; if $n = \prod_{j=1}^{r} p_j^{e_j}$ where the p_j are distinct primes and $e_j \geq 1$, then

$$\mu(n) = \begin{cases} (-1)^r & \text{if } e_j = 1 \text{ for all } j, \\ 0 & \text{otherwise,} \end{cases}$$

and, in particular, $\mu(1) = 1$.

Example 3 Consider $q = p^\alpha$ where p is an odd prime. Then $d \mid q$ implies $d = p^\beta$, where $0 \leq \beta \leq \alpha$ and $c = p^\gamma$ where $0 \leq \gamma \leq \beta$. For $d = 1$ we get $\ell_d = 1$ and so

$$\frac{1}{\ell_d} \sum_{c|d} \mu\left(\frac{d}{c}\right) c^r = 1 \cdot \mu(1) = 1.$$

If $d = p^\beta > 1$, then

$$\mu\left(\frac{d}{c}\right) c^r = \mu(p^{\beta-\gamma})\, p^\gamma = \begin{cases} p^{\beta r} & \text{for } \gamma = \beta, \\ -p^{(\beta-1)r} & \text{for } \gamma = \beta - 1, \\ 0 & \text{for } \gamma < \beta - 1. \end{cases}$$

Hence

$$\vartheta_r(p^\alpha) = 1 + \sum_{\beta=1}^{\alpha} \frac{1}{\ell_{p^\beta}} \left(p^{\beta r} - p^{(\beta-1)r}\right).$$

4 Determining $\omega_{2,0,r}(q)$

As we determine $\omega_{2,k_-,r}(q)$, we will see that the expressions we get depend on whether q is odd, q is singly even, or q is doubly even. Throughout the following sub-sections, for $S \subseteq \mathbb{Z}_q^r$ and $(k_+, k_-) = (2, 0)$, we have $M = [0, 2]^* = \{1, 2\}$ and

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

4.1 The case of odd q

For an r-tuple $\mathbf{a} \in \mathbb{Z}_q^r$, the corresponding cyclotomic coset modulo q is

$$\sigma(\mathbf{a}) = \left\{2^j \mathbf{a} \bmod q \mid j \geq 0\right\}.$$

Clearly, the cyclotomic coset $\sigma(\mathbf{0})$ has size 1. If q is a prime and $a \not\equiv 0 \pmod q$, then

$$a\, 2^\ell \equiv a \pmod q \quad \text{if and only if} \quad 2^\ell \equiv 1 \pmod q.$$

Hence, $|\sigma(\mathbf{a})| = \ell_q$ for all $\mathbf{a} \neq \mathbf{0}$.

Theorem 5 *For all odd q we have*

$$\omega_{2,0,r}(q) = \frac{q^r - 2 + \vartheta_r(q_0)}{2},$$

where q_0 is defined by (6).

Proof An element $\mathbf{a} \in \mathbb{Z}_q$ covers two elements, namely $\mathbf{a}$ and $2\mathbf{a}$. To cover a non-zero coset $\sigma(\mathbf{a})$ we therefore need at least $\lceil |\sigma(\mathbf{a})|/2 \rceil$ distinct non-zero elements. A possible minimal covering is

$$\left\{2^{2j}\mathbf{a} \bmod q \;\middle|\; 0 \leq j \leq \left\lceil \frac{|\sigma(\mathbf{a})|}{2} \right\rceil - 1\right\}.$$

In the Appendix (Proof of Theorem 5), we prove that the number of cosets of odd size, including $\sigma(\mathbf{0})$, is given by $\vartheta_r(q_0)$. Summing over all non-zero cosets, we get

$$\omega_{2,0,r}(q) = \frac{(q^r - 1) + (\vartheta_r(q_0) - 1)}{2} = \frac{q^r - 2 + \vartheta_r(q_0)}{2}.$$

□

For $r = 1$, the expression in Theorem 5 was given in [6], in a slightly different notation.

Theorem 5 clearly implies the following corollary.

Corollary 1 *For all odd q, $\vartheta_r(q_0)$ is odd.*

We can prove this result directly from (7), and we show this next.

For all primes p dividing q_0, ℓ_p is odd by definition of q_0. By Lemma 5 (in the Appendix), ℓ_d is odd for all d dividing q_0. Also, c is odd for all c dividing q_0. Hence, modulo 2, we get

$$\vartheta_r(q_0) = \sum_{d|q_0} \frac{1}{\ell_d} \sum_{c|d} \mu\left(\frac{d}{c}\right) c^r \equiv \sum_{d|q_0} \sum_{c|d} \mu\left(\frac{d}{c}\right) \pmod 2.$$

For $d = 1$, we clearly have $\sum_{c|d} \mu\left(\frac{d}{c}\right) = 1$, and for $d > 1$ it is a well-known fact that $\sum_{c|d} \mu\left(\frac{d}{c}\right) = 0$ (see for example [1, Theorem 6-5]).

4.2 The case of even q

Let $q = 2t$. We have $\mathbb{Z}_{2t;\mathrm{e}}^r = (2\mathbb{Z}_t)^r$ and so $|\mathbb{Z}_{2t;\mathrm{e}}^r| = t^r$. Thus, $\mathbb{Z}_{2t;\mathrm{o}}^r = \mathbb{Z}_{2t}^r \backslash \mathbb{Z}_{2t;\mathrm{e}}^r$, and so

$$\left|\mathbb{Z}_{2t;\mathrm{o}}^r\right| = (2t)^r - t^r = \left(2^r - 1\right) t^r.$$

We note that an odd $\mathbf{a}$ can never be represented as $\mathbf{a} = 2\mathbf{b}$ when q is even. Therefore, any covering set for $\mathbb{Z}_{2t}^r$ must contain $\mathbb{Z}_{2t;\mathrm{o}}^r$ as a subset.

As noted above, if q is singly even, then any even $\mathbf{a}$ can be represented as $\mathbf{a} = 2\mathbf{b}$ where $\mathbf{b} \in \mathbb{Z}_{q;\mathrm{o}}^r$. Hence $\mathbb{Z}_{q;\mathrm{o}}^r$ is a minimal covering set in this case. This gives the following result.

Theorem 6 *For $q = 2t$ where t is odd, we have*

$$\omega_{2,0,r}(2t) = \left(2^r - 1\right) t^r.$$

Next, we consider q doubly even, that is, $t = 2m$ and $q = 4m$.

Lemma 1 *For all $m \geq 1$ we have*

$$\omega_{2,0,r}(4m) = 2^r \left(2^r - 1\right) m^r + \omega_{2,0,r}(m).$$

Proof If D is an optimal $(2, 0, r; m)$-covering set, let $X = \mathbb{Z}_{q;\mathrm{o}}^r \cup 4D$. We will show that X is a $(2, 0, r; 4m)$-covering set. If $\mathbf{a} \in \mathbb{Z}_q^r$ is odd, then $\mathbf{a} \in \mathbb{Z}_{q;\mathrm{o}}^r \subset X$. If $\mathbf{a} \in \mathbb{Z}_q^r$ is singly even, then $\mathbf{a} \in 2\mathbb{Z}_{q;\mathrm{o}}^r \subset 2X$. Finally, if $\mathbf{a} \in \mathbb{Z}_q^r \backslash \{\mathbf{0}\}$ is doubly even, then $\mathbf{a} = 4\mathbf{b}$ where $\mathbf{b} \in \mathbb{Z}_m^r \backslash \{\mathbf{0}\}$. If $\mathbf{b} \in D$, then $\mathbf{a} \in 4D \subset X$. On the other hand, if $\mathbf{b} \notin D$, then there exists a $\mathbf{c} \in D$ such that $\mathbf{b} \equiv 2\mathbf{c} \pmod{m}$. Then $\mathbf{a} = 4\mathbf{b} \equiv 2 \cdot 4\mathbf{c} \pmod{4m}$, and so $\mathbf{a} \in 2(4D) \subset 2X$. Hence, X covers $\mathbb{Z}_q^r \backslash \{\mathbf{0}\}$. Since X has size $(2m)^r \left(2^r - 1\right) + \omega_{2,0,r}(m)$, we get,

$$\omega_{2,0,r}(4m) \leq 2^r \left(2^r - 1\right) m^r + \omega_{2,0,r}(m). \tag{8}$$

On the other hand, let S be a $(2, 0, r; 4m)$-covering set. As noted above, S must contain $\mathbb{Z}_{4m;\mathrm{o}}^r$, and all the singly-even vectors are covered due to this fact. Let $X = S \backslash \mathbb{Z}_{4m;\mathrm{o}}^r$ and let $\mathbf{s} \in X$. We note that $\mathbf{s}$ is even. If $\mathbf{s}$ is singly even then it is already covered and we can replace $\mathbf{s}$ by $2\mathbf{s}$ in S and still have a covering set. Hence, replacing all singly-even $\mathbf{s} \in X$ by $2\mathbf{s}$, can get a covering set S' such that all vectors in $X' = S' \backslash \mathbb{Z}_{4m;\mathrm{o}}^r$ are doubly even.

Let $D = \frac{1}{4} X'$. We contend that D is a $(r, 2, 0; m)$-covering set. Let $\mathbf{a} \in \mathbb{Z}_m^r$, and so $4\mathbf{a} \in \mathbb{Z}_{4m}^r$. Hence, we have two possibilities: If $4\mathbf{a} \in X'$ then $\mathbf{a} \in D$. Otherwise, $4\mathbf{a} \notin X'$. In that case, $4\mathbf{a} = 2 \cdot 4\mathbf{b}$, where $4\mathbf{b} \in X'$, and so $\mathbf{a} = 2\mathbf{b}$ where $\mathbf{b} \in D$. Hence $MD \supseteq \mathbb{Z}_m \backslash \{\mathbf{0}\}$. Therefore, we get

$$\omega_{2,0,r}(4m) = \left|\mathbb{Z}_{q;\mathrm{o}}^r\right| + \left|X'\right| = \left|\mathbb{Z}_{q;\mathrm{o}}^r\right| + |D| \geq 2^r \left(2^r - 1\right) m^r + \omega_{2,0,r}(m).$$

Combined with (8), this proves the lemma. □

Using Lemma 1 and induction, we get the following theorem.

Theorem 7 *For all $m \geq 1$ and $s \geq 1$ we have*

$$\omega_{2,0,r}(4^s m) = 2^r \frac{4^{rs} - 1}{2^r + 1} m^r + \omega_{2,0,r}(m).$$

Combining Theorems 5, 6, and 7, we can get explicit expressions for $\omega_{2,0,r}(q)$ for all q.

5 Determining $\omega_{2,2,r}(q)$ for odd q and for singly-even q

These cases are almost identical to $\omega_{2,0,r}(q)$. To avoid tedious repetitiveness, we only sketch the proofs. For $S \subseteq \mathbb{Z}_q^r$ and $(k_+, k_-) = (2, 2)$, we have $M = [-2, 2]^* = \{-2, -1, 1, 2\}$ and

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

5.1 The case of odd q

Theorem 8 *For all odd q we have*

$$\omega_{2,2,r}(q) = \frac{q^r - 4 + \vartheta_r(q_0) + 2\vartheta_r(q_1)}{4}.$$

The proof of Theorem 8 is similar to the proof of Theorem 5 but somewhat more complicated. We give the main details in the Appendix (Proof of Theorem 8).

5.2 The case of singly-even q

We recall that $\mathbb{Z}_{q;\mathrm{o,p}}^r$ is the set of odd positive vectors in $\mathbb{Z}_q^r$. Let $\mathbf{a} \in \mathbb{Z}_q^r$ be some vector. If $\mathbf{a}$ is odd, then $\mathbf{a} \in \mathbb{Z}_{q;\mathrm{o,p}}^r$ or $-\mathbf{a} \in \mathbb{Z}_{q;\mathrm{o,p}}^r$. If $\mathbf{a}$ is even, then there is an odd positive $\mathbf{b}$ such that $\mathbf{a} = 2\mathbf{b}$. Hence $\mathbf{a} \in [-2, 2]^* \mathbb{Z}_{q;\mathrm{o,p}}^r$. Therefore $\mathbb{Z}_{q;\mathrm{o,p}}^r$ is a minimal covering set. This gives the following result in a similar fashion to Theorem 6.

Theorem 9 *For $q = 2t$ where t is odd, we have*

$$\omega_{2,2,r}(2t) = \left(2^r - 1\right) \frac{t+1}{2} t^{r-1}.$$

6 Determining $\omega_{2,1,r}(q)$ for odd q and for singly-even q

We now turn to the case of $(k_+, k_-) = (2, 1)$. The proofs for the claims in this case appear to be more involved. For $S \subseteq \mathbb{Z}_q^r$ and $(k_+, k_-) = (2, 1)$, we have $M = [-1, 2]^* = \{-1, 1, 2\}$ and

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

6.1 The case of odd q

Theorem 10 *For all odd q and $r \geq 1$ we have*

$$\omega_{2,1,r}(q) = \frac{q^r - 1}{2}.$$

Proof The set $\mathbb{Z}_{q;\mathrm{p}}^r$, containing the non-zero vectors whose first non-zero entry is from $\left[1, \frac{q-1}{2}\right]$, is clearly a $(2, 1, r; q)$-covering set. This is because vectors $\mathbf{s}$ of this kind, and their inverse $-\mathbf{s}$, already cover all the non-zero vectors of $\mathbb{Z}_q^r$. Hence

$$\omega_{2,1,r}(q) \leq \frac{q^r - 1}{2}. \tag{9}$$

Now, let S be a set of minimal size covering $\mathbb{Z}_q^r \setminus \{\mathbf{0}\}$. We will determine a particular ordering $\mathbf{s}_1, \mathbf{s}_2, \ldots$ of the elements of S. We use the notation $S_i = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_i\}$. We shall say MS_i is of configuration (j, k) if MS_i contains j positive vectors and k negative vectors. 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) $\mathbf{a} \in MS_i$ iff $-\mathbf{a} \in MS_i$.
   (b) $|MS_i| \leq 2i$.
2. If MS_i is almost balanced then:
   (a) $\mathbf{a} \in MS_i$ iff $-\mathbf{a} \in MS_i$, except for exactly one element in MS_i.
   (b) $-2\mathbf{s}_i \notin MS_i$.
   (c) $|MS_i| \leq 2i + 1$.
3. MS_i is never imbalanced.

We first consider the case when q is divisible by 3. We note, that a non-zero vector $\mathbf{s}$ containing *only* entries from $D = \left\{0, \frac{q}{3}, 2 \cdot \frac{q}{3}\right\}$ can be covered only by $\mathbf{s}$ or $-\mathbf{s}$, and that $-\mathbf{s} \equiv 2\mathbf{s} \pmod{q}$. Thus, a minimal covering of this set of vectors requires exactly one vector from each pair $\{\mathbf{s}, -\mathbf{s}\}$. This gives a total of $(3^r - 1)/2$ vectors, and we let these be the first elements of the sequence. We see that the corresponding S_i for $i \leq (3^r - 1)/2$ are balanced. This is the basis for the induction.

If $3 \nmid q$ we can use $S_0 = \emptyset$, which is balanced, as basis for the induction.

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

1. MS_i is balanced. We choose as $\mathbf{s}_{i+1}$ any vector in $S \setminus S_i$. By definition,
$$MS_{i+1} = MS_i \cup \{\mathbf{s}_{i+1}, -\mathbf{s}_{i+1}, 2\mathbf{s}_{i+1}\}.$$
We have three subcases to consider.
   (a) $-2\mathbf{s}_{i+1} \in MS_i$. Then $-2\mathbf{s}_{i+1} \in MS_{i+1}$. By the induction hypothesis, $2\mathbf{s}_{i+1} \in MS_i$. Hence $MS_{i+1} = MS_i \cup \{\mathbf{s}_{i+1}, -\mathbf{s}_{i+1}\}$. Therefore, MS_{i+1} is balanced.
   (b) $-2\mathbf{s}_{i+1} \notin MS_{i+1}$. Then MS_{i+1} is almost balanced.
   (c) $-2\mathbf{s}_{i+1} \notin MS_i$, but $-2\mathbf{s}_{i+1} \in MS_{i+1}$. We show that this is not possible. Since $\mathbf{s}_{i+1} \not\equiv 0$ we obviously have $-2\mathbf{s}_{i+1} \not\equiv -\mathbf{s}_{i+1}$ and $-2\mathbf{s}_{i+1} \not\equiv 2\mathbf{s}_{i+1}$. Finally $-2\mathbf{s}_{i+1} \equiv \mathbf{s}_{i+1}$ would imply $3\mathbf{s}_{i+1} \equiv 0$; this is only possible if $3|q$ and $\mathbf{s}_{i+1} \equiv 0 \pmod{q/3}$. But then $-2\mathbf{s}_{i+1} \in MS_i$ by the basis of the induction, a contradiction.
2. MS_i is almost balanced. By the induction hypothesis $-2\mathbf{s}_i \notin MS_i$. We must have $-2\mathbf{s}_i \in \{\mathbf{s}, -\mathbf{s}, 2\mathbf{s}\}$ for some $\mathbf{s} \in S$. We choose $\mathbf{s}_{i+1}$ to be one such $\mathbf{s}$. We therefore have three subcases here to consider:
   (a) $\mathbf{s}_{i+1} \equiv -2\mathbf{s}_i$. In that case $-\mathbf{s}_{i+1}$ is already covered. We note that $2\mathbf{s}_{i+1}$ and $-2\mathbf{s}_{i+1}$ are both covered or both not covered, which results in MS_{i+1} being balanced or almost balanced (with $-2\mathbf{s}_{i+1} \notin MS_{i+1}$) respectively.
   (b) $-\mathbf{s}_{i+1} \equiv -2\mathbf{s}_i$, that is, $\mathbf{s}_{i+1} \equiv 2\mathbf{s}_i$. This is exactly like the previous case only $\mathbf{s}_{i+1}$ is already covered.
   (c) $2\mathbf{s}_{i+1} \equiv -2\mathbf{s}_i$, that is, $\mathbf{s}_{i+1} \equiv -\mathbf{s}_i$ (since q is odd). In this case both $\mathbf{s}_{i+1}$ and $-\mathbf{s}_{i+1}$ are already covered, as well as $-2\mathbf{s}_{i+1} \equiv 2\mathbf{s}_i$ being covered. We now have $2\mathbf{s}_{i+1} \equiv -2\mathbf{s}_i \in MS_{i+1}$ 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 that the size of MS_{i+1} does not exceed the claim.

Having proved the claims by induction, let $i = \omega_{2,1,r}(q)$. Then $MS_i \supseteq \mathbb{Z}_q^r \setminus \{\mathbf{0}\}$. Since MS_i is obviously balanced, by the claims above, $2\omega_{2,1,r}(q) \geq |MS_i| \geq q^r - 1$. Combining this with (9), the theorem follows. □

6.2 The case of singly-even q

The results differ for $r = 1$ and $r \geq 2$. We start with the latter case, which is simpler.

Theorem 11 *For all odd $t \geq 1$ and $r \geq 2$ we have*

$$\omega_{2,1,r}(2t) = \frac{1}{2}(2^r - 1)(t^r + 1).$$

Proof Every odd vector $\mathbf{s} \in \mathbb{Z}_{2t}^r$ can be covered only by $\mathbf{s}$ or $-\mathbf{s}$. Thus, from each set $\{\mathbf{s}, -\mathbf{s}\}$, where $\mathbf{s}$ is odd, we need to choose at least one element to be in the set. However, if we define F to be the set of vectors containing only elements from $\{0, t\}$, then for any non-zero $\mathbf{s} \in F$ we have that $\mathbf{s}$ is odd and $\mathbf{s} \equiv -\mathbf{s} \pmod{2t}$. Thus, the non-zero elements from F can only be covered by themselves.

The total number of odd vectors is

$$(2t)^r - t^r = (2^r - 1)t^r,$$

and the number of non-zero vectors in F is given by $2^r - 1$. From the arguments above, a $(2, 1, r; 2t)$-covering set should contain at least half the odd vectors not in F, and all of the non-zero vectors in F, i.e.,

$$\omega_{2,1,r}(2t) \geq \frac{1}{2}\left\{(2t)^r - t^r - (2^r - 1)\right\} + (2^r - 1) = \frac{1}{2}(2^r - 1)(t^r + 1).$$

On the other hand, let S be the set of odd vectors such that the first element not zero or t (if any) is less than t. A simple counting argument shows that S has size $\frac{1}{2}(2^r - 1)(t^r + 1)$. We will show that S is a covering set.

If $\mathbf{a} \in \mathbb{Z}_{2t}^r$ is odd, but $\mathbf{a} \notin S$, then $-\mathbf{a} \in S$.

If $\mathbf{a} \in \mathbb{Z}_{2t}^r$ is even, then $\mathbf{a} = 2\mathbf{b}$ where all the elements of $\mathbf{b}$ are odd. If $\mathbf{b} \notin S$, let b_i be the first element of $\mathbf{b}$ not in $\{0, t\}$. Then $b_i > t$. Define $\mathbf{b}'$ by $b_i' = b_i - t$ and $b_j' = b_j$ for $j \neq i$. Then $\mathbf{b}' \in S$ and $2\mathbf{b}' = 2\mathbf{b} = \mathbf{a}$. □

Example 4 The optimal $(2, 1, 2; 6)$ set given in the proof of Theorem 11 has size 15. In Table 5 we give the vectors $\mathbf{s}$ in the set, together with $-\mathbf{s}$ and $2\mathbf{s}$.

The situation is more complicated when $r = 1$.

Lemma 2 *For all odd $t \geq 1$ we have*

$$\omega_{2,1,1}(2t) \geq \frac{t+1}{2} + \omega_{2,2,1}(t).$$

Proof Let S be an optimal $(2, 1, 1; 2t)$-covering set. We first note that the only way to cover $t \in \mathbb{Z}_{2t}$ is by having $t \in S$. We now use an argument similar to that used in the proof of Theorem 1. The odd elements of $\mathbb{Z}_{2t}$ can only be covered by odd elements in S. Since $s \in S$ covers both s and $-s$, in order to cover the $t - 1$ remaining odd elements of $\mathbb{Z}_{2t}$ we need at least $(t - 1)/2$ odd elements in S in addition to our initial choice of $t \in S$. Furthermore, this

Table 5 An optimal (2, 1, 2; 6) set

s	(0,1)	(0,3)		(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)
−s	(0,5)	(0,3)		(5,0)	(5,5)	(5,4)	(5,3)	(5,2)	(5,1)
2s	(0,2)	(0,0)		(2,0)	(2,2)	(2,4)	(2,0)	(2,2)	(2,4)
s	(2,1)	(2,3)	(2,5)	(3,0)	(3,1)	(3,2)	(3,3)		
−s	(4,5)	(4,3)	(4,1)	(3,0)	(3,5)	(3,4)	(3,3)		
2s	(4,2)	(4,0)	(4,4)	(0,0)	(0,2)	(0,4)	(0,0)		

implies that of the $t-1$ even non-zero elements of $\mathbb{Z}_{2t}$, at least $(t-1)/2$ are already covered, since distinct odd elements cover distinct even elements. It is also crucial that we note that for each even non-zero element a of $\mathbb{Z}_{2t}$, a or $-a$ (perhaps both) are already covered by some odd element $s \in S$.

Assume S has exactly $(t+1)/2$ odd elements. Adding another odd element s to S can, at most, add the element $2s$ to the elements of $\mathbb{Z}_{2t}$ covered by S. We can therefore add the element $2s$ to S instead of adding the element s, without reducing the number of elements covered. Thus, for the purpose of counting the number of elements in an optimal $(2, 1, 1; 2t)$-covering set S, we may assume, without loss of generality, that S contains exactly $(t+1)/2$ odd elements.

We are therefore left with the task of covering the even non-zero elements of $\mathbb{Z}_{2t}$ of which exactly $(t-1)/2$ elements have been pre-covered. Since the even elements of $\mathbb{Z}_{2t}$ are isomorphic to $\mathbb{Z}_t$, we move to the problem of covering the non-zero elements of $\mathbb{Z}_t$, where of each pair $a, -a \in \mathbb{Z}_t$, exactly one element has already been pre-covered. Let us denote the pre-covered elements by $T \subseteq \mathbb{Z}_t$, where we remember $|T| = (t-1)/2$, and for any non-zero $a \in \mathbb{Z}_t$ we have $|\{a, -a\} \cap T| = 1$.

Let $S' \subseteq \mathbb{Z}_t$ be the smallest subset such that

$$\bigcup_{s' \in S'} \{s', -s', 2s'\} \cup T = \mathbb{Z}_t \setminus \{0\}. \tag{10}$$

If $s' \in S'$ and $2s' \in T$, we can replace s' with $-s'$ in S' without affecting (10). Hence, without loss of generality, we may assume $s' \in S'$ implies $-2s' \in T$. We now contend that S' is in fact a $(2, 2, 1; t)$-covering set. This is easily seen by

$$\bigcup_{s' \in S'} \{s', -s', 2s', -2s'\} = \bigcup_{s' \in S'} \{s', -s', 2s'\} \cup T = \mathbb{Z}_t \setminus \{0\}.$$

It therefore follows that

$$|S'| \geq \omega_{2,2,1}(t).$$

Returning to the original problem of covering $\mathbb{Z}_{2t}$ we arrive at

$$\omega_{2,1,1}(2t) = |S| = + |S'| \geq \frac{t+1}{2} + \omega_{2,2,1}(t),$$

which completes the proof. □

A recursive construction is described next.

Construction 1 Let $S' \subseteq [1, (t-1)/2]$ be a $(2, 2, 1; t)$-covering set. Let $S = X \cup Y$, where the sets $X, Y \subseteq \mathbb{Z}_{2t}$ are defined by

$$X = \{2a + 1 \mid a \in [0, (t-1)/2]\}, \quad Y = \left\{2s' \mid s' \in S'\right\}.$$

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

Proof First, we see that X covers all the odd elements of $\mathbb{Z}_{2t}$. Next, we note that the even elements of $\mathbb{Z}_{2t}$ are isomorphic to $\mathbb{Z}_t$. Thus, the elements of Y cover all the even non-zero elements of $\mathbb{Z}_{2t}$ except perhaps elements of the form $-4s'$ for $s' \in S'$. However

$$-4s' \equiv 2\left(2(m - s') + 1\right) \pmod{2t},$$

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

Theorem 12 *For all odd $t \geq 1$,*

$$\omega_{2,1,1}(2t) = \frac{t+1}{2} + \omega_{2,2,1}(t).$$

Proof Let $S' \subseteq \mathbb{Z}_t$ be a $(2, 2, 1; t)$ optimal covering set. Without loss of generality, we may assume that $S' \subseteq [1, (t-1)/2]$, since s and $-s \equiv t - s \pmod{t}$ cover the same elements of $\mathbb{Z}_t$. From Construction 1 we get

$$\omega_{2,1,1}(2t) \leq |S| = |X| + |Y| = \frac{t+1}{2} + \omega_{2,2,1}(t).$$

To complete the proof we combine the upper bound with the lower bound from Lemma 2. □

In Theorem 9 above, we gave an expression for $\omega_{2,2,1}(t)$. In particular, we get the following corollary.

Corollary 2 *If* $\mathrm{ord}_p(2)$ *is doubly even for all primes p dividing t, then*

$$\omega_{2,1,1}(2t) = \frac{3t+1}{4},$$

and Construction 1 produces an optimal $(2, 1, 1; 2t)$-covering set.

Proof A simple counting argument shows that if a perfect $(2, 2, 1; t)$-covering set exists, then $\omega_{2,2,1}(t) = \frac{t-1}{4}$. By Theorem 12 we obtain the desired result. □

Example 5 Consider $t = 25$. One (perfect) $(2, 2, 1; 25)$-covering set is $\{1, 4, 5, 6, 9, 11\}$. Using this in Construction 1 we get an optimal $(2, 1, 1; 50)$-covering set of size 19, illustrating Corollary 2. The elements of X and Y are given in Table 6.

Example 6 Of the first 1,000 values of $t \equiv 1 \pmod 4$, 390 satisfy the condition of Corollary 2; the first ten are 5, 13, 17, 25, 29, 37, 41, 53, 61, 65. Of the 5,000 odd t below 1,0000, 1,745 satisfy the condition of Corollary 2.

Table 6 An optimal $(2, 1, 1; 50)$ set $X \cup Y$

s	X													Y					
	1	3	5	7	9	11	13	15	17	19	21	23	25	2	8	10	12	18	22
$-s$	49	47	45	43	41	39	37	35	33	31	29	27	25	48	42	40	38	32	28
$2s$	2	6	10	14	18	22	26	30	34	38	42	46	0	4	16	20	24	36	44

7 Determining $\omega_{2,1,r}(q)$ and $\omega_{2,2,r}(q)$ for doubly-even q

Let $q = 4m$. We give a recursion that applies both for $k_- = 1$ and $k_- = 2$. The result and proof are very similar to Lemma 1 and its proof.

Lemma 3 *For all $m \geq 1$ and $k_- \in \{1, 2\}$ we have*

$$\omega_{2,k_-,r}(4m) = 2^{r-1}\left(2^r - 1\right)m^r + \omega_{2,k_-,r}(m).$$

Proof Let $E \subseteq \mathbb{Z}_{4m}^r$ be the set of odd vectors whose first odd entry is from $[1, 2m-1]$. Then

$$[-1, 2]^* E = \mathbb{Z}_{4m;\mathrm{o}}^r \cup \mathbb{Z}_{4m;\mathrm{se}}^r.$$

Let D be an optimal $(2, -k_-, r; m)$-covering set. Then the set $E \cup 4D$ is easily seen to be a $(2, 1, r; 4m)$-covering set of size $2^{r-1}\left(2^r - 1\right)m^r + \omega_{2,1,r}(m)$. Hence,

$$\omega_{2,k_-,r}(4m) \leq 2^{r-1}\left(2^r - 1\right)m^r + \omega_{2,k_-,r}(m). \tag{11}$$

On the other hand, let S be an optimal $(2, k_-, r; 4m)$-covering set. Let S_0 be the set of even vectors in S and S_1 be the set of odd vectors in S. First, we see that for an odd vector $\mathbf{a} \in \mathbb{Z}_{4m;\mathrm{o}}^r$, we must have $\mathbf{a} \in S_1$ or $-\mathbf{a} \in S_1$. Hence, S_1 contains at least $2^{r-1}\left(2^r - 1\right)m^r$ vectors. Let $S' = S_0 \cup E$. Then $[-k_-, 2]^* S_1 \subseteq [-k_-, 2]^* E$ and so $[-k_-, 2]^* S' \supseteq \mathbb{Z}_{4m}^r \backslash \{\mathbf{0}\}$. Also

$$\omega_{2,k_-,r}(4m) \leq \left|S'\right| = 2^{r-1}\left(2^r - 1\right)m^r + |S_0| \leq |S_1| + |S_0| = \omega_{2,k_-,r}(4m),$$

and so S' is an optimal $(2, k_-, r; 4m)$-covering set.

Next, if $\mathbf{s} \in S_0$ is singly even, then $\mathbf{s}$ covers $\mathbf{s}$, $-\mathbf{s}$, and $\mathbf{s}' = 2\mathbf{s}$. The first two are also covered by E. Therefore, if we replace $\mathbf{s}$ by $\mathbf{s}'$, the set is still a $(2, k, r; 4m)$-covering set. Repeating the process for all singly-even vectors in S_0, we get a set S_0' where all vectors are doubly even, and such that $E \cup S_0'$ is a covering set, of size $\omega_{2,k_-,r}(4m)$. Let $D = \frac{1}{4}S_0'$. Then it is easy to see that D is a $(2, k_-, r; m)$-covering set. Hence, $\left|S_0'\right| \geq \omega_{2,k_-,r}(m)$ and so

$$\omega_{2,k_-,r}(4m) = |S| = |E| + \left|S_0'\right| \geq 2^{r-1}\left(2^r - 1\right)m^r + \omega_{2,k_-,r}(m).$$

Combined with (11), the lemma follows. □

Using Lemma 3 and induction, we get the following theorem.

Theorem 13 *For all $m \geq 1$, $k_- \in \{1, 2\}$, and $s \geq 1$ we have*

$$\omega_{2,k_-,r}(4^s m) = 2^{r-1}\frac{4^{rs} - 1}{2^r + 1}m^r + \omega_{2,k_-,r}(m).$$

8 On a problem by Stein

The essence of this work is to study how to cover a given abelian group G with products of the form ms, $m \in M$ and $s \in S$. The set M is given to us, and we have to find $S \subseteq G$ as small as possible. The groups we considered throughout this work are $G = \mathbb{Z}_q^r = \mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q$, where in the extreme, when $r = 1$, $G = \mathbb{Z}_q$ is a cyclic group.

Stein and Szabó [13, Chap. 4, Problem 7] (originally in [12]) asked whether the smallest covering when $M = [1, k_+]$ is always attainable with a cyclic group. For $k_+ = 2$ the question was answered in the affirmative by Szabó [14].

We ask a similar question: Is $\omega_{k_+,k_-,1}(q^r) \le \omega_{k_+,k_-,r}(q)$ for all k_+, k_-, q, and $r \ge 2$?

This question is more general than Stein and Szabó's in the sense of having a more general $M = [-k_-, k_+]^*$. On the other hand, it is less general in the sense that, even though any abelian group may be factored as a direct product of cyclic groups, we shall only be considering direct products of cyclic groups where all the cyclic groups are identical.

As an illustration of the use of our explicit expressions for $\omega_{2,k_-,r}(q)$, we will prove an affirmative answer to this problem when $0 \le k_- \le k_+ = 2$.

Theorem 14 *Let $r \ge 2$, $q \ge 2$, and $k_- \in [0, 2]$. Then*

$$\omega_{2,k_-,1}(q^r) \le \omega_{2,k_-,r}(q).$$

Proof First, consider q odd. From Theorem 5 above and Lemma 10 (in the Appendix) we get

$$\omega_{2,0,1}(q^r) = \frac{q^r - 2 + \vartheta_1(q_0^r)}{2} \le \frac{q^r - 2 + \vartheta_r(q_0)}{2} = \omega_{2,0,r}(q).$$

Similarly, Theorem 8 and Lemma 10 give

$$\omega_{2,2,1}(q^r) \le \omega_{2,2,r}(q).$$

From Theorem 10, we immediately get

$$\omega_{2,1,1}(q^r) = \frac{q^r - 1}{2} = \omega_{2,1,r}(q).$$

We now turn to consider singly-even q. Let $q = 2t$, with t odd. We treat $k_- = 1$ in detail. The proofs for $k_- = 0$ and $k_- = 2$ are very similar. By Theorem 11,

$$\omega_{2,1,r}(2t) = \frac{2^r - 1}{2}(t^r + 1).$$

If r is even, $r = 2\rho$, then Theorem 13 gives

$$\omega_{2,1,1}((2t)^r) = \omega_{2,1,1}(4^\rho t^r) = \frac{4^\rho - 1}{3}t^r + \omega_{2,1,1}(t^r) = \frac{2^r - 1}{3}t^r + \frac{t^r - 1}{2}.$$

Hence

$$\omega_{2,1,r}(q) - \omega_{2,1,1}(q^r) = \frac{2^r - 4}{6}t^r + 2^{r-1} > 0.$$

Next, if r is odd, $r = 2\rho+1$, we first observe that $[1, \frac{t^r-1}{2}]$ obviously is a $(2, 2, 1; t^r)$-covering set, and so $\omega_{2,2,1}(t^r) \le \frac{t^r-1}{2}$. Combined with Theorems 12 and 13 we get

$$\begin{aligned}\omega_{2,1,1}((2t)^r) &= \omega_{2,1,1}(4^\rho \cdot 2t^r) = \frac{4^\rho - 1}{3} \cdot 2t^r + \omega_{2,1,1}(2t^r) \\ &= \frac{2^r - 2}{3} \cdot t^r + \frac{t^r + 1}{2} + \omega_{2,2,1}(t^r) \le \frac{2^r - 2}{3} \cdot t^r + \frac{t^r + 1}{2} + \frac{t^r - 1}{2}.\end{aligned}$$

Hence, with Theorem 11 we get that

$$\omega_{2,1,r}(q) - \omega_{2,1,1}(q^r) \ge \frac{2^r - 5}{6}t^r + \frac{2^r - 1}{2} > 0$$

since $r \ge 3$.

For the similar proof for $k_- = 0$ and $k_- = 2$, we use the simple observations $\omega_{2,0,1}(t^r) \le t^r - 1$ and $\omega_{2,2,1}(t^r) \le (t^r - 1)/2$. We omit further details.

Finally, consider doubly-even $q = 4^s m$ where $s \geq 1$ and m is odd or singly even. By Theorem 13,

$$\omega_{2,1,r}(4^s m) = 2^{r-1}\frac{4^{rs}-1}{2^r+1}m^r + \omega_{2,1,r}(m),$$
$$\omega_{2,1,1}(4^{rs}m^r) = \frac{4^{rs}-1}{3}m^r + \omega_{2,1,1}(m^r).$$

By the results above, $\omega_{2,1,r}(m) \geq \omega_{2,1,1}(m^r)$. Hence

$$\omega_{2,1,r}(q) - \omega_{2,1,1}(q^r) \geq \left(\frac{2^{r-1}}{2^r+1} - \frac{1}{3}\right)(4^{rs}-1)m^r \geq 0.$$

The proofs for $k_- = 0$ and $k_- = 2$ are again very similar; we omit the details. □

We remark in passing that by a similar argument, we can show that $\frac{2}{3}\omega_{2,1,r}(q) < \omega_{2,1,1}(q^r)$ for all even q.

9 Determining $\theta_{2,k_-,r}(q)$ for $k_- \in [0, 2]$

We now switch gears to consider error-correcting codes instead of covering codes. In this section we study optimal $(2, k_-, r; q)$-packing sets (which give optimal error-correcting codes).

Theorem 15 *For all odd q we have*

$$\theta_{2,0,r}(q) = \frac{q^r - \vartheta_r(q_0)}{2}, \tag{12}$$
$$\theta_{2,1,r}(q) = \theta_{2,2,r}(q) = \frac{q^r + 2 - \vartheta_r(q_0) - 2\vartheta_r(q_1)}{4}. \tag{13}$$

where q_0 and q_1 are defined by (6).

Proof We start by considering $\theta_{2,0,r}(q)$. Similarly to the proof of Theorem 5, a maximal packing set must contain exactly $\lfloor |\sigma(\mathbf{a})|/2 \rfloor$ of the elements in a coset $\sigma(\mathbf{a})$. Summing over all non-zero cosets, we get

$$\theta_{2,0,r}(q) = \frac{(q^r-1) - (\vartheta_r(q_0)-1)}{2} = \frac{q^r - \vartheta_r(q_0)}{2},$$

which proves (12). We note that for $r = 1$ this expression was given in [7], in a slightly different notation. For general q, if $\vartheta_r(q_0) = 1$, that is, $q_0 = 1$, then the set is perfect. In the other cases, the error-correcting codes derived from Theorem 5 are better (larger) than the codes given in [7,8].

The proof for $\theta_{2,2,r}(q)$ is a similar modification of the proof of Theorem 5. For $r = 1$, a similar proof was given in [9].

Finally, we consider $\theta_{2,1,r}(q)$. In [15] it was shown that $\theta_{2,1,1}(q) = \theta_{2,2,1}(q)$ for odd q. The proof generalizes to all r, and we sketch this here for completeness.

First, we note that any $(2, 2, r; q)$-packing set is clearly a $(2, 1, r; q)$-packing set. We will show that the converse is true. For any $\mathbf{s} \in \mathbb{Z}_q^r$, let $T\mathbf{s} = \{\mathbf{s}, -\mathbf{s}, 2\mathbf{s}\}$ and $T'\mathbf{s} = \{\mathbf{s}, -\mathbf{s}, 2\mathbf{s}, -2\mathbf{s}\}$. Let S be a $(2, 1, r; q)$-packing set. By definition, the sets $T\mathbf{s}$, where $\mathbf{s} \in S$, are disjoint. We will show that then the sets $T'\mathbf{s}$, where $\mathbf{s} \in S$, are also disjoint, i.e., that S is a $(2, 2, r; q)$-packing set.

Let $\mathbf{a} \in S$. We start by noting that $-2\mathbf{a}$ which is added to $T\mathbf{a}$ in order to obtain $T'\mathbf{a}$, does not equal an element already in $T\mathbf{a}$. We cannot have $-2\mathbf{a} = -\mathbf{a}$ for then $2\mathbf{a} = \mathbf{a}$ and S is not a $(2, 1, r; q)$-packing set. Similarly we cannot have $-2\mathbf{a} = \mathbf{a}$. Finally, since q is odd, $-2\mathbf{a} = 2\mathbf{a}$ implies $-\mathbf{a} = \mathbf{a}$, which is again a contradiction.

To continue, let $\mathbf{a}, \mathbf{b} \in S$, $\mathbf{a} \neq \mathbf{b}$. It is now sufficient to show that $-2\mathbf{a} \notin T'\mathbf{b}$. We have $2\mathbf{a} \neq \mathbf{b}$ and so $-2\mathbf{a} \neq -\mathbf{b}$. Similarly, $2\mathbf{a} \neq -\mathbf{b}$ and so $-2\mathbf{a} \neq \mathbf{b}$. Further, $\mathbf{a} \neq \mathbf{b}$ and so $-2\mathbf{a} \neq -2\mathbf{b}$, since q is odd. Similarly, $\mathbf{a} \neq -\mathbf{b}$ and so $-2\mathbf{a} \neq 2\mathbf{b}$. In any case, $-2\mathbf{a} \notin T'\mathbf{b}$. This completes the proof of (14). □

From [7, Theorem 4; 9, Theorem 7; 15, Theorem 6] we quote the following results.

Theorem 16 *For all singly-even $q = 2t$, $t \geq 1$ odd, we have*

$$\theta_{2,0,1}(2t) = t - 1,$$
$$\theta_{2,1,1}(2t) = \theta_{2,2,1}(2t) = \frac{t-1}{2}.$$

We now prove similar results for $r \geq 2$. We curiously note that when comparing Theorem 16 with Theorem 17, $\theta_{2,1,1}(2t) = \theta_{2,2,1}(2t)$, but $\theta_{2,1,r}(2t) = 2\theta_{2,2,r}(2t)$ for $r \geq 2$.

Theorem 17 *For all singly-even $q = 2t$, $t \geq 1$ odd, and $r \geq 2$, we have*

$$\theta_{2,0,r}(2t) = \theta_{2,1,r}(2t) = t^r - 1, \tag{14}$$
$$\theta_{2,2,r}(2t) = \frac{t^r - 1}{2}. \tag{15}$$

Proof We start by proving (14). For all $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_q^r$, we say $\mathbf{a} \simeq \mathbf{b}$ if and only if $\mathbf{a} \equiv \mathbf{b} \pmod{t}$. Obviously, $\simeq$ is an equivalence relation. All the equivalence classes have size 2^r. We see that if $\mathbf{a} \equiv \mathbf{b} \pmod{t}$, then $2\mathbf{a} \equiv 2\mathbf{b} \pmod{2t}$. Hence, a $(2, 0, r; 2t)$-packing set S can contain at most one vector from each equivalence class, and no vectors from the equivalence class of $\mathbf{0}$. Hence,

$$\theta_{2,1,r}(2t) \leq \theta_{2,0,r}(2t) \leq \frac{(2t)^r - 2^r}{2^r} = t^r - 1. \tag{16}$$

Let X be the set of vectors in $\mathbb{Z}_{2t}^r \setminus \{(t, t, \ldots, t)\}$ such that if a_i is the first element not equal to t, then $a_i \in [1, t-1]$, and a_j is odd for all $j > i$. Then $|X| = t^r - 1$ and it is easy to see that X is a $(2, 1, r; 2t)$-packing set for $r \geq 2$ (but not for $r = 1$). Hence

$$\theta_{2,1,r}(2t) \geq |X| = t^r - 1.$$

Combined with (16), this proves (14).

To prove (15), we similarly define a relation $\cong$ in $\mathbb{Z}_{2t}^r$ by

$$\mathbf{a} \cong \mathbf{b} \text{ if and only if } \mathbf{a} \equiv \mathbf{b} \text{ or } \mathbf{a} \equiv -\mathbf{b} \pmod{t}.$$

This is again an equivalence relation. The equivalence class of $\mathbf{0}$ contains 2^r vectors, all the other equivalence classes contain 2^{r+1} vectors. A $(2, 2, r; 2t)$-packing set S can contain at most one vector from each equivalence class, and no vectors from the equivalence class of $\mathbf{0}$. Hence,

$$\theta_{2,2,r}(2t) \leq \frac{(2t)^r - 2^r}{2^{r+1}} = \frac{t^r - 1}{2}. \tag{17}$$

Let Y be the set of vectors in X for which all the elements are odd. It is easy to see that Y is a $(2, 2, r; 2t)$-packing set. Hence,

$$\theta_{2,2,r}(2t) \geq |Y| = \frac{t^r - 1}{2}.$$

Combined with (17), this proves (15). □

We remark that the set Z of vectors in $\mathbb{Z}_{2t} \setminus \{(t, t, \ldots, t)\}$ where all the elements are odd is another $(2, 0, r; 2t)$-packing set of size $t^r - 1$. However, this is not a $(2, 1, r; 2t)$-packing set; we have $Z = Y \cup (-Y)$.

Example 7 For $q = 2t$, $t = 3$ and $r = 3$, we have (we use a condensed notation for vectors, in which we omit parentheses and commas)

$$\begin{aligned}
X = \{&111, 113, 115, 131, 133, 135, 151, 153, 155,\ 311, 313, 315,\ 331,\\
&211, 213, 215, 231, 233, 235, 251, 253, 255,\ 321, 323, 325,\ 332\},\\
Y = \{&111, 113, 115, 131, 133, 135, 151, 153, 155,\ 311, 313, 315,\ 331\},\\
Z = \{&111, 113, 115, 131, 133, 135, 151, 153, 155,\ 311, 313, 315,\ 331,\\
&555, 553, 551, 535, 533, 531, 515, 513, 511,\ 355, 353, 351,\ 335\}.
\end{aligned}$$

We now consider doubly-even q. For $r = 1$, these were given in [7, Theorem 5], [15, Theorem 6], and [9, Theorem 8], respectively. We now prove them for general r.

Theorem 18 *For all doubly-even $q = 4m$, $m \geq 1$, $r \geq 2$, we have*

$$\theta_{2,0,r}(4m) = (2^r - 1)m^r + \theta_{2,0,r}(m), \tag{18}$$

$$\theta_{2,1,r}(4m) = (2^r - 1)m^r + \theta_{2,1,r}(m), \tag{19}$$

$$\theta_{2,2,r}(4m) = (2^r - 1)\left\lfloor \frac{m^r}{2} \right\rfloor + \theta_{2,2,r}(m). \tag{20}$$

Proof We start with proving (18). Let $E \subseteq \mathbb{Z}_{4m}^r$ be the set of odd vectors in $[0, 2m-1]^r$ and D an optimal $(2, 0, r; m)$-packing set. Then it is easy to see that $E \cup 4D$ is a $(2, 0, r; 4m)$-packing set. Hence

$$\theta_{2,0,r}(4m) \geq |E| + |D| = (2^r - 1)m^r + \theta_{2,0,r}(m).$$

On the other hand, let $S \subseteq \mathbb{Z}_{4m}^r$ be an optimal $(2, 0, r; 4m)$-packing set. If S contains a singly-even vector $2\mathbf{a}$ we can replace this with the odd vector $\mathbf{a}$ and get a another packing set of the same size. Repeating the argument, we get a $(2, 0, r; 4m)$-packing set S' of the same size as S and containing no singly-even vectors.

Again, we define the equivalence relation $\mathbf{a} \simeq \mathbf{b}$ if and only if $\mathbf{a} \equiv \mathbf{b} \pmod{2m}$, for all $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_{4m}^r$. For an odd vector $\mathbf{a}$, all the 2^r vectors equivalent to $\mathbf{a}$, under the relation $\simeq$, are also odd. Let S'_o denote the set of odd vectors in S'. Since the number of odd vectors in $\mathbb{Z}_{4m}^r$ is $(4m)^r - (2m)^r$, the size of S'_o satisfies

$$\left|S'_o\right| \leq \frac{(4m)^r - (2m)^r}{2^r} = (2^r - 1)m^r.$$

The remaining vectors in S', denoted S'_e, are doubly even, and it is easy to see that $\frac{1}{4}S'_e$ is a $(2, 0, r; m)$-packing set. Hence,

$$\theta_{2,0,r}(4m) = \left|S'\right| = \left|S'_o\right| + \left|S'_e\right| \leq (2^r - 1)m^r + \theta_{2,0,r}(m).$$

This completes the proof of (18).

The proof of (19) is essentially the same. If D is an optimal $(2, 1, r; m)$-packing set, then $E \cup 4D$ is a $(2, 1, r; 4m)$-packing set and so

$$\theta_{2,1,r}(4m) \geq |F| + |D| = (2^r - 1)m^r + \theta_{2,1,r}(m).$$

On the other hand, if S is an optimal $(2, 1, r; 4m)$-packing set, we let S_2 be the set of doubly-even vectors in S and S_1 the remaining vectors in S. As before, we can conclude that $|S_2| \le \theta_{2,1,r}(m)$. Furthermore, S_1 is in particular a $(2, 0, r; 4m)$-packing set where all the vectors are odd or singly even. The proof of (18) showed that $|S_1| \le (2^r - 1)m^r$. Hence

$$\theta_{2,1,r}(4m) = |S| = |S_1| + |S_2| \le (2^r - 1)m^r + \theta_{2,1,r}(m).$$

This proves (19).

The proof of (20) is also similar. First, similarly to the proof of (18) we can show that there is an optimal $(2, 2, r; 4m)$-packing set S where all vectors are odd or doubly even. This is done by replacing singly-even vectors $2\mathbf{a}$, by the odd vectors $\mathbf{a}$. One can easily verify this replacement process does not violate the $(2, 2, r; 4m)$-packing requirement. Like before, we denote by S_o the set of odd vectors in S, and by S_e the set of all doubly-even vectors in S.

As in the proof of (15), we define the congruence relation $\cong$ by $\mathbf{a} \cong \mathbf{b}$ if and only if $\mathbf{a} \equiv \pm\mathbf{b} \pmod{2m}$. If m is even, each equivalence class contains exactly 2^{r+1} vectors. Hence,

$$|S_o| \le \frac{(4m)^r - (2m)^r}{2^{r+1}} = (2^r - 1)\frac{m^r}{2} = (2^r - 1)\left\lfloor \frac{m^r}{2} \right\rfloor.$$

If m is odd and $\mathbf{a} \in \{0, m, 2m, 3m\}^r$, then $\mathbf{a} \cong -\mathbf{a}$. Hence, the corresponding equivalence class contain exactly 2^r vectors. Moreover, $2\mathbf{a} \equiv -2\mathbf{a} \pmod{4m}$. Hence, $\mathbf{a}$ cannot be contained in S. For the remaining $(4m)^r - (2m)^r - (4^r - 2^r)$ odd vectors, the corresponding equivalence class contains 2^{r+1} vectors. Hence

$$|S_o| \le \frac{(4m)^r - (2m)^r - (4^r - 2^r)}{2^{r+1}} = (2^r - 1)\frac{m^r - 1}{2} = (2^r - 1)\left\lfloor \frac{m^r}{2} \right\rfloor.$$

In both cases, $|S_e| \le \theta_{2,2,r}(m)$. Hence

$$\theta_{2,2,r}(4m) = |S| = |S_o| + |S_e| \le (2^r - 1)\left\lfloor \frac{m^r}{2} \right\rfloor + \theta_{2,2,r}(m). \tag{21}$$

We now prove the other direction. Let Y be the set vectors $(a_1, a_2, \ldots, a_r) \in [0, 2m-1]^r$ for which there is an $i \in [1, r]$ such that $a_j \in \{0, m\}$ for $1 \le j < i$ and $a_i \in [1, m-1]$. We will determine $|Y_o|$, the number of odd vectors in Y. Clearly, $|Y_o| = |Y| - |Y_e|$, where Y_e is the set of even vectors in Y.

The number of vectors in Y for a given i is $2^{i-1}(m-1)(2m)^{r-i}$. Hence

$$|Y| = \sum_{i=1}^{r} 2^{i-1}(m-1)(2m)^{r-i} = 2^{r-1}(m^r - 1).$$

If m is even, then

$$|Y_e| = \sum_{i=1}^{r} 2^{i-1}\frac{m-2}{2}m^{r-i} = \frac{1}{2}(m^r - 2^r),$$

and so

$$|Y_o| = 2^{r-1}(m^r - 1) - \frac{1}{2}(m^r - 2^r) = (2^r - 1)\frac{m^r}{2} = (2^r - 1)\left\lfloor \frac{m^r}{2} \right\rfloor.$$

If m is odd, then a_i above is the first non-zero element since m is odd. Hence

$$|Y_e| = \sum_{i=1}^{r} \frac{m-1}{2}m^{r-i} = \frac{1}{2}(m^r - 1),$$

and

$$|Y_o| = 2^{r-1}(m^r - 1) - \frac{1}{2}(m^r - 1) = (2^r - 1)\frac{m^r - 1}{2} = (2^r - 1)\left\lfloor \frac{m^r}{2} \right\rfloor.$$

If D is an optimal $(2, 2, r; m)$-packing set, $Y_o \cup 4D$ is a $(2, 2, r; 4m)$-packing set. Hence

$$\theta_{2,2,r}(4m) \geq |Y_o| + |D| = (2^r - 1)\left\lfloor \frac{m^r}{2} \right\rfloor + \theta_{2,2,r}(m).$$

□

10 Summary

In this paper we studied linear codes for the channel of limited-magnitude errors. The codes are given by sets of columns for the parity-check matrix, and we mainly considered covering sets, giving covering codes, but we also considered packing sets giving error-correcting codes. In Sect. 2 we gave some simple general results. In the rest of the paper, we determined optimal $(2, k_-, r; q)$-covering sets and optimal packing sets for all q and $0 \leq k_- \leq 2$. We also used these optimal coverings to partially answer a problem by Stein.

For values of $k_+ \geq 3$ it is an open problem to determine $\omega_{k_+,k_-,r}(q)$ and $\theta_{k_+,k_-,r}(q)$, except that $\theta_{k_+,k_-,1}(q)$ is known for a few classes of cases.

Acknowledgments This study is supported by The Norwegian Research Council and by ISF Grant 134/10.

Appendix

Proof of Theorem 5

In the setting of Theorem 5 we have q odd. Let $\varsigma_r(q)$ denote the number of cyclotomic cosets of odd size. In [8], an expression for $\varsigma_1(q)$ was given, in a slightly different notation. Here we will use a similar method to show that $\varsigma_r(q) = \vartheta_r(q_0)$ for all r.

Let

$$\mathbb{Z}_q^* = \{a \mid \gcd(a, q) = 1, a \in [1, q - 1]\},$$

and for $d|q$, let

$$\mathbb{Z}_{q,d} = \left\{ a\frac{q}{d} \,\middle|\, a \in \mathbb{Z}_d^* \right\}.$$

In particular, $\mathbb{Z}_{q,1} = \{0\}$. The size of $\mathbb{Z}_{q,d}$ is $\varphi(d)$, where $\varphi(\cdot)$ is Euler's totient function. We have the following disjoint-union decomposition [8, Lemma 4]:

$$\mathbb{Z}_q = \bigcup_{d|q} \mathbb{Z}_{q,d}. \tag{22}$$

Lemma 4 *Let d be a divisor of q. For any $b \in \mathbb{Z}_{q,d}$, the least positive ℓ such that $2^\ell b \equiv b \pmod q$ is exactly ℓ_d.*

Proof Let $b = a \cdot q/d$. Since $\gcd(a, q) = 1$ by definition, we have the following equivalences:

$$2^\ell \equiv 1 \pmod d \Leftrightarrow 2^\ell \frac{q}{d} \equiv \frac{q}{d} \pmod q \Leftrightarrow 2^\ell a\frac{q}{d} \equiv a\frac{q}{d} \pmod q.$$

□

We observe that Lemma 4 implies that $\mathbb{Z}_{q,d}$ is the disjoint union of $\varphi(d)/\ell_d$ cosets of size ℓ_d.

In [8, Lemma 5] the following result was given.

Lemma 5 *(i) For odd $d = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$, with p_i distinct odd primes, we have*

$$\ell_d = \operatorname{lcm}\left(\ell_{p_1^{e_1}}, \ell_{p_2^{e_2}}, \dots, \ell_{p_s^{e_s}}\right).$$

In particular, $v_2(\ell_d) = i$ if and only if $\max_{1\le j\le s} v_2(\ell_{p_j^{e_j}}) = i$.

(ii) For any odd prime p, suppose $2^{\ell_p} = 1 + p^{u_p} s_p$ with $p \nmid s_p$. Then

$$\ell_{p^k} = \begin{cases} \ell_p & \text{if } k \le u_p, \\ p^{k-u_p}\ell_p & \text{if } k > u_p. \end{cases}$$

From Lemma 5 we get the following more general result:

Lemma 6 *For any odd q, and $d_1, d_2, \dots, d_r$ divisors of q we have*

$$\operatorname{lcm}(\ell_{d_1}, \ell_{d_2}, \dots, \ell_{d_r}) = \ell_{\operatorname{lcm}(d_1,d_2,\dots,d_r)}.$$

Proof Let p_j, $j = 1, 2, \dots, s$, be the set of all primes dividing q, and let $d_i = \prod_{j=1}^{s} p_j^{e_{i,j}}$. Then

$$\operatorname{lcm}(d_1, d_2, \dots, d_r) = \prod_{j=1}^{s} p_j^{\max_{1\le i\le r} e_{i,j}}.$$

By Lemma 5 we get

$$\begin{aligned}\operatorname{lcm}_{1\le i\le r}(\ell_{d_i}) &= \operatorname{lcm}_{1\le i\le r} \operatorname{lcm}_{1\le j\le s}(\ell_{p_j^{e_{i,j}}}) = \operatorname{lcm}_{1\le j\le s} \operatorname{lcm}_{1\le i\le r}(\ell_{p_j^{e_{i,j}}}) \\ &= \operatorname{lcm}_{1\le j\le s}(\ell_{p_j^{\max_{1\le i\le r} e_{i,j}}}) = \ell_{\operatorname{lcm}(d_1,d_2,\dots,d_r)}.\end{aligned}$$

□

Now, consider a cyclotomic coset in $\mathbb{Z}_q^r$, generated by $(a_1, a_2, \dots a_r)$. Suppose $a_i \in \mathbb{Z}_{q,d_i}$. Then the size of the coset is $\operatorname{lcm}(\ell_{d_1}, \ell_{d_2}, \dots, \ell_{d_r}) = \ell_{\operatorname{lcm}(d_1,d_2,\dots,d_r)}$, and the number of such cosets is

$$\frac{\varphi(d_1)\varphi(d_2)\dots\varphi(d_r)}{\ell_{\operatorname{lcm}(d_1,d_2,\dots,d_r)}}.$$

We get cosets of odd order if and only if $d_i | q_0$ for all i. Hence we get

$$\varsigma_r(q) = \sum_{d_1|q_0} \sum_{d_2|q_0} \cdots \sum_{d_r|q_0} \frac{\varphi(d_1)\varphi(d_2)\dots\varphi(d_r)}{\ell_{\operatorname{lcm}(d_1,d_2,\dots,d_r)}} = \sum_{d|q_0} \frac{\Phi_r(d)}{\ell_d}, \tag{23}$$

where

$$\Phi_r(d) = \sum_{\operatorname{lcm}(d_1,d_2,\dots,d_r)=d} \varphi(d_1)\varphi(d_2)\dots\varphi(d_r).$$

It follows that

$$\sum_{c|d} \Phi_r(c) = \sum_{d_1|d, d_2|d, \ldots, d_r|d} \varphi(d_1)\varphi(d_2)\ldots\varphi(d_r)$$
$$= \left(\sum_{d_1|d} \varphi(d_1)\right)\left(\sum_{d_2|d} \varphi(d_2)\right)\ldots\left(\sum_{d_r|d} \varphi(d_r)\right) = \left(\sum_{a|d} \varphi(a)\right)^r = d^r.$$

Using Möbius inversion, we get

$$\Phi_r(d) = \sum_{c|d} \mu\left(\frac{d}{c}\right) c^r. \tag{24}$$

Substituting this expression in (23) we get

$$\varsigma_r(q) = \vartheta_r(q_0).$$

This completes the proof of Theorem 5.

For $r = 1$, the expression in (23) was given in [8, Theorem 2], in a slightly different notation. In the same theorem we determined $\theta_{2,0,1}(q)$. For $r > 1$, the result is new.

Example 8 If $q_0 = p^a$, where p is a prime and $a \geq 1$, the divisors of q_0 are p^b, $b \in [0, a]$. If $d = p^b > 1$, then $\mu(d/c) \neq 0$ for $c \mid d$ exactly for $c = p^a$ and $c = p^{a-1}$. Since $\mu(1) = 1$ and $\mu(p) = -1$, we get

$$\vartheta_r(p^a) = 1 + \sum_{b=1}^{a} \frac{p^{br} - p^{(b-1)r}}{\ell_{p^b}}.$$

In particular, if $v_2\left(2^{\ell_p} - 1\right) = 1$, that is $u_p = 0$ (which is the situation in most cases), Lemma 5 implies that $\ell_{p^b} = p^{b-1}\ell_p$ for all $b \geq 1$. Hence, in this case we get

$$\vartheta_1(p^a) = 1 + \frac{1}{\ell_p} \sum_{b=1}^{a} (p-1) = 1 + \frac{a(p-1)}{\ell_p}.$$

and for $r > 1$ we get

$$\vartheta_r(p^a) = 1 + \frac{1}{\ell_p} \sum_{b=1}^{a} \left(p^{b(r-1)+1} - p^{(b-1)(r-1)}\right) = 1 + \frac{(p^r - 1)(p^{a(r-1)} - 1)}{(p^{r-1} - 1)\ell_p}.$$

In particular,

$$\vartheta_1(p^r) = 1 + \frac{r(p-1)}{\ell_p} \quad \text{and} \quad \vartheta_r(p) = 1 + \frac{p^r - 1}{\ell_p},$$

and so $\vartheta_1(p^r) < \vartheta_r(p)$. This is a special case of Lemma 10 below.

Proof of Theorem 8

The expressions for $\omega_{2,0,r}(q)$ in Theorem 5 and $\theta_{2,0,r}(q)$ in (12), and their proofs, are closely related. In the same way we will get closely related expressions and proofs for $\omega_{2,2,r}(q)$ and $\theta_{2,2,r}(q)$. For $\theta_{2,2,1}(q)$, the expression in Theorem 8 was given in [9], in a slightly different notation. For general r we get a proof that generalizes its proof.

Consider the coset generated by a non-zero $\mathbf{a} = (a_1, a_2, \ldots, a_r) \in \mathbb{Z}_q^r$. We first remark that if $-\mathbf{a} \in \sigma(\mathbf{a})$, that is, $\sigma(-\mathbf{a}) = \sigma(\mathbf{a})$, then $|\sigma(\mathbf{a})|$ is even: if $u > 0$ is minimal such that $-\mathbf{a} = 2^u\mathbf{a} \pmod q$, then $|\sigma(\mathbf{a})| = 2u$.

The coset $\sigma(\mathbf{a})$ has odd size if and only if $\sigma(a_i)$, $1 \le i \le r$, all have odd size. In this case $\sigma(\mathbf{a})$ and $\sigma(-\mathbf{a})$ are disjoint, and the $(|\sigma(\mathbf{a})| + 1)/2$ elements $2^{2i}\mathbf{a}$, $i \in [0, (|\sigma(\mathbf{a})| - 1)/2]$ will cover $\sigma(\mathbf{a}) \cup \sigma(-\mathbf{a})$, and the union cannot be covered by fewer elements. We select these elements in a covering set. Hence we get a contribution $(|\sigma(\mathbf{a})| + 1)/4$ to $\omega_{2,2,r}(q)$ from the coset $\sigma(\mathbf{a})$ and $(|\sigma(\mathbf{a})| + 1)/4 = (|\sigma(-\mathbf{a})| + 1)/4$ from the coset $\sigma(-\mathbf{a})$. The number of such cosets is $\vartheta_r(q_0)$ as was shown in the proof of Theorem 5.

If $|\sigma(\mathbf{a})|$ is even, but $\sigma(-\mathbf{a}) \ne \sigma(\mathbf{a})$ (that is, the two sets are disjoint), then we select the $|\sigma(\mathbf{a})|/2$ elements $2^{2i}\mathbf{a}$, $i \in [0, |\sigma(\mathbf{a})|/2 - 1]$ to cover $\sigma(\mathbf{a}) \cup \sigma(-\mathbf{a})$. The contribution to $\omega_{2,2,r}(q)$ from the cosets $\sigma(\mathbf{a})$ and $\sigma(-\mathbf{a})$ is therefore $|\sigma(\mathbf{a})|/4 + |\sigma(-\mathbf{a})|/4$.

Now, consider the situation when $\sigma(-\mathbf{a}) = \sigma(\mathbf{a})$. As before, let $u > 0$ be the minimal integer such that $-\mathbf{a} = 2^u\mathbf{a} \pmod q$. If u is even, then the $u/2 = |\sigma(\mathbf{a})|/4$ elements $2^{2i}\mathbf{a}$, $i \in [0, u/2 - 1]$ cover $\sigma(\mathbf{a})$. Finally, if u is odd, then the $(u+1)/2 = (|\sigma(\mathbf{a})|+2)/4$ elements $2^{2i}\mathbf{a}$, $i \in [0, (u-1)/2]$ cover $\sigma(\mathbf{a})$. We see that u is odd if and only if $\sigma(a_i)$ is singly even for all i. In the proof of [9, Theorem 6], it was shown that this occurs exactly when $a_i \in \mathbb{Z}_{q,d_i}$ for some $d_i | q_1$. A proof similar to the proof in Appendix 10 shows that the number of such cosets is $\vartheta_r(q_1)$. Summing over all the cosets, we get the expression in Theorem 8.

A result for $\vartheta_r(q)$

A simple, but useful relation is the following.

Lemma 7 *If $d_1 | d_2$, then $\ell_{d_1} \le \ell_{d_2}$.*

Proof By definition, $d_2 | 2^{\ell_{d_2}} - 1$ and so $d_1 | 2^{\ell_{d_2}} - 1$, which implies that $\ell_{d_1} \le \ell_{d_2}$ (and in fact $\ell_{d_1} | \ell_{d_2}$). □

We recall that $\Phi_r(d)$ was defined by (24). This is a multiplicative function, as the following lemma shows.

Lemma 8 *If $\gcd(d_1, d_2) = 1$, then $\Phi_r(d_1 d_2) = \Phi_r(d_1)\Phi_r(d_2)$.*

Proof If $c | d_1 d_2$, then $c = c_1 c_2$, where $c_1 | d_1$ and $c_2 | d_2$. Hence

$$\Phi_r(d_1 d_2) = \sum_{c | d_1 d_2} \mu\left(\frac{d_1 d_2}{c}\right) c^r = \left(\sum_{c | d_1} \mu\left(\frac{d_1}{c}\right) c^r\right)\left(\sum_{c | d_2} \mu\left(\frac{d_2}{c}\right) c^r\right) = \Phi_r(d_1)\Phi_r(d_2).$$

□

For a prime p, define $\Delta_r(p^\beta)$ by

$$\Delta_r(p^\beta) = \begin{cases} 1 & \beta = 0, \\ p^{r\beta} - p^{r(\beta-1)} & \text{otherwise.} \end{cases}$$

For convenience, we let $\Delta(p^\beta) = \Delta_1(p^\beta)$.

Lemma 9 *If p is a prime and $\beta \ge 1$, then*

$$\Phi_r(p^\beta) = \Delta_r(p^\beta) = \sum_{j=0}^{r-1} \Delta(p^{\beta-j}).$$

Proof We have

$$\Phi_r(p^\beta) = p^{r\beta} - p^{r(\beta-1)} = \Delta_r(p^\beta) = \sum_{j=0}^{r-1} \left(p^{r\beta-j} - p^{r\beta-j-1} \right) = \sum_{j=0}^{r-1} \Delta(p^{\beta-j}).$$

□

We now give a main lemma on $\vartheta_r(q)$.

Lemma 10 *For all $r \geq 2$ and odd q we have $\vartheta_1(q^r) \leq \vartheta_r(q)$.*

Proof By definition, $\vartheta_r(q) = \sum_{d|q} \frac{1}{\ell_d} \Phi_r(d)$. Let $q = \prod_{i=1}^s p_i^{\alpha_i}$ be the prime factorization of q. The divisors of q^r are all numbers of the form $\prod_{i=1}^s p_i^{\beta_i}$ where $0 \leq \beta_i \leq r\alpha_i$. Using Lemmas 8 and 9, we get

$$\Phi_r\left(\prod_{i=1}^s p_i^{\beta_i} \right) = \prod_{i=1}^s \Phi_r\left(p_i^{\beta_i} \right) = \prod_{\substack{1 \leq i \leq s \\ \beta_i > 0}} \sum_{j_i=0}^{r-1} \Delta\left(p_i^{r\beta_i - j_i} \right).$$

Hence

$$\vartheta_r(q) = \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \cdots \sum_{\beta_s=0}^{\alpha_s} \frac{1}{\ell_{\prod_{1 \leq i \leq s} p_i^{\beta_i}}} \prod_{\substack{1 \leq i \leq s \\ \beta_i > 0}} \sum_{j_i=0}^{r-1} \Delta\left(p_i^{r\beta_i - j_i} \right).$$

Similarly, we get

$$\vartheta_1(q^r) = \sum_{\beta_1=0}^{r\alpha_1} \sum_{\beta_2=0}^{r\alpha_2} \cdots \sum_{\beta_s=0}^{r\alpha_s} \frac{1}{\ell_{\prod_{1 \leq i \leq s} p_i^{\beta_i}}} \prod_{i=1}^s \Delta\left(p_i^{\beta_i} \right).$$

In order to compare the two expressions we note all the summands are non-negative, and of the form $\prod_{i=1}^s \Delta(p_i^{\gamma_i})$. One can verify that the coefficient of $\prod_{i=1}^s \Delta(p_i^{\gamma_i})$ in $\vartheta_r(q)$ is

$$C_r = \ell^{-1}_{\prod_{1 \leq i \leq s} p_i^{\lceil \gamma_i / r \rceil}},$$

whereas its coefficient in $\vartheta_1(q^r)$ is

$$C_1 = \ell^{-1}_{\prod_{1 \leq i \leq s} p_i^{\gamma_i}}.$$

Since $\lceil \gamma_i / r \rceil \leq \gamma_i$ we have

$$\prod_{1 \leq i \leq s} p_i^{\lceil \gamma_i / r \rceil} \Bigg| \prod_{1 \leq i \leq s} p_i^{\gamma_i},$$

and so $C_r \geq C_1$ by Lemma 7. Hence $\vartheta_r(q) \geq \vartheta_1(q^r)$. □

We illustrate the proof by a simple example.

Example 9 Let $q = p^2\pi$ where p and π are distinct odd primes, and let $r = 2$. Then

$$\begin{aligned}\vartheta_2(q) &= 1 + \frac{\Delta_2(p)}{\ell_p} + \frac{\Delta_2(p^2)}{\ell_{p^2}} + \frac{\Delta_2(\pi)}{\ell_\pi} + \frac{\Delta_2(p)\Delta_2(\pi)}{\ell_{p\pi}} + \frac{\Delta_2(p^2)\Delta_2(\pi)}{\ell_{p^2\pi}} \\ &= 1 + \frac{\Delta(p^2)+\Delta(p)}{\ell_p} + \frac{\Delta(p^4)+\Delta(p^3)}{\ell_{p^2}} \\ &\quad + \frac{\Delta(\pi^2)+\Delta(\pi)}{\ell_\pi} + \frac{\big(\Delta(p^2)+\Delta(p)\big)\big(\Delta(\pi^2)+\Delta(\pi)\big)}{\ell_{p\pi}} \\ &\quad + \frac{\big(\Delta(p^4)+\Delta(p^3)\big)\big(\Delta(\pi^2)+\Delta(\pi)\big)}{\ell_{p^2\pi}},\end{aligned}$$

and

$$\begin{aligned}\vartheta_1(q^2) &= 1 + \frac{\Delta(p)}{\ell_p} + \frac{\Delta(p^2)}{\ell_{p^2}} + \frac{\Delta(p^3)}{\ell_{p^3}} + \frac{\Delta(p^4)}{\ell_{p^4}} \\ &\quad + \frac{\Delta(\pi)}{\ell_\pi} + \frac{\Delta(p)\Delta(\pi)}{\ell_{p\pi}} + \frac{\Delta(p^2)\Delta(\pi)}{\ell_{p^2\pi}} + \frac{\Delta(p^3)\Delta(\pi)}{\ell_{p^3\pi}} + \frac{\Delta(p^4)\Delta(\pi)}{\ell_{p^4\pi}} \\ &\quad + \frac{\Delta(\pi^2)}{\ell_{\pi^2}} + \frac{\Delta(p)\Delta(\pi^2)}{\ell_{p\pi^2}} + \frac{\Delta(p^2)\Delta(\pi^2)}{\ell_{p^2\pi^2}} + \frac{\Delta(p^3)\Delta(\pi^2)}{\ell_{p^3\pi^2}} + \frac{\Delta(p^4)\Delta(\pi^2)}{\ell_{p^4\pi^2}}.\end{aligned}$$

For example, for $\Delta(p^3)\Delta(\pi)$, the coefficients are $1/\ell_{p^3\pi}$ and $1/\ell_{p^2\pi}$ respectively, and $\ell_{p^2\pi} \le \ell_{p^3\pi}$.

References

1. Andrews G.E.: Number Theory. W. B. Saunders Co., Philadelphia (1971).
2. Cassuto Y., Schwartz M., Bohossian V., Bruck J.: Codes for asymmetric limited-magnitude errors with applications to multilevel flash memories. IEEE Trans. Inf. Theory **56**(4), 1582–1595 (2010).
3. Chen Z., Shparlinski I.E., Winterhof A.: Covering sets for limited-magnitude errors. arXiv:1310.0120v1 [cs.IT] 1 Oct 2013.
4. Hardy G.H., Wright E.M.: An Introduction to the Theory of Numbers, 4th edn. Oxford University Press, London (1960).
5. Jiang A., Langberg M., Schwartz M., Bruck J.: Trajectory codes for flash memory. IEEE Trans. Inf. Theory **59**(7), 4530–4541 (2013).
6. Kløve T., Schwartz M.: Covering sets for limited-magnitude errors. In: Preproceedings, International Workshop on Coding and Cryptography (WCC), Bergen, 15–19 April 2013, pp. 69–78. http://www.selmer.uib.no/WCC2013/PreProceedings.
7. Kløve T., Bose B., Elarief N.: Systematic, single limited magnitude error correcting codes for flash memories. IEEE Trans. Inf. Theory **57**(7), 4477–4487 (2011).
8. Kløve T., Luo J., Naydenova I., Yari S.: Some codes correcting asymmetric errors of limited magnitude. IEEE Trans. Inf. Theory **57**(11), 7459–7472 (2011).
9. Kløve T., Luo J., Yari S.: Codes correcting single errors of limited magnitude. IEEE Trans. Inf. Theory **58**(4), 2206–2219 (2012).
10. Schwartz M.: Quasi-cross lattice tilings with applications to flash memory. IEEE Trans. Inf. Theory **58**(4), 2397–2405 (2012).
11. Schwartz M.: On the non-existence of lattice tilings by quasi-crosses. Eur. J. Comb. **36**, 130–142 (2014).
12. Stein S.K.: Tiling, packing, and covering by clusters. Rocky Mt. J. Math. **16**, 277–321 (1986).
13. Stein S.K., Szabó S.: Algebra and Tiling. The Mathematical Association of America, Washington, DC (1994).
14. Szabó S.: Lattice covering by semicrosses of arm length 2. Eur. J. Comb. **12**, 263–266 (1991).
15. Yari S., Kløve T., Bose B.: Some codes correcting unbalanced errors of limited magnitude for flash memories. IEEE Trans. Inf. Theory **59**(11), 7278–7287 (2013).