Covering Sets for Limited-Magnitude Errors

Torleiv Kløve and Moshe Schwartz

Channel model

Let μ, λ be integers such that $0 \leq \mu \leq \lambda$, 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

$$\{(a+e) \bmod q \mid -\mu \leq e \leq \lambda\} .$$

Some notations

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

$$[a, b] = \{a, a+1, a+2, \ldots, b\},$$

$$[a, b]^* = [a, b] \setminus \{0\}.$$

In particular, for $0 \leq \mu \leq \lambda$,

$$M = [-\mu, \lambda]^* = \{-\mu, -\mu+1, -\mu+2, \ldots, -1\} \cup \{1, 2, \ldots, \lambda\}.$$

For any $S \subseteq \mathbb{Z}_q$ we define

$$MS = \{xs \in \mathbb{Z}_q \mid x \in M, s \in S\}.$$

Packing sets and error correcting codes

If $|MS| = (\mu + \lambda)|S|$, then S is packing set.
A packing set S where $0 \notin MS$ is a $B[-\mu, \lambda](q)$ set.

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

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

is a code that can correct a single limited-magnitude error from the set $[-\mu, \lambda]$.
Such codes have been studied in a number of papers by a number of people; see references in the proceedings.

Covering sets and covering codes

A set S is called a $(\lambda, \mu; q)$ covering set if $MS = \mathbb{Z}_q$.
The corresponding code is a covering code.

For packing sets, we want to pack as many disjoint translates Ms, $s \in S$ as possible into $\mathbb{Z}_q$.

For the covering set, we are interested in having the union of Ms, $s \in S$, cover $\mathbb{Z}_q$ entirely with S being as small as possible.

Covering sets

Covering sets is the topic for this talk.

Goal: determine or estimate $\omega(q) = \omega_{\lambda,\mu}(q)$, the smallest size of a $(\lambda, \mu; q)$ covering set.

Two bounds

- A Hamming type bound:

$$\omega_{\lambda,\mu}(q) \geq \left\lceil \frac{q}{\lambda+\mu} \right\rceil .$$

Two bounds

- A Hamming type bound:

$$\omega_{\lambda,\mu}(q) \geq \left\lceil \frac{q}{\lambda+\mu} \right\rceil .$$

- A BCH type bound:
  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

$$\omega_{\lambda,\mu}(p) \leq \left\lceil \frac{p-1}{\delta} \right\rceil + 1.$$

Simple examples

Example

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

Example

Let $\mu = \lambda = 1$. Clearly $|MS| \leq 2|S|$. Hence

$$\omega_{1,1}(q) \geq \left\lceil \frac{q}{2} \right\rceil .$$

On the other hand

$$M\left[1, \left\lceil \frac{q}{2} \right\rceil\right] = \mathbb{Z}_q .$$

Hence

$$\omega_{1,1}(q) = \left\lceil \frac{q}{2} \right\rceil .$$

On the general situation

For $\lambda \geq 2$, it seems to be quite complicated to determine and ω in many cases.

Here, we consider $\omega_{2,0}(q)$ and $\omega_{2,1}(q)$.

$\omega_{2,0}(q)$ for odd q

If $p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$ is the prime factorization of q, let

$$q_o = \prod_{\substack{1 \le i \le s \\ p_i \in P_o}} p_i^{t_i},$$

where P_o is the set of odd primes p such that $\mathrm{ord}_p(2)$ is odd. Then

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

$\omega_{2,0}(q)$ for $q \equiv 2 \pmod 4$

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

$\omega_{2,0}(q)$ for $q \equiv 2 \pmod 4$

- For $m \geq 0$ we have $\omega_{2,0}(4m+2) = 2m+1$.
- Proof:

$\omega_{2,0}(q)$ for $q \equiv 2 \pmod 4$

- For $m \geq 0$ we have $\omega_{2,0}(4m+2) = 2m+1$.
- Proof:
- By the upper bound, $\omega_{2,0}(4m+2) \geq 2m+1$.

$\omega_{2,0}(q)$ for $q \equiv 2 \pmod 4$

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

- Proof:
- By the upper bound, $\omega_{2,0}(4m+2) \geq 2m+1$.
- On the other hand, $\{1, 3, 5, \ldots, 4m+1\}$ is a covering set of size $2m+1$.

$\omega_{2,0}(q)$ for $q \equiv 0 \pmod 4$

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

$\omega_{2,0}(q)$ for $q \equiv 0 \pmod 4$

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

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

$\omega_{2,0}(q)$ for $q \equiv 0 \pmod 4$

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

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

- To show that $\omega_{2,0}(4m) \geq 2m + \omega_{2,0}(m)$ is also relatively easy.

$\omega_{2,1}(q)$ for q odd

- For all $m \geq 1$ we have $\omega_{2,1}(2m+1) = m+1$.

$\omega_{2,1}(q)$ for q odd

- For all $m \geq 1$ we have $\omega_{2,1}(2m+1) = m+1$.
- The set $[0, m]$ is clearly a $(1, 1; 2m+1)$ covering set. Hence $\omega_{1,1}(2m+1) = m+1$.

$\omega_{2,1}(q)$ for q odd

- For all $m \geq 1$ we have $\omega_{2,1}(2m+1) = m+1$.
- The set $[0, m]$ is clearly a $(1, 1; 2m+1)$ covering set. Hence $\omega_{1,1}(2m+1) = m+1$.
- This implies that $\omega_{2,1}(2m+1) \geq \omega_{1,1}(2m+1) = m+1$.

$\omega_{2,1}(q)$ for q odd

- For all $m \geq 1$ we have $\omega_{2,1}(2m+1) = m+1$.
- The set $[0, m]$ is clearly a $(1, 1; 2m+1)$ covering set. Hence $\omega_{1,1}(2m+1) = m+1$.
- This implies that $\omega_{2,1}(2m+1) \geq \omega_{1,1}(2m+1) = m+1$.
- To show that $\omega_{2,1}(2m+1) = \omega_{1,1}(2m+1)$ is a little tricky.

$\omega_{2,1}(q)$ for $q \equiv 0 \pmod 4$

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

$\omega_{2,1}(q)$ for $q \equiv 0 \pmod 4$

- For all $m \geq 1$ we have $\omega_{2,1}(4m) = m + \omega_{2,1}(m)$.
- Let D be an optimal $(2, 1; m)$ covering set. The set

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

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

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

$\omega_{2,1}(q)$ for $q \equiv 0 \pmod 4$

- For all $m \geq 1$ we have $\omega_{2,1}(4m) = m + \omega_{2,1}(m)$.
- Let D be an optimal $(2, 1; m)$ covering set. The set

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

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

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

- To show that $\omega_{2,1}(4m) \geq m + \omega_{2,1}(m)$ is also relatively easy.

$\omega_{2,1}(q)$ for $q \equiv 2 \pmod 4$

- This case is harder.

$\omega_{2,1}(q)$ for $q \equiv 2 \pmod 4$

- This case is harder.
- Optimal sets for $q \geq 18$:

$4m + 2$	$\omega_{2,1}(4m + 2)$	an optimal $(2, 1; 4m + 2)$ covering set
2	1	$\{1\}$
6	3	$\{1, 3, 5\}$
10	4	$\{1, 3, 4, 5\}$
14	6	$\{1, 3, 4, 5, 7, 12\}$
18	8	$\{1, 3, 4, 5, 7, 8, 9, 12\}$

$\omega_{2,1}(q)$ for $q \equiv 2 \pmod 4$

- A lower bound:
  For all $m \geq 1$ we have

$$\omega_{2,1}(4m+2) \geq \frac{3m}{2} + 1.$$

$\omega_{2,1}(q)$ for $q \equiv 2 \pmod 4$

- A lower bound:
  For all $m \geq 1$ we have

$$\omega_{2,1}(4m+2) \geq \frac{3m}{2} + 1.$$

- For an upper bound:
  Let v_2 denote the 2-ary evaluation,
  that is $n = 2^{v_2(n)} n_1$, where n_1 is odd.

$\omega_{2,1}(q)$ for $q \equiv 2 \pmod 4$

- For $m \geq 0$, let $S = X \cup Y \cup Z$, where

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

$\omega_{2,1}(q)$ for $q \equiv 2 \pmod 4$

- For $m \geq 0$, let $S = X \cup Y \cup Z$, where

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

- S is a $(2,1;4m+2)$ covering set.

$\omega_{2,1}(q)$ for $q \equiv 2 \pmod 4$

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

$\omega_{2,1}(q)$ for $q \equiv 2 \pmod 4$

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

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

A recursive construction

- Let $S' \subseteq \mathbb{Z}_{2m+1}$ be a $(2, 2; 2m + 1)$ covering set such that $S' \subseteq [0, m]$.

A recursive construction

- 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

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

A recursive construction

- 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

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

- S is a $(2,1;4m+2)$ covering set.

A recursive construction

- 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

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

- S is a $(2, 1; 4m + 2)$ covering set.
- $\omega_{2,1}(4m + 2) \leq m + \omega_{2,2}(2m + 1)$.

Optimal (2,1) sets

- If $v_2(\mathrm{ord}_p(2)) \geq 2$ for any prime p dividing $2m+1$, then

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

Optimal (2,1) sets

- If $v_2(\mathrm{ord}_p(2)) \geq 2$ for any prime p dividing $2m+1$, then
$$\omega_{2,1}(4m+2) = \frac{3m}{2} + 1.$$
- Of the first 1000 even m, 390 satisfy the condition, the first ten are 2, 6, 8, 12, 14, 18, 20, 26, 30, 32.

Optimal (2,1) sets

- If $v_2(\mathrm{ord}_p(2)) \geq 2$ for any prime p dividing $2m+1$, then

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

- Of the first 1000 even m, 390 satisfy the condition, 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.

Some new results - not in proceedings

- Expression for $\omega_{2,2}(2m+1)$ (somewhat complicated).

Some new results - not in proceedings

- Expression for $\omega_{2,2}(2m+1)$ (somewhat complicated).
- $\omega_{2,2}(4m+2) = m+1$.

Some new results - not in proceedings

- Expression for $\omega_{2,2}(2m+1)$ (somewhat complicated).
- $\omega_{2,2}(4m+2) = m+1$.
- $\omega_{2,2}(4m) = m + \omega_{2,2}(m)$

Some new results - not in proceedings

- Expression for $\omega_{2,2}(2m+1)$ (somewhat complicated).
- $\omega_{2,2}(4m+2) = m+1$.
- $\omega_{2,2}(4m) = m + \omega_{2,2}(m)$
- $\omega_{2,1}(4m+2) = m + \omega_{2,2}(2m+1)$.

THANK YOU