Codes for errors of limited magnitude

Torleiv Kløve

MMC, September 7, 2017

Some notations

The ring of integers modulo q is represented by the integers $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$.
For integers $q > 0$ and a, $(a \bmod q)$ denotes the main residue of a modulo q, that is, the least non-negative integer r such that q divides $a - r$.
For $a, b \in \mathbb{Z}_q$ and $x \in \mathbb{Z}$, we denote addition, subtraction, and multiplication by

- $a \oplus b = ((a + b) \bmod q)$
- $a \ominus b = ((a - b) \bmod q)$
- $x \otimes b = (xb \bmod q)$

Limited errors

We consider the following channel:
Our alphabet is $\mathbb{Z}_q$.

Let λ and μ be integers, where $0 \leq \mu \leq \lambda < q - \mu$.
Let $[-\mu, \lambda] = \{-\mu, -\mu + 1, \ldots, \lambda - 1, \lambda\}$ and
$[-\mu, \lambda]^* = \{-\mu, -\mu + 1, \ldots, -1\} \cup \{1, 2, \ldots, \lambda\}$.

An element $a \in \mathbb{Z}_q$ may be changed into $a \oplus x$, where $x \in [-\mu, \lambda]$.

Example

Suppose that $q = 9$, $\mathbb{Z}_q = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.
Let $\mu = 1$ and $\lambda = 2$. Then

element	can be changes to
0	$8, 0, 1, 2$
1	$0, 1, 2, 3$
2	$1, 2, 3, 4$
3	$2, 3, 4, 5$
4	$3, 4, 5, 6$
5	$4, 5, 6, 7$
6	$5, 6, 7, 8$
7	$6, 7, 8, 0$
8	$7, 8, 0, 1$

Codes: packings and coverings

The (λ, μ)-quasi-cross with center $\mathbf{a}$ in $\mathbb{Z}_q^n$ is the set

$$X(\mathbf{a}) = \bigcup_{i=1}^{n} \{(a_1, a_2, \ldots, a_{i-1}, a_i \oplus x_i, a_{i+1}, \ldots, a_n) \mid x_i \in [-\mu, \lambda]\}.$$

We see that $|X(\mathbf{a})| = 1 + n(\lambda + \mu)$.

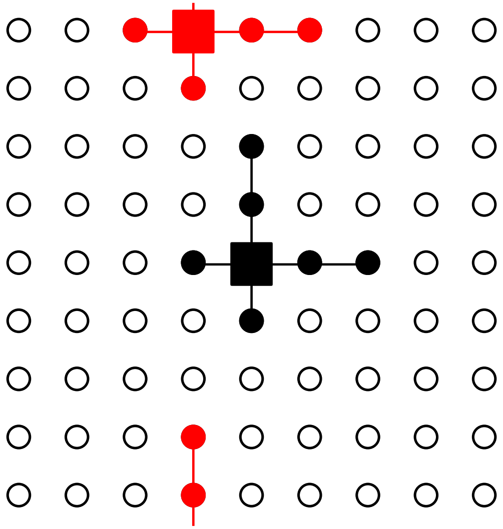
A code of length n is a set $C \subset \mathbb{Z}_q^n$.

The code is a (λ, μ)-packing (or single error correcting code) if the quasi-crosses $X(\mathbf{a})$ where $\mathbf{a} \in C$ are disjoint.

The code is a (λ, μ)-covering if $\bigcup_{\mathbf{a} \in C} X(\mathbf{a}) = \mathbb{Z}_q^n$.

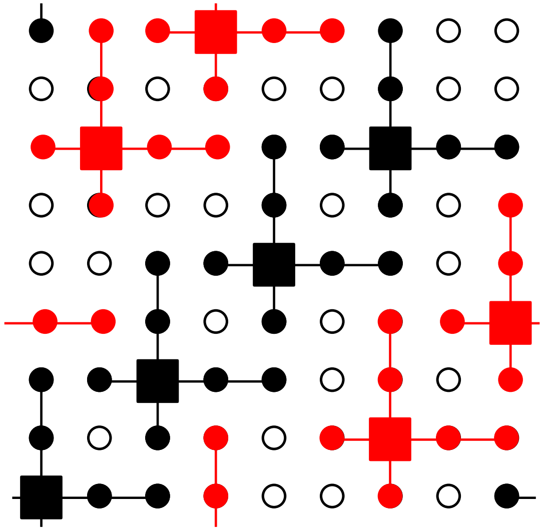
Example of $(2,1)$-packing of length 2 in $\mathbb{Z}_9^2$

A "sphere" is a quasi-cross with arms of lengths 1 and 2.
A code, i.e. $(2,1)$-packing, $C \subset \mathbb{Z}_9^2$ can correct single errors if all the quasi-crosses corresponding to codewords are disjoint.
Example. Codewords$=(3,8),(4,4)$:



Example continued

A possible code of size 8 in $\mathbb{Z}_9^2$ is
$\{(0,0),(2,2),(4,4),(6,6),(1,6),(6,1),(3,8),(8,3)\}$.
This has maximal size for $(2,1)$-packings of $\mathbb{Z}_9^2$ (checked by exhaustive search).



We see that for $q = 2$, a $(1, 0)$-code is an ordinary binary code.

More general, a $(q - 1, 0)$ is an ordinary q-ary code.
From now on, we consider $\lambda < q - 1$.

Construction of packing and covering codes for these channels have been studied over many years. Most results are for the cases where we have some limitation on the parameters, in particular $\mu = 0$ (an asymmetric channel) and $\mu = \lambda$ (a symmetric channel).
The case $0 < \mu < \lambda$ has only been studied the last 5-6 years.

Content of the talk

In this talk I will describe some of the these codes. They are mainly

- linear codes for $\mu < \lambda$.
- linear codes for $n = 2$.
- non-linear codes for $n = 2$.

A general situation:

Let q be a positive integer.
Let G be a finite Abelian group such that

$$q\,g = 0 \text{ for all } g \in G.$$

A $(-\mu, \lambda)$-splitter set $S = \{s_1, s_2, \dots s_n\}$ of G is a subset of G such that all ℓs, where $\ell \in [-\mu, \lambda]^*$ and $s \in S$, are distinct and non-zero elements of G.

For $v \in G$, let

$$C_v = \{(x_1, x_2, \dots, x_n) \in \mathbb{Z}_q^n \mid x_1 s_1 + x_2 s_2 + \cdots + x_n s_n = v\}.$$

This is a code that can correct a single error.
Ref: (Varshamov and Tenengoltz 1965), (Stein 1984), (Ahlswede et al. 2004), (Schwartz 2012).

$B[-\mu, \lambda](q)$ sets.

$(-\mu, \lambda)$-splitter sets in $\mathbb{Z}_q$ are also called $B[-\mu, \lambda](q)$ sets. A number of constructions of such sets are known, in particular for $\mu = 0$ and for $\mu = \lambda$.

Constructions for all μ and λ (Yari, Kløve, Bose 2013): Let $L = \mu + \lambda + 1$.

Construction

Let $a \geq 1$, $m \geq 1$, and $q = L^a m$.
For each $r \in [0, a-1]$, let κ_r be the largest integer less than or equal to λ that divides $L^r m$.
Let C be a $B[-\mu, \lambda](m)$ set. Then

$$B = \bigcup_{r=0}^{a-1} \left\{ L^{a-1-r}(Li+1) \middle| 0 \leq i \leq \frac{L^r}{\kappa_r} - 1 \right\} \cup \{L^a c \mid c \in C\}$$

is a $B[-\mu, \lambda](L^a m)$ set.

Construction

Let $p > \lambda$ be an odd prime and g a primitive root modulo p. If a is a divisor of $p-1$ and

$$|\{ind_g(\ell) \pmod{a} \mid \ell \in [-\mu, \lambda]^*\}| = \mu + \lambda,$$

then

$$\left\{ g^{ai} \pmod{p} \middle| 0 \le i \le \frac{p-1}{a} - 1 \right\}$$

is a $B[-\mu, \lambda](p)$ set.

Here, $\mathrm{ind}_g(\ell)$ is the index (or discrete logarithm),

$$g^{\mathrm{ind}_g(\ell)} = \ell \pmod{p}.$$

Construction

Let $\mu \equiv \lambda \pmod 2$. *Let* p *be a prime such that* $p \equiv 1 \pmod{L-1}$ *and let* g *be a primitive root modulo* p. *Let*

$$\theta = \gcd\{ind_g(\ell) \mid \ell \in [-\mu,\lambda]^*\}.$$

If $p \equiv 1 \pmod{\theta(L-1)}$ *and*

$$\left\{ \frac{ind_g(\ell)}{\theta} \pmod{L-1} \middle| \ell \in [-\mu,\lambda]^* \right\} = [0, L-2],$$

then

$$\left\{ g^{\theta(L-1)i+j} \pmod p \middle| i \in \left[0, \frac{p-1}{\theta(L-1)} - 1\right], j \in [0, \theta - 1] \right\}$$

is a perfect $B[-\mu,\lambda](p)$ *set.*

On the condition

p is a prime and

$$\left\{\frac{\mathrm{ind}_g(\ell)}{\theta} \pmod{\lambda+\mu} \,\middle|\, \ell \in [-\mu,\lambda]^*\right\} = [0, \lambda+\mu-1],$$

where

$$\theta = \gcd\{\mathrm{ind}_g(\ell) \mid \ell \in [-\mu,\lambda]^*\}.$$

If $\mu \equiv \lambda \pmod{2}$, we conjecture that there are infinitely many primes satisfying the condition.

For $\mu = 1$ and $\lambda = 3$, the smallest such prime is $p = 5$ and there are ten such primes ≤ 797.
For $\mu = 1$ and $\lambda = 5$, the smallest such prime is $p = 7$ and there are ten such primes ≤ 5407.
For $\mu = 1$ and $\lambda = 7$, the smallest such prime is $p = 475729$ and there are ten such primes ≤ 3127441.

On the condition

p is a prime and

$$\left\{ \frac{\mathrm{ind}_g(\ell)}{\theta} \pmod{\lambda+\mu} \,\middle|\, \ell \in [-\mu,\lambda]^* \right\} = [0,\lambda+\mu-1],$$

where

$$\theta = \gcd\{\mathrm{ind}_g(\ell) \mid \ell \in [-\mu,\lambda]^*\}.$$

If $\mu \equiv \lambda \pmod 2$, we conjecture that there are infinitely many primes satisfying the condition.

For $\mu = 2$ and $\lambda = 4$, the smallest such prime is $p = 7$ and there are ten such primes ≤ 1087.
For $\mu = 2$ and $\lambda = 6$, the smallest such prime is $p = 315361$ and there are ten such primes ≤ 1207441.
For $\mu = 2$ and $\lambda = 8$, the smallest such prime is $p = 11$ and there are ten such primes ≤ 183691.

Construction

Let B_1 *be a* $B[-\mu, \lambda](q_1)$ *set and* B_2 *be a* $B[-\mu, \lambda](q_2)$ *set.*
If $\gcd(\lambda!, q_2) = 1$, *then*

$$\{c + rq_1 \mid c \in B_1, r \in [0, q_2 - 1]\} \cup \{q_1 c \mid c \in B_2\}$$

is a $B[-\mu, \lambda](q_1 q_2)$ *set.*

Codes of length 2

We first consider linear codes.
In this case, a $B[-\mu, \lambda](q)$ set is a set $\{a, b\}$ such that all $(x \otimes a) \oplus (y \otimes b)$ where $x, y \in [-\mu, \lambda]^*$ are distinct.
We start by defining the codes and the problem precisely.
Let $(a, b) \in \mathbb{Z}_q^2$ where $a \neq b$. The corresponding code is

$$C = C_{a,b} = \{(u, v) \in \mathbb{Z}_q^2 \mid (u \otimes a) \oplus (v \otimes b) = 0\}.$$

When $(u, v) \in C_{a,b}$ is transmitted and (u', v') is received, the corresponding syndrom is $(u' \otimes a) \oplus (v' \otimes b)$.

Check pairs

Let $(u, v) \in C_{a,b}$. We see that if $(u', v') = (u \oplus e, v)$, the syndrom is

$$((u \oplus e) \otimes a) \oplus (v \otimes b) = (u \otimes a) \oplus (e \otimes a) \oplus (v \otimes b) = e \otimes a.$$

Similarly, if $(u', v') = (u, v \oplus e)$, the syndrom is $e \otimes b$. Therefore, the code is single error correcting if and only if the $1 + 2\lambda + 2\mu$ syndroms

$$\{0\} \cup \{e \otimes a \mid e \in [-\mu, -1] \cup [1, \lambda]\} \cup \{e \otimes b \mid e \in [-\mu, -1] \cup [1, \lambda]\}$$

are all distinct. If this is the case, we say that (a, b) is a (q, λ, μ) check pair or just a check pair if the values of q, λ and μ are clear from the context.

Problems considered

A problem can now be precisely formulated as follows:

> *For which q, λ and μ does a (q, λ, μ) check pair exist?*
>
> *For given λ and μ, let*
> *$q_L(\lambda, \mu)$ be the smallest q for which a (q, λ, μ) check pair exists,*
> *$q_M(\lambda, \mu)$ be minimal such that a (q, λ, μ) check pair exists for all $q \geq q_M$.*

A simpler problem is the following: determine (or give bounds on) $q_L(\lambda, \mu)$ and $q_M(\lambda, \mu)$.

Values of $q_L(\mu, \lambda)$

μ	$\lambda = 1$	2	3	4	5	6	7	8	9	10	11	12	13
0	3	5	7	9	11	13	15	17	19	21	23	25	27
1	5	8	14	16	22	24	30	32	38	40	46	48	54
2		10	15	21	30	33	39	48	51	57	66	69	75
3			17	24	34	40	52	56	68	72	84	88	100
4				26	35	45	55	65	80	85	95	105	115
5					37	48	62	75	88	96	114	120	138
6						50	63	77	91	105	119	133	154
7							65	80	98	112	132	144	166
8								82	99	117	138	153	171
9									101	120	142	160	184
10										122	143	165	187
11											145	168	194
12												170	195
13													197

$\mu = 0$

Theorem

$q_L(\lambda, 0) = q_M(\lambda, 0) = 2\lambda + 1.$

Proof:
If (a, b) is a $(q, \lambda, 0)$ check pair, then the 2λ syndroms

$$\{\{ai \mod q, bi \mod q \mid 1 \le i \le \lambda\}$$

are distinct and non-zero, and so $q \ge 2\lambda + 1$.

If $q \ge 2\lambda + 1$, then $(1, q-1)$ is a $(q, \lambda, 0)$ check pair;
the syndroms are

$$\{0, 1, \ldots, \lambda, q-\lambda, q-\lambda+1, \ldots, q-1\}$$

and $q - \lambda > \lambda$.

q_L in the general case

In Kløve, Luo, Yari (2012) it was shown that

Theorem

For all $\lambda \geq 1$ *we have* $q_L(\lambda, \lambda) = (\lambda + 1)^2 + 1$.

Conjecture

i) For all λ *and* μ *we have*

$$(\lambda + 1)^2 - (\lambda - \mu)^2 \leq q_L(\lambda, \mu) \leq (\lambda + 1)^2 - (\lambda - \mu)^2 + \mu + 1.$$

ii) We have $q_L(\lambda, \mu) = (\lambda + 1)^2 - (\lambda - \mu)^2$
for $\lambda = \mu + 1$ *and for* $\lambda = 2\mu$ *(and many others).*
iii) For $\lambda = 2\mu + 1$, *we have* $q_L(\lambda, \mu) = (\lambda + 1)^2 - (\lambda - \mu)^2 + \mu + 1$.

q_M in the general case

We observe that $q_M(\lambda, \mu) \leq q_M(\lambda, \mu + 1)$.
In particular $q_M(\lambda, \mu) \leq q_M(\lambda, \lambda)$.

We now consider $q_M(\lambda, \lambda)$. We observe that

$$q_M(\lambda, \lambda) \geq q_L(\lambda, \lambda) = (\lambda + 1)^2 + 1.$$

This presentation is based on Kløve (2015).
We split the presentation into two cases:

Case I, $q \geq (\lambda + 1)^2 + 1$, $q \neq (\lambda + 1)(\lambda + 2)$. For this case we show that there exists a simple check pair.
Case II, $q = (\lambda + 1)(\lambda + 2)$. This is the hardest case. A check pair exists for some λ, but not all.

The case $q \geq (\lambda+1)^2+1$, $q \neq (\lambda+1)(\lambda+2)$

We will give explicit check pairs for all q in this case.
First, consider the pair $(1, \lambda+1)$. The corresponding syndrom set is

$$[0,\lambda] \cup [q-\lambda, q-1] \cup \{x(\lambda+1) \mid x \in [1,\lambda]\} \cup \{q-x(\lambda+1) \mid x \in [1,\lambda]\}.$$

If $q-\lambda(\lambda+1) > \lambda(\lambda+1)$, that is, $q \geq 2\lambda(\lambda+1)+1$, then clearly all the syndroms are distinct and so $(1,\lambda+1)$ is a check pair.
Similarly, if $q \in [(\lambda+1)^2+1, 2\lambda(\lambda+1)-1]$ but $q \not\equiv 0 \pmod{\lambda+1}$, then again all the syndroms are distinct.
It remains to consider $q \in \{x(\lambda+1) \mid x \in [\lambda+3, 2\lambda]\}$. For these q, $q \not\equiv 0 \bmod (\lambda+2)$. By an argument similar to the one above, we see that that $(1,\lambda+2)$ is a check pair.

The case $q \geq (\lambda+1)^2+1$, $q \neq (\lambda+1)(\lambda+2)$, summary

We summarize these results in a theorem.

Theorem

Let $q \geq (\lambda+1)^2+1$, $q \neq (\lambda+1)(\lambda+2)$*.*

- *If* $q \geq 2\lambda(\lambda+1)+1$*, then* $(1, \lambda+1)$ *is a check pair.*
- *If* $q \in [(\lambda+1)^2+1, 2\lambda(\lambda+1)-1]$ *but* $q \not\equiv 0 \pmod{\lambda+1}$*, then* $(1, \lambda+1)$ *is a check pair.*
- *If* $q \in \{x(\lambda+1) \mid x \in [\lambda+3, 2\lambda]\}$*, then* $(1, \lambda+2)$ *is a check pair.*

Corollary

$q_M(\lambda,\lambda) = (\lambda+1)^2+1$ *or* $q_M(\lambda,\lambda) = (\lambda+1)(\lambda+2)+1$*.*

$q = (\lambda+1)(\lambda+2)$, $\lambda+1$ not a prime power

Theorem

If $\lambda + 1 = \sigma\rho$ *where* $1 < \sigma < \rho$, *and* $\gcd(\sigma, \rho) = 1$, *then* $(\sigma, \rho(\lambda + 2 - \sigma))$ *is a check pair.*

The corresponding code is

$$\begin{aligned} C &= \{(u, v) \mid u, v \in [0, q-1], \sigma u \oplus \rho(\lambda+2-\sigma)v = 0\} \\ &= \{(\rho U, \sigma V) \mid U \in [0, \sigma(\lambda+2)-1], V \in [0, \rho(\lambda+2)-1], \\ &\qquad U - \sigma V \equiv 0 \pmod{\lambda+2}\}. \end{aligned}$$

Some numerical results and a conjecture

For $2 \leq \lambda \leq 100$ and $q = (\lambda+1)(\lambda+2)$, a complete search has shown that there are no check pairs when $\lambda + 1$ a prime power.

Possibly this is the case for all λ and we formulate this conjecture:

Conjecture

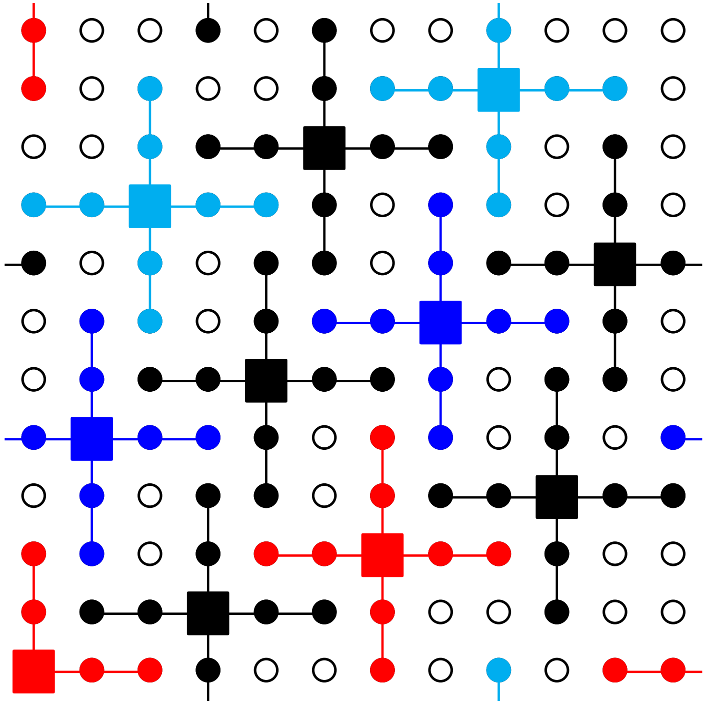
- *If $\lambda + 1$ is a prime power, then $q_M(\lambda, \lambda) = (\lambda+1)(\lambda+2) + 1$.*
- *If $\lambda + 1$ is not a prime power, then $q_M(\lambda, \lambda) = (\lambda+1)^2 + 1$.*

Nonlinear codes?

When $\lambda + 1 > 2$ is a prime power and $q = (\lambda + 1)(\lambda + 2)$, is there a code $C \in \mathbb{Z}_q^2$ of size q and correcting any single error of size at most λ?
We conjectured above that no **linear** such code exists.

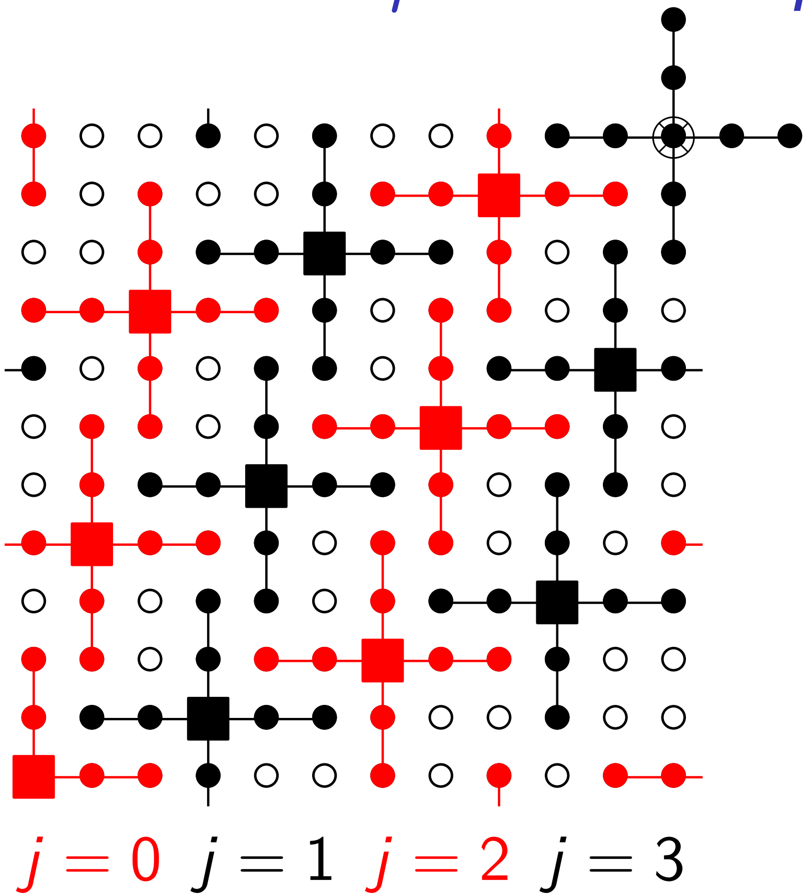
How about a non-linear code?
A non-linear code corresponds to a set of disjoint crosses with arms of length λ.

A code for $\lambda = \mu = 2$ and $q = 12$



This code has size 11 (a linear code would have size 12).

A code for $\lambda = \mu = 2$ and $q = 12$, more



The structure of the code is

$$\{(i + 3j, 4i + j) \mid i = [0, 2], j = [0, 3]\} \setminus \{(11, 11)\}$$

Similar codes for any $\lambda = \mu$ and $q = (\lambda+1)(\lambda+2)$

$$\{(i+(\lambda+1)j, (\lambda+2)i+j) \mid i=[0,\lambda], j=[0,\lambda+1]\} \setminus \{(q-1,q-1)\}$$

,

Note: we get $(q-1, q-1)$ for $i = \lambda+1$ and $j = \lambda$.

This code has $q-1$ codewords.

Is there a code with q codewords?

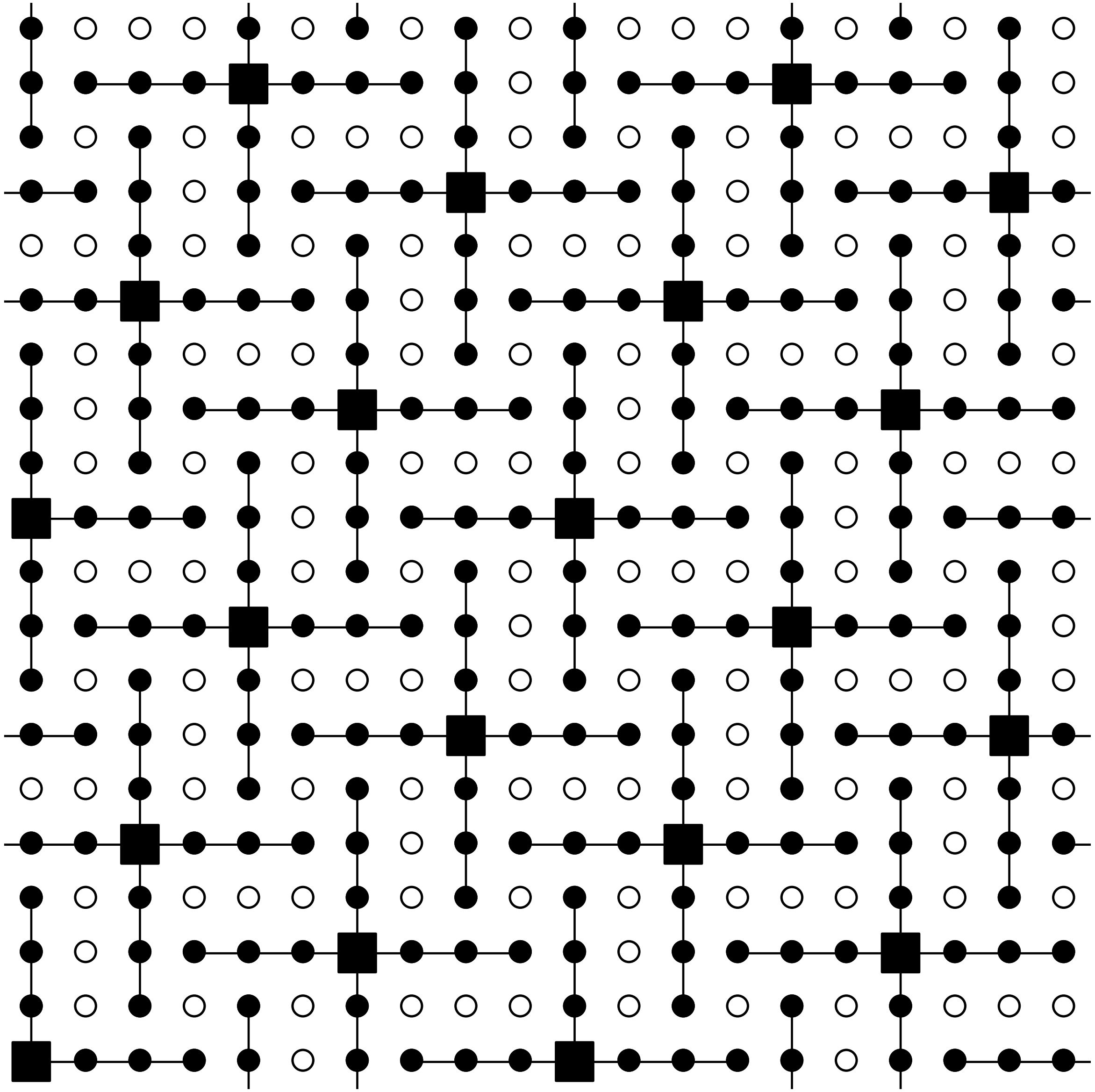
A code for $\lambda = \mu = 3$ and $q = 20$

The general construction above gives a code with 19 codewords.

However, there is a code with 20 codewords (Battaglioni, Chiaraluce, Kløve 2017):

$$\{(2i, 4i \bmod 20) \mid i \in [0,9]\} \cup \{(2i, (4i+10) \bmod 20) \mid i \in [0,9]\}.$$

A code of size 20 for $\lambda = \mu = 3$ and $q = 20$



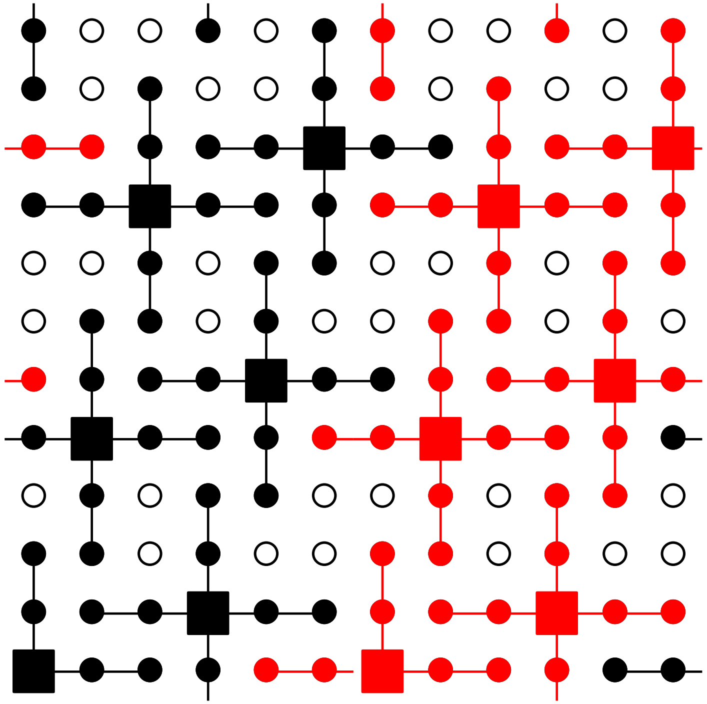
Similar codes for larger odd λ?

If $\lambda = 2m - 1$, the distance between closest codewords in the same row is $5m$. We have $q = (\lambda + 1)(\lambda + 2) = 2m(2m + 1)$.
We get a code if $5m | 2m(2m + 1)$, that is $m \equiv 2 \bmod 5$, that is $\lambda \equiv 3 \bmod 10$.

Since $\lambda + 1 \equiv 4 \bmod 10$, $\lambda + 1$ is even.
Hence, $\lambda + 1$ is a power of a prime if and only if $\lambda + 1$ is a power of 2.
We see that for $\lambda = 2^{4\alpha+2} - 1$, we get get a code of size $(\lambda + 1)(\lambda + 2)$.

A code of size 12 for $\lambda = \mu = 2$ and $q = 12$

(Battaglioni, Chiaraluce, Kløve 2017):



The structure of the code is

$$\{(6i + 3j + k, j + 4k) \mid i \in [0, 1], j \in [0, 1], k \in [0, 2]\}$$

Maximal packings

General question: Given λ, μ and q, let $\Omega(\lambda, \mu, q)$ be the maximal size of a (λ, μ)-packing (error correcting code) of $\mathbb{Z}_q^2$, linear or non-linear.

What can we say about $\Omega(\lambda, \mu, q)$?

Open questions for $q = (\lambda + 1)(\lambda + 2)$

We showed above that

$$\Omega(\lambda, \lambda, (\lambda + 1)(\lambda + 2)) \geq (\lambda + 1)(\lambda + 2) - 1$$

for all λ,
and that

$$\Omega(\lambda, \lambda, (\lambda + 1)(\lambda + 2)) \geq (\lambda + 1)(\lambda + 2)$$

sometimes.

For which λ is $\Omega(\lambda, \lambda, (\lambda + 1)(\lambda + 2)) \geq (\lambda + 1)(\lambda + 2)$?

Is $\Omega(\lambda, \lambda, (\lambda + 1)(\lambda + 2)) > (\lambda + 1)(\lambda + 2)$ for any λ?

Known cases for $q = (\lambda + 1)(\lambda + 2)$

We have shown that

$$\Omega(\lambda, \lambda, (\lambda + 1)(\lambda + 2)) \geq (\lambda + 1)(\lambda + 2)$$

for

- $\lambda = 1, 2, 3, 4.$
- λ odd, except possibly $\lambda = 2^\beta - 1$ where $\beta \not\equiv 2 \bmod 4$.

NEW RESULT 5. SEPTEMBER 2017

Let $q = (\lambda + 1)(\lambda + 2)$ where $\lambda = 2\nu$ is even.

Let C be defined by

$$\begin{aligned} C = &\{(2i(\lambda+1)+j, j(\lambda+2) \mid 0 \le i \le \nu, 0 \le j \le \lambda\} \\ &\cup \{(2i+1)(\lambda+1)i + j, j(\lambda+2)+1 \mid 0 \le i \le \nu, 0 \le j \le \lambda\}. \end{aligned}$$

Then C is a (λ, λ)-packing of Z_q^2 of size $(\lambda+1)(\lambda+2)$.

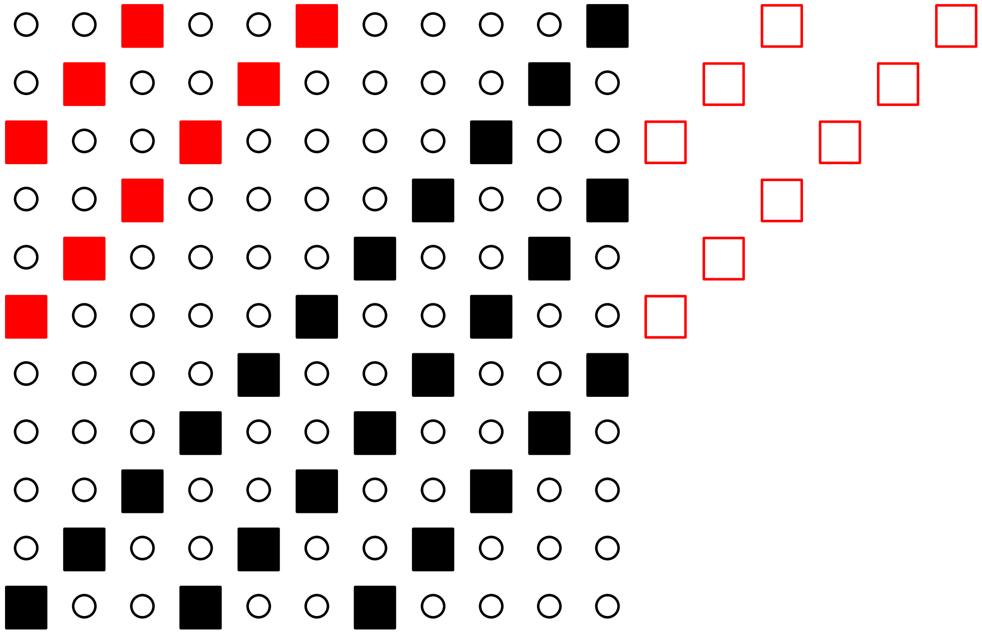
Remaining open case:
$\lambda = 2^\beta - 1$ where $\beta \not\equiv 2 \bmod 4$

Codes for $\mu = 0$, $\lambda \geq 1$ and $q > \lambda$

A solution is

$$\{((2\lambda+1)j+i, i) \mid i \in [0, q-1], j \in [0, \lfloor (q/(2\lambda+1) \rfloor - 1]\}.$$

Example, $q = 11$, $\lambda = 1$. Size of solution is $3 \cdot 11 = 33$.



Codes for $\mu = 0$, $\lambda \geq 1$, more

(Battaglioni, Chiaraluce, Kløve 2017):
Assume that $\lambda \geq 1$ and $q = r(2\lambda + 1) - \eta$, where $r \geq 1$ and $1 \leq \eta \leq \lambda$.
For $0 \leq j \leq r - 1$ let

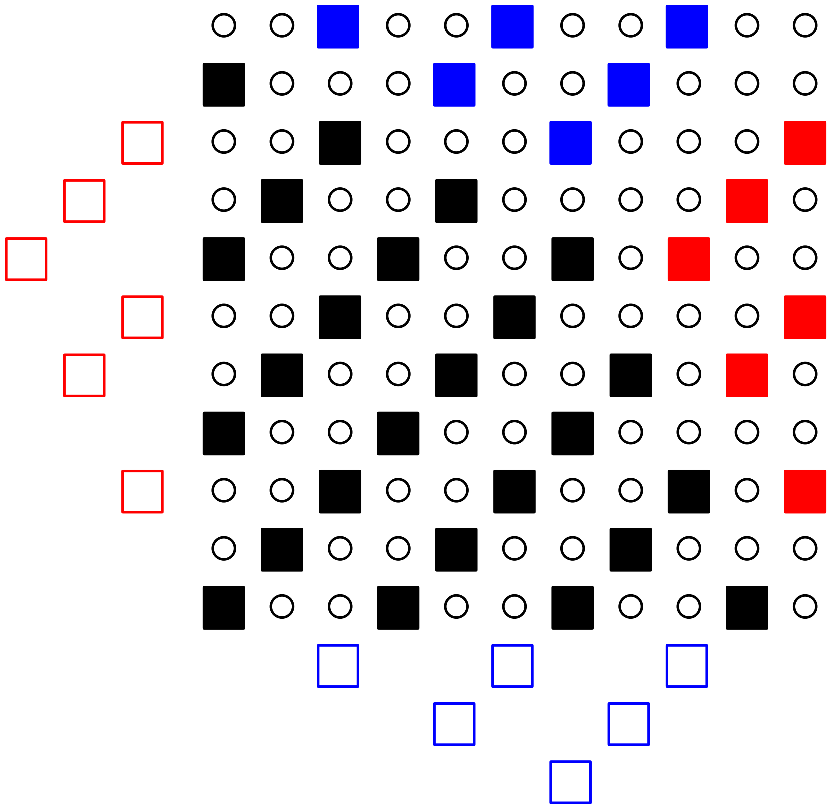
$$T_j = \{(i, i + j\pi) \mid i \in [-j\lambda, r(\lambda + 1) - 1 - \eta - j(\lambda + 1)]\}$$
$$T_{-j} = \{(y, x) \mid (x, y) \in T_j\}.$$

Then

$$\bigcup_{j=-(r-1)}^{r-1} T_j$$

are a set of centers of a packing of Z_q^2.

Example for $q = 11$, $\lambda = 1$. Size is 37.



A best (λ, λ)-packing of $\mathbb{Z}^2$

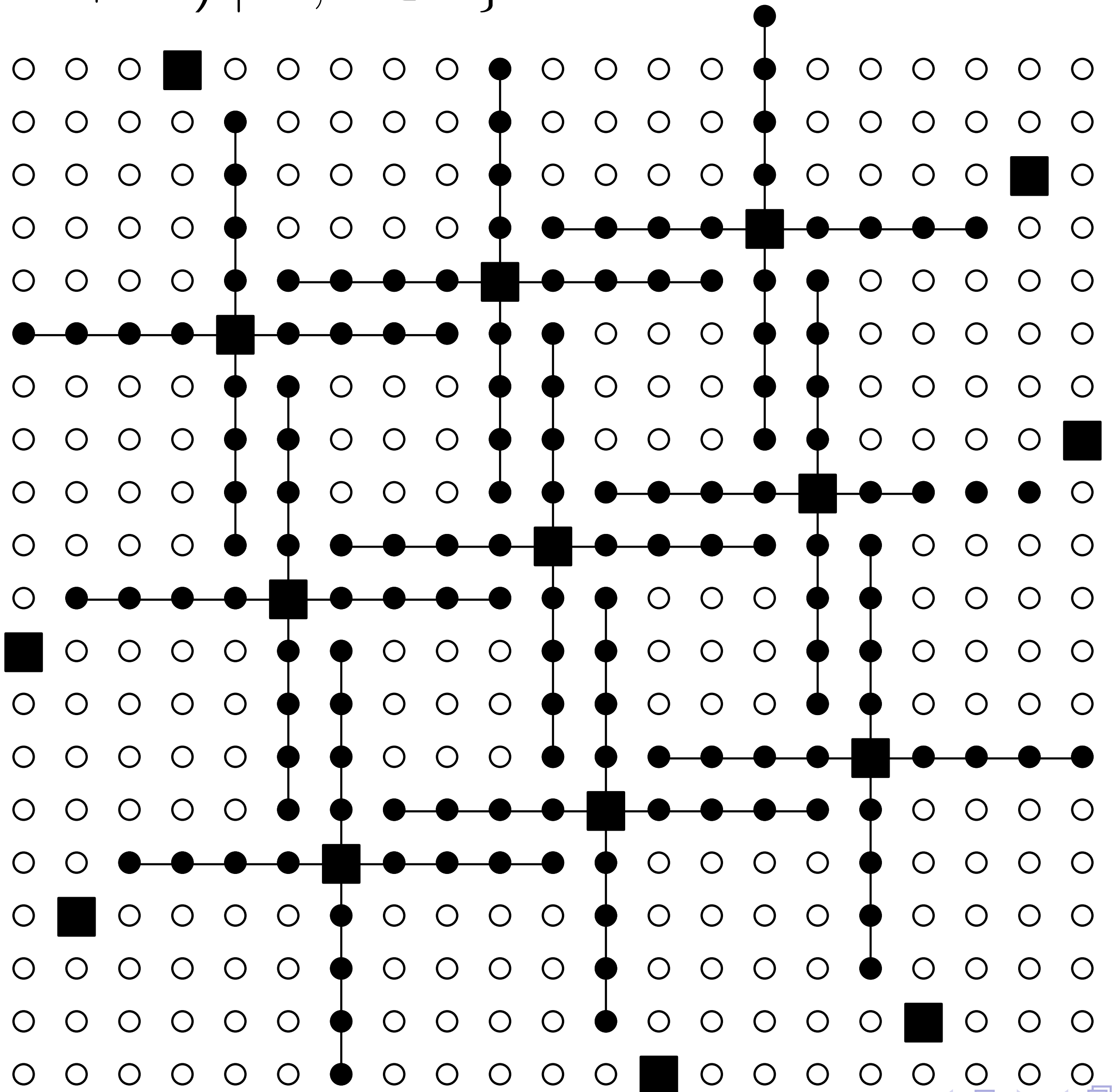
$\{((\lambda+1)m - n, m + (\lambda+1)n) \mid m, n \in \mathbb{Z}\}$ is known to be a (λ, λ)-packing of $\mathbb{Z}^2$ of maximal density (Everett and Hickerson 1979).

Its density is

$$\frac{1}{\lambda^2 + 2\lambda + 2}.$$

A best $(4,4)$-packing of $\mathbb{Z}^2$

$\{(5m - n, m + 5n) \mid m, n \in \mathbb{Z}\}$



For $q = (\lambda+1)(\lambda+2) = \lambda^2 + 3\lambda + 2$ this implies for a (λ, λ)- packing of size $\Omega(\lambda, \lambda, q)$ that

$$\frac{\Omega(\lambda, \lambda, q)}{(\lambda^2 + 3\lambda + 2)^2} \leq \frac{1}{\lambda^2 + 2\lambda + 2}$$

and so

$$\begin{aligned}\Omega(\lambda, \lambda, q) \leq \frac{(\lambda^2 + 3\lambda + 2)^2}{\lambda^2 + 2\lambda + 2} &= \frac{(\lambda^2 + 2\lambda + 2 + \lambda)^2}{\lambda^2 + 2\lambda + 2} \\ &= \lambda^2 + 2\lambda + 2 + 2\lambda + \frac{\lambda^2}{\lambda^2 + 2\lambda + 2}.\end{aligned}$$

Hence

$$\Omega(\lambda, \lambda, q) \leq \lambda^2 + 4\lambda + 2 + 2\lambda = q + \lambda.$$

A best (λ, μ)-packing of $\mathbb{Z}^2$ for $\mu < \lambda$

Let $0 \leq \mu < \lambda$.
Then (Cruz, d'Azevedo Breda, Pinto 2015)

$$\{(u(\lambda+1) - v(\lambda-\mu), v(\lambda+1) - u(\lambda-\mu)) \mid u, v \in \mathbb{Z}\}$$

is a (λ, μ)-packing of $\mathbb{Z}^2$ of maximal density.
Its density is

$$\frac{1}{(\lambda+1)^2 - (\lambda-\mu)^2}.$$

Packing of $\mathbb{Z}^2$

Let C be a (λ, μ)-packing of $\mathbb{Z}_q^2$ of maximal size $\Omega(\lambda, \mu, q)$.
Let

$$C^* = \{(a + rq, b + sq) \mid (a, b) \in C, r, s \in \mathbb{Z}\}.$$

Then C^* is a (λ, μ)-packing of $\mathbb{Z}^2$ with density $\Omega(\lambda, \mu, q)/q^2$.

Corollary

If $\mu < \lambda$, then

$$\Omega(\lambda, \mu, q) \leq \frac{q^2}{(\lambda + 1)^2 - (\lambda - \mu)^2}.$$

$$\Omega(\lambda, \lambda, q) \leq \frac{q^2}{\lambda^2 + 2\lambda + 2}.$$

$$* + * + * + * + * + * + * + * + * + * + * + *$$

On the linear codes for the case $q \neq (\lambda+1)(\lambda+2)$

We take a closer look at the codes corresponding to the second case ($q \in [(\lambda+1)^2+1, 2k(\lambda+1)-1]$ but $q \not\equiv 0 \pmod{\lambda+1}$). The code is

$$C_{1,\lambda+1} = \{((-(\lambda+1)) \otimes v, v) \mid v \in \mathbb{Z}_q\}.$$

The most natural encoding is:
encode the information $m \in \mathbb{Z}_q$ into $((-(\lambda+1)) \otimes m, m))$.
This gives a systematic code.

Possible syndroms

For decoding, we assume that (u', v') is received and that at most one of the elements are in error, and by an amount at most λ. From this we want to recover the sent information. We look at the possible syndroms.

- If there are no errors, the syndrom is 0.
- If $u' = u \oplus e$ where $e \in [1, \lambda]$, then the syndrom is $s = e$. In this case $m = v'$.
- If $u' = u \oplus e$ where $e \in [-\lambda, -1]$, then the syndrom is $s = q + e$. Also in this case $m = v'$.
- If $v' = v \oplus e$ where $e \in [1, \lambda]$, then the syndrom is $s = (\lambda + 1)e$. In this case $m = v' \oplus (-s/(\lambda + 1))$.
- If $v' = v \oplus e$ where $e \in [-\lambda, -1]$, then the syndrom is $s = q + (\lambda + 1)e$. In this case $m = v' \oplus ((s - q)/(\lambda + 1))$.

Decoding algorithm

This gives the following decoding algorithm:

- if $s \in [0, \lambda]$ or $s \in [q - \lambda, q - 1]$, $m = v'$,
- else if $(s \mod (\lambda + 1)) = 0$, then $m = v' \oplus (-s/(\lambda + 1))$,
- else if $((q - s) \mod (\lambda + 1)) = 0$, then $m = v' \oplus ((s - q)/(\lambda + 1))$.

This gives a correct answer for all errors of the type we consider.

On the linear codes for $q = (\lambda+1)(\lambda+2)$, $\lambda+1$ not a prime power

Theorem

If $\lambda + 1 = \sigma\rho$ where $1 < \sigma < \rho$, and $\gcd(\sigma, \rho) = 1$, then $(\sigma, \rho(\lambda + 2 - \sigma))$ is a check pair.

The corresponding code is

$$\begin{aligned} C &= \{(u,v) \mid u,v \in [0,q-1], \sigma u \oplus \rho(\lambda+2-\sigma)v = 0\} \\ &= \{(\rho U, \sigma V) \mid U \in [0, \sigma(\lambda+2)-1], V \in [0, \rho(\lambda+2)-1], \\ &\qquad U - \sigma V \equiv 0 \pmod{\lambda+2}\}. \end{aligned}$$

Example, $\lambda = 5$, $\sigma = 2$, $\rho = 3$, $q = 42$

$$C = \{(3U, 2V) \mid U \in [0, 13], V \in [0, 20], U - 2V \equiv 0 \pmod{7}\}.$$

U	V	$(3U, 2V)$	
$0, 7$	$0, 7, 14$	$(0, 14), (0, 28), (0, 0),$	$(21, 14), (21, 28), (21, 0)$
$1, 8$	$4, 11, 18$	$(3, 8), (3, 22), (3, 36),$	$(24, 8), (24, 22), (24, 36)$
$2, 9$	$1, 8, 15$	$(6, 2), (6, 16), (6, 30),$	$(27, 2), (27, 16), (27, 30)$
$3, 10$	$5, 12, 19$	$(9, 10), (9, 24), (9, 38),$	$(30, 10), (30, 24), (30, 38)$
$4, 11$	$2, 11, 18$	$(12, 4), (12, 22), (12, 36),$	$(33, 4), (33, 22), (33, 36)$
$5, 12$	$6, 13, 20$	$(15, 12), (15, 26), (15, 40),$	$(36, 12), (36, 26), (36, 40)$
$6, 13$	$3, 10, 17$	$(18, 6), (18, 20), (18, 34),$	$(39, 6), (39, 20), (39, 34)$

Note that $|C| = 42 = q$. Also in general, $|C| = q$.

Encoding

The encoding can be done as follows: any integer $m \in [0, q-1]$ can be represented as

$$m = \sigma\mu + \nu \text{ where } \nu \in [0, \sigma - 1].$$

We encode m into $(u, v) = (\rho(-\mu + \nu(\lambda + 2)) \mod q, \sigma\mu)$. The information can easily be recovered from (u, v). Let

$$V = v/\sigma \text{ and } U = (u/\rho + V)/(\lambda + 2) \mod \sigma.$$

Then $m = v + U$.

Syndroms

We next consider the correction of errors for a codeword $(\rho U, \sigma V)$.

- If $u' = u + e$ where $e \in [0, \lambda]$, then the syndrom is $s = \sigma e$ and so $e = s/\rho$.
- If $u' = u + e$ where $e \in [-\lambda, -1]$, then $s = q + \sigma e$ and so $e = (s - q)/\rho$.
- If $v' = v + e$, where $e \in [-\lambda, -1] \cup [1, \lambda]$, then $s \equiv \rho(\lambda + 2 - \sigma)e \pmod{\rho\sigma(\lambda+2)}$ and so $s/\rho \equiv (\lambda+2-\sigma)e \pmod{\sigma(\lambda+2)}$. We see that $\gcd(\lambda + 2 - \sigma, \sigma(\lambda + 2)) = 1$. Hence

$$e \equiv f = (\lambda + 2 - \sigma)^{-1} \mod (\sigma(\lambda + 2)),$$

where the inverse is modulo $\sigma(\lambda + 2)$. If $f \leq k$, then $e = f$. If $f \geq \sigma(\lambda + 2) - \lambda$, then $e = \sigma(\lambda + 2) - f$.

.

Decoding algorithm

From this, we get the following decoding algorithm.

- If $s \equiv 0 \pmod{\sigma}$ and $s/\sigma \in [0, \lambda]$, then decode into $(u \ominus (s/\sigma), v)$,
- else if $s \equiv 0 \pmod{\sigma}$ and $s/\sigma \in [\rho(\lambda+2) - \lambda, \rho(\lambda+2) - 1]$, then decode into $(u \ominus ((s-q)/\sigma), v)$,
- else if $s \equiv 0 \pmod{\rho}$, let

$$f = ((\lambda + 2 - \sigma)^{-1} \frac{s}{\rho} \mod \sigma(\lambda + 2)),$$

  - if $f \leq \lambda$, then decode into $(u, v \ominus f)$,
  - else decode into $(u, (v \ominus (f - \sigma(\lambda+2)) \mod q))$.

.

References

- R. Ahlswede, H. Aydinian, L. H. Khachatrian, L. M. G. M. Tolhuizen, “On q-ary codes correcting all unidirectional errors of a limited magnitude”, Proc. of Ninth Internat. Workshop on Algebraic and Comb. Coding Theory, Kranevo, Bulgaria, pp. 20-26, Jun. 2004.
- M. Battaglioni, F. Chiaraluce, T. Kløve, ”On non-linear codes correcting errors of limited size”, Proc. Globecom 2017, to appear.
- C. N. Cruz, A. d’Avezedo Breda, R. Pinto, “Packing of R by crosses,” Mathematica Slovaca, vol. 65, no. 5, pp. 935–956, Oct. 2015.
- H. Everett and D. Hickerson, “Packing and covering by translates of certain nonconvex bodies,” Proceedings of the American Mathematical Society, vol. 75, no. 1, pp. 87–91, Jun. 1979.
- T. Kløve, “Codes of length 2 correcting single errors of limited size,” in Groth J. (eds) Cryptography and Coding. Lecture Notes in Computer Science, vol. 9496. Springer, 2015, pp. 190–201.

References, cont.

- T. Kløve, J. Luo, and S. Yari, “Codes correcting single errors of limited magnitude,” IEEE Trans. Inf. Theory, vol. 58, no. 4, pp. 2206–2219, Apr. 2012.
- M. Schwartz, “Quasi-cross lattice tilings with applications to flash memory,” IEEE Trans. Inf. Theory, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.
- S. Stein, "Packing of R^n by certain error spheres", IEEE Trans. Inf. Theory, vol. 30, no. 2, pp. 356-363, Feb. 1984.
- R. Varshamov and G. Tenenholtz, “A code for correcting a single asymmetric error,” Automatica i Telemekhanika, vol. 26, no. 2, pp. 288–292, 1965.
- S. Yari, T. Kløve, and B. Bose, “Some codes correcting unbalanced errors of limited magnitude for flash memories,” IEEE Trans. Inf. Theory, vol. 59, no. 11, pp. 7278–7287, Nov. 2013.

Thank you for your attention.