Squares of cyclic codes

Ignacio Cascudo (Aalborg University)

13th Nordic Combinatorial Conference - NORCOM 2019
6th August 2019

Linear codes

A linear error-correcting code C of length n over a finite field $\mathbb{F}_q$ is a $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$.

Linear codes

A linear error-correcting code C of length n over a finite field $\mathbb{F}_q$ is a $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$.

- Dimension of C ($\dim C$): its dimension as $\mathbb{F}_q$-vector space.
- $[n, k]$-code: a linear code with length n and dimension k.
- Rate of C: k/n.

Linear codes

A linear error-correcting code C of length n over a finite field $\mathbb{F}_q$ is a $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$.

- Dimension of C ($\dim C$): its dimension as $\mathbb{F}_q$-vector space.
- $[n, k]$-code: a linear code with length n and dimension k.
- Rate of C: k/n.

- Minimum distance of C, $d(C)$, is

$$min\{w_H(\mathbf{c}) : \mathbf{c} \in C \setminus \{0\}\}$$

where $w_H(\mathbf{c})$ denotes the Hamming weight of $\mathbf{c}$ (number of nonzero coordinates of $\mathbf{c}$).

Squares of linear codes

The square (wrt the componentwise product) of a linear code C is

$$C^{*2} = < \{\mathbf{c} * \mathbf{d} : \mathbf{c}, \mathbf{d} \in C\} >$$

Squares of linear codes

The square (wrt the componentwise product) of a linear code C is

$$C^{*2} =< \{\mathbf{c} * \mathbf{d} : \mathbf{c}, \mathbf{d} \in C\} >$$

where:

- $<>$ denotes the linear span over the finite field
- $\mathbf{c} * \mathbf{d}$ is the component-wise product of $\mathbf{c}$ and $\mathbf{d}$.
  If $\mathbf{c} = (c_1, c_2, \ldots, c_n)$, $\mathbf{d} = (d_1, d_2, \ldots, d_n)$, then
  $\mathbf{c} * \mathbf{d} = (c_1 \cdot d_1, c_2 \cdot d_2, \ldots, c_n \cdot d_n)$.

The main problem

$$C^{*2} = < \{\mathbf{c} * \mathbf{d} : \mathbf{c}, \mathbf{d} \in C\} >$$

Construct $[n, k]$-linear codes C with:

- k/n large.
- $d(C^{*2})$ large.

The main problem

$$C^{*2} = < \{\mathbf{c} * \mathbf{d} : \mathbf{c}, \mathbf{d} \in C\} >$$

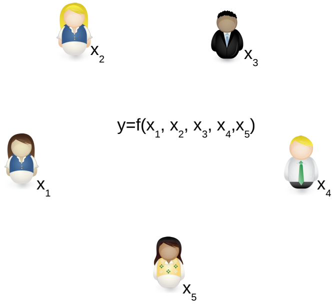
Construct $[n, k]$-linear codes C with:

- k/n large.
- $d(C^{*2})$ large.

Note that $d(C) \geq d(C^{*2})$

Motivation

Secure multiparty computation



Some known results - Asymptotics

- Randriambololona 12: Over every field there exist families of linear codes $\{C_n\}$ with:
  - Length $n \to \infty$,
  - $k/n \to C > 0$,
  - $d(C^{*2})/n \to D > 0$.

  These are algebraic-geometric constructions.

Some known results - Asymptotics

- Randriambololona 12: Over every field there exist families of linear codes $\{C_n\}$ with:
  - Length $n \to \infty$,
  - $k/n \to C > 0$,
  - $d(C^{*2})/n \to D > 0$.

  These are algebraic-geometric constructions.
- C., Cramer, Mirandola, Zemor 14:
  Random codes do not achieve this with large probability.
  No "Gilbert-Varshamov bound for squares".

Some known results - Singleton-like bound and MDS-like codes

- Randriambololona 13: Singleton-like bound.

$$d(C^{*2}) + 2k \leq n + 2$$

- Mirandola-Zemor 15: "Square-MDS" codes must essentially be Reed-Solomon.

However, RS require $q \geq n$... What about $q < n$?, e.g. $q = 2$.

Some known results - Singleton-like bound and MDS-like codes

- Randriambololona 13: Singleton-like bound.

$$d(C^{*2}) + 2k \leq n + 2$$

- Mirandola-Zemor 15: "Square-MDS" codes must essentially be Reed-Solomon.

However, RS require $q \geq n$... What about $q < n$?, e.g. $q = 2$.

Rest of this talk, based on results from:
Cas19: *On Squares of Cyclic Codes*, IEEE Transactions of Information Theory, 2019.

Cyclic codes

- Let $\mathbb{F}_q$ field of q elements, n coprime to q.
- Identify vectors

$$(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$$

with elements

$$c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \in \mathbb{F}_q[X] \,/ < X^n - 1 > .$$

- Then, a cyclic code is an ideal of $\mathbb{F}_q[X] \,/ < X^n - 1 >$.
- Note that $(c_0, c_1, \ldots, c_{n-1}) \in C$ iff $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.

Cyclic codes - generator polynomial

- Every ideal in $\mathbb{F}_q[X] \;/ < X^n - 1 >$ is generated by a polynomial g which divides $X^n - 1$ (generator polynomial).
- Let α be an n-th primitive root of unity in $\overline{\mathbb{F}_q}$.

Cyclic codes - generator polynomial

- Every ideal in $\mathbb{F}_q[X] \; / < X^n - 1 >$ is generated by a polynomial g which divides $X^n - 1$ (generator polynomial).
- Let α be an n-th primitive root of unity in $\overline{\mathbb{F}_q}$.
- Then g is of the form

$$g = \frac{X^n - 1}{\prod_{i \in I}(X - \alpha^i)}$$

where $I \subseteq \mathbb{Z}/n\mathbb{Z}$ is such that

$$x \in I \Rightarrow q \cdot x \in I$$

i.e. I is a union of q-cyclotomic cosets (we will call it q-cyclotomic)

Dimension and minimum distance

The cyclic code C generated by

$$g = \frac{X^n - 1}{\prod_{i \in I}(X - \alpha^i)}$$

satisfies

- $\dim C = |I|$.
- If $I \subseteq \{c, c+1, \ldots, c+b-1\}$ for some c and b, then $d(C) \geq n - b + 1$.

Dimension and minimum distance

The cyclic code C generated by

$$g = \frac{X^n - 1}{\prod_{i \in I}(X - \alpha^i)}$$

satisfies

- $\dim C = |I|$.
- If $I \subseteq \{c, c+1, \ldots, c+b-1\}$ for some c and b, then $d(C) \geq n - b + 1$.

So...

- If $|I|$ is "large", then $\dim C$ is "large".
- If I is contained in a "small" interval, then $d(C)$ is "large".

Squares of cyclic codes - main result

If C is a cyclic code generated by

$$g = \frac{X^n - 1}{\prod_{i \in I}(X - \alpha^i)}$$

then C^{*2} is a cyclic code generated by

$$g = \frac{X^n - 1}{\prod_{\ell \in I+I}(X - \alpha^\ell)}$$

where $I + I = \{i_1 + i_2 : i_1, i_2 \in I\} \subseteq \mathbb{Z}/n\mathbb{Z}$.

Squares of cyclic codes - main result

If C is a cyclic code generated by

$$g = \frac{X^n - 1}{\prod_{i \in I}(X - \alpha^i)}$$

then C^{*2} is a cyclic code generated by

$$g = \frac{X^n - 1}{\prod_{\ell \in I+I}(X - \alpha^\ell)}$$

where $I + I = \{i_1 + i_2 : i_1, i_2 \in I\} \subseteq \mathbb{Z}/n\mathbb{Z}$.

Therefore:
If $I + I \subseteq \{c, c+1, \dots, c+b-1\}$, then $d(C^{*2}) \geq n - b + 1$.

Reformulation of the problem

Therefore we want to find $I \subseteq \mathbb{Z}/n\mathbb{Z}$ such that:

- I is q-cyclotomic (necessary for defining code).
- I "large" (necessary for $\dim C$ large).
- $I + I$ contained in "small" interval $\{c, c+1, \ldots, c+b-1\}$ (to ensure $d(C^{*2})$ large).

Reformulation of the problem

Therefore we want to find $I \subseteq \mathbb{Z}/n\mathbb{Z}$ such that:

- I is q-cyclotomic (necessary for defining code).
- I "large" (necessary for dim C large).
- $I + I$ contained in "small" interval $\{c, c+1, \ldots, c+b-1\}$ (to ensure $d(C^{*2})$ large).

I will now restrict to:

- $n = q^k - 1$. Then every q-cyclotomic coset $\{x, qx, q^2x, ...\}$ contains at most k elements (very helpful).
- $q = 2$ (many results carry to other q with minor modifications).

Finding a good I

Remember we want I to be 2-cyclotomic and relatively large, but $I + I$ to be relatively small.

Idea 1: Pick largest 2-cyclotomic $I \subseteq \{0, 1, ..., t\}$ for some t. Then $I + I \subseteq \{0, ..., 2t\}$, so $d(C^{*2}) \geq n - 2t$.

Finding a good I

Remember we want I to be 2-cyclotomic and relatively large, but $I + I$ to be relatively small.

Idea 1: Pick largest 2-cyclotomic $I \subseteq \{0, 1, ..., t\}$ for some t.
Then $I + I \subseteq \{0, ..., 2t\}$, so $d(C^{*2}) \geq n - 2t$.

Problem:
Either
$t < 2^{k-1}$, and then $I = \{0\}$, so $\dim C = 1$.
Or
$t \geq 2^{k-1}$, and then $n - 2t < 0$ and the bound for $d(C^{*2})$ is trivial.

Finding a good I

Remember we want I to be 2-cyclotomic and relatively large, but $I + I$ to be relatively small.

Idea 1: Pick largest 2-cyclotomic $I \subseteq \{0, 1, ..., t\}$ for some t.
Then $I + I \subseteq \{0, ..., 2t\}$, so $d(C^{*2}) \geq n - 2t$.

Problem:
Either
$t < 2^{k-1}$, and then $I = \{0\}$, so $\dim C = 1$.
Or
$t \geq 2^{k-1}$, and then $n - 2t < 0$ and the bound for $d(C^{*2})$ is trivial.

Disclaimer: The bound $d(C^{*2}) \geq n - 2t$ is not tight.

Finding a good I

Idea 2 (indices of small Hamming weight):
Take

$$I = \{i \in \{0, \ldots, n-1\} : w_2(i) \leq t\}$$

for some t, where
$w_2(i) = w_H(\texttt{binrep}(i))$, the Hamming weight of binary representation (of length k) of i.

Finding a good I

Idea 2 (indices of small Hamming weight):
Take

$$I = \{i \in \{0, \ldots, n-1\} : w_2(i) \leq t\}$$

for some t, where
$w_2(i) = w_H(\texttt{binrep}(i))$, the Hamming weight of binary representation (of length k) of i.

Then:

Finding a good I

Idea 2 (indices of small Hamming weight):
Take

$$I = \{i \in \{0, \ldots, n-1\} : w_2(i) \leq t\}$$

for some t, where
$w_2(i) = w_H(\texttt{binrep}(i))$, the Hamming weight of binary representation (of length k) of i.

Then:

- Since $n = 2^k - 1$, $i \mapsto 2i$ preserves Hamming weight, and hence I is 2-cyclotomic.

Finding a good I

Idea 2 (indices of small Hamming weight):
Take

$$I = \{i \in \{0, \ldots, n-1\} : w_2(i) \leq t\}$$

for some t, where
$w_2(i) = w_H(\texttt{binrep}(i))$, the Hamming weight of binary representation (of length k) of i.

Then:

- Since $n = 2^k - 1$, $i \mapsto 2i$ preserves Hamming weight, and hence I is 2-cyclotomic.
- One can prove $w_2(x + y) \leq w_2(x) + w_2(y)$. Hence

$$I + I = \{i \in \{0, \ldots, n-1\} : w_2(i) \leq 2t\}.$$

  But then $I + I \subseteq (0, A)$, where
  $\texttt{binrep}(A) = (1, 1, 1, ..., 1, 0, 0, ..., 0)$ [$2t$ ones].

Finding a good I

Idea 2: Take

$$I = \{i \in \{1, \ldots, n-1\} : w_2(i) \leq t\}$$

for some t.

"Problem":

- Not really a problem, but already known construction: equivalent to Reed-Muller codes.
- Somewhat limited choice of parameters.

Finding a good I

Idea 3: Based on *s-restricted binary weights*

Let $s \leq k$. Again take binary rep. of indices are of length k.

Finding a good I

Idea 3: Based on *s-restricted binary weights*

Let $s \leq k$. Again take binary rep. of indices are of length k.

The s-restricted binary weight $w_2^{(s)}(i)$ of $i \in \{0, \ldots, 2^k - 1\}$ is:

$$w_2^{(s)}(i) = max\{w_H(v) : v \text{ subvector of } s \text{ cyclically consecutive bits in } \texttt{binrep}_k(i)\}$$

Restricted weights - Example

E.g. let $n = 63$, so $k = 6$. Let $s = 3$.
Let $i = 17$.
Binary representation:

$$\texttt{binrep}_6(17) = (0, 1, 0, 0, 0, 1).$$

Restricted weights - Example

E.g. let $n = 63$, so $k = 6$. Let $s = 3$.
Let $i = 17$.
Binary representation:

$$\texttt{binrep}_6(17) = ({\color{red}0}, {\color{red}1}, {\color{red}0}, 0, 0, 1).$$

We look at all windows of 3 consecutive positions.
$(0, 1, 0) \rightarrow$ weight 1

Restricted weights - Example

E.g. let $n = 63$, so $k = 6$. Let $s = 3$.
Let $i = 17$.
Binary representation:

$$\texttt{binrep}_6(17) = (0, 1, 0, 0, 0, 1).$$

We look at all windows of 3 consecutive positions.
$(0, 1, 0) \rightarrow$ weight 1
$(1, 0, 0) \rightarrow$ weight 1

Restricted weights - Example

E.g. let $n = 63$, so $k = 6$. Let $s = 3$.
Let $i = 17$.
Binary representation:

$$\texttt{binrep}_6(17) = (0, 1, 0, 0, 0, 1).$$

We look at all windows of 3 consecutive positions.
$(0, 1, 0) \rightarrow$ weight 1
$(1, 0, 0) \rightarrow$ weight 1
$(0, 0, 0) \rightarrow$ weight 0

Restricted weights - Example

E.g. let $n = 63$, so $k = 6$. Let $s = 3$.
Let $i = 17$.
Binary representation:

$$\texttt{binrep}_6(17) = (0, 1, 0, \color{red}{0}, \color{red}{0}, \color{red}{1}).$$

We look at all windows of 3 consecutive positions.
$(0, 1, 0) \to$ weight 1
$(1, 0, 0) \to$ weight 1
$(0, 0, 0) \to$ weight 0
$(0, 0, 1) \to$ weight 1

Restricted weights - Example

E.g. let $n = 63$, so $k = 6$. Let $s = 3$.
Let $i = 17$.
Binary representation:

$$\texttt{binrep}_6(17) = (0, 1, 0, 0, 0, 1).$$

We look at all windows of 3 consecutive positions.
$(0, 1, 0) \rightarrow$ weight 1
$(1, 0, 0) \rightarrow$ weight 1
$(0, 0, 0) \rightarrow$ weight 0
$(0, 0, 1) \rightarrow$ weight 1
$(0, 1, 0) \rightarrow$ weight 1

Restricted weights - Example

E.g. let $n = 63$, so $k = 6$. Let $s = 3$.
Let $i = 17$.
Binary representation:

$$\texttt{binrep}_6(17) = ({\color{red}0}, {\color{red}1}, 0, 0, 0, {\color{red}1}).$$

We look at all windows of 3 consecutive positions.
$(0, 1, 0) \rightarrow$ weight 1
$(1, 0, 0) \rightarrow$ weight 1
$(0, 0, 0) \rightarrow$ weight 0
$(0, 0, 1) \rightarrow$ weight 1
$(0, 1, 0) \rightarrow$ weight 1
$(1, 0, 1) \rightarrow$ weight 2

Restricted weights - Example

E.g. let $n = 63$, so $k = 6$. Let $s = 3$.
Let $i = 17$.
Binary representation:

$$\texttt{binrep}_6(17) = (0, 1, 0, 0, 0, 1).$$

We look at all windows of 3 consecutive positions.
$(0, 1, 0) \rightarrow$ weight 1
$(1, 0, 0) \rightarrow$ weight 1
$(0, 0, 0) \rightarrow$ weight 0
$(0, 0, 1) \rightarrow$ weight 1
$(0, 1, 0) \rightarrow$ weight 1
$(1, 0, 1) \rightarrow$ weight 2
Therefore $w_2^{(3)}(17) = 2$

Construction based on s-restricted weights

Idea 3, construction: Take s, t with $s < k$, and $2m < s$.
We define

$$I = \{i \in \{1, \dots, n-1\} : w_2^{(s)}(i) \leq m\}.$$

Construction based on s-restricted weights

Idea 3, construction: Take s, t with $s < k$, and $2m < s$.
We define

$$I = \{i \in \{1, \ldots, n-1\} : w_2^{(s)}(i) \leq m\}.$$

- The s-restricted weight is also preserved under multiplication by $2 \mod n$ because $n = 2^k - 1$. Therefore I is 2-cyclotomic.

Construction based on s-restricted weights

Idea 3, construction: Take s, t with $s < k$, and $2m < s$.
We define

$$I = \{i \in \{1, \dots, n-1\} : w_2^{(s)}(i) \leq m\}.$$

- The s-restricted weight is also preserved under multiplication by $2 \mod n$ because $n = 2^k - 1$. Therefore I is 2-cyclotomic.
- One can also prove $w_2^{(s)}(x+y) \leq w_2^{(s)}(x) + w_2^{(s)}(y)$ and hence

$$I + I \subseteq \{i \in \{1, \dots, n-1\} : w_2^{(s)}(i) \leq 2m\}.$$

Construction based on s-restricted weights

Idea 3, construction: Take s, t with $s < k$, and $2m < s$.
We define

$$I = \{i \in \{1, \ldots, n-1\} : w_2^{(s)}(i) \leq m\}.$$

- The s-restricted weight is also preserved under multiplication by $2 \mod n$ because $n = 2^k - 1$. Therefore I is 2-cyclotomic.
- One can also prove $w_2^{(s)}(x+y) \leq w_2^{(s)}(x) + w_2^{(s)}(y)$ and hence

$$I + I \subseteq \{i \in \{1, \ldots, n-1\} : w_2^{(s)}(i) \leq 2m\}.$$

Because $2m < s$, one can give a non-trivial interval containing $I + I$, hence a lower bound on $d(C^{*2})$. Easy to compute.

Computing the dimensions

Let s, t with $s < k$, and $2m < s$ and

$$I = \{i \in \{1, \ldots, n-1\} : w_2^{(s)}(i) \leq m\}.$$

Recall that $\dim C = |I|$. How large is $|I|$?

Computing the dimensions

Let s, t with $s < k$, and $2m < s$ and

$$I = \{i \in \{1, \dots, n-1\} : w_2^{(s)}(i) \leq m\}.$$

Recall that $\dim C = |I|$. How large is $|I|$?

In other words, we need to:

Count all binary strings of length k, such that all substrings of s cyclically consecutive positions have at most m ones.

Computing the dimensions

Count all binary strings of length k, such that all substrings of s cyclically consecutive positions have at most m ones.

Computing the dimensions

Count all binary strings of length k, such that all substrings of s cyclically consecutive positions have at most m ones.

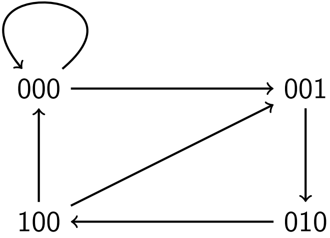
Equivalent to

Count all closed walks of length k in the directed graph where:

- Nodes are binary strings of length s and weight at most m.
- There is an edge from $v = (v_1, v_2, \ldots, v_s)$ to $w = (w_1, \ldots, w_s)$ if $v_2 = w_1, v_3 = w_2, \ldots, v_s = w_{s-1}$.

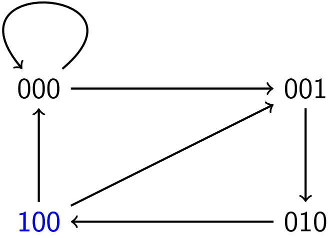
Correspondence: indices in I - closed walks of length k

$k = 7,\ s = 3,\ m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

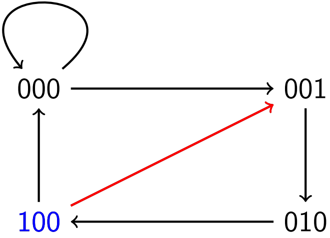
$k = 7$, $s = 3$, $m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

Correspondence: indices in I - closed walks of length k

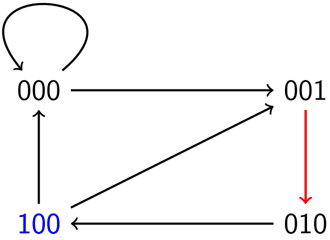
$k = 7,\ s = 3,\ m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

Correspondence: indices in I - closed walks of length k

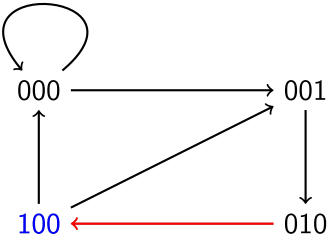
$k = 7$, $s = 3$, $m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

Correspondence: indices in I - closed walks of length k

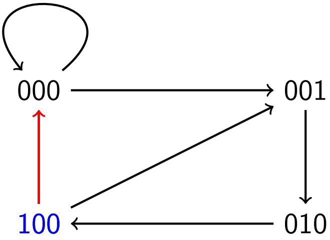
$k = 7$, $s = 3$, $m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

Correspondence: indices in I - closed walks of length k

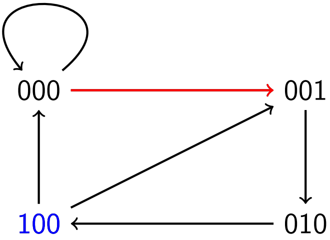
$k = 7,\ s = 3,\ m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

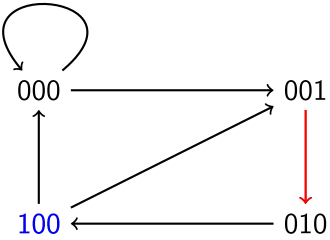
Correspondence: indices in I - closed walks of length k

$k = 7$, $s = 3$, $m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

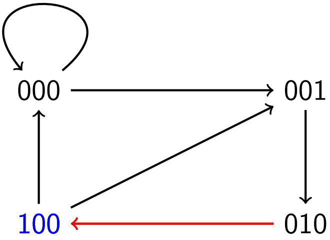
$k = 7$, $s = 3$, $m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

Correspondence: indices in I - closed walks of length k

$k = 7$, $s = 3$, $m = 1$



For example, take (1,0,0,1,0,0,0)$\in I$

Recursive formula for k

- The number of closed walks of length k is exactly $Tr(A^k)$, where A is the adjacency matrix of the graph.
- Note the graph and therefore A does not depend on k.

Recursive formula for k

- The number of closed walks of length k is exactly $Tr(A^k)$, where A is the adjacency matrix of the graph.
- Note the graph and therefore A does not depend on k.
- From Cayley-Hamilton theorem and linearity of trace:

$$p(Tr(A)) = 0$$

  where p is the characteristic polynomial of A.
- This can be extended, for $j \geq 0$, to

$$\sum_{i=0}^{g} p_i Tr(A^{i+j}) = 0$$

  where $p(X) = \sum_{i=0}^{g} p_i(X)$.

Recursive formula for k

- Hence if we fix m and s, and increase k (therefore increasing the length $n = 2^k - 1$ of the codes), we have a recursive formula for their dimensions.

Example

For $m = 1$, $s = 3$, dimensions given by

$$Tr(A^k) = Tr(A^{k-1}) + Tr(A^{k-3}), \quad Tr(A) = Tr(A^2) = 1, Tr(A^3) = 4$$

Example

For $m = 1$, $s = 3$, dimensions given by

$$Tr(A^k) = Tr(A^{k-1}) + Tr(A^{k-3}), \quad Tr(A) = Tr(A^2) = 1, Tr(A^3) = 4$$

k	n	dim C	$d(C^{*2}) \geq$	Observations*
3	7	4	1	Both C and C^{*2} optimal
4	15	5	3	Both C and C^{*2} optimal
5	31	6	7	C optimal, C^{*2} not
6	63	10	9	C best known, C^{*2} not
7	127	15	19	Both C and C^{*2} best known
8	255	21	39	Both C and C^{*2} best known
9	511	31	73	

Example

For $m = 1$, $s = 3$, dimensions given by

$$Tr(A^k) = Tr(A^{k-1}) + Tr(A^{k-3}), \quad Tr(A) = Tr(A^2) = 1, Tr(A^3) = 4$$

k	n	dim C	$d(C^{*2}) \geq$	Observations*
3	7	4	1	Both C and C^{*2} optimal
4	15	5	3	Both C and C^{*2} optimal
5	31	6	7	C optimal, C^{*2} not
6	63	10	9	C best known, C^{*2} not
7	127	15	19	Both C and C^{*2} best known
8	255	21	39	Both C and C^{*2} best known
9	511	31	73	

* C optimal: $d(C)$ being largest possible for $(n, \dim C)$
* C^{*2} optimal: $d(C^{*2})$ being largest possible for $(n, \dim C^{*2})$

Open question: Is $d(C^{*2})$ optimal for $(n, \dim C)$?

Further work

- Ongoing work with J.S. Gundersen, D. Ruano, *Squares of Matrix-product Codes* (arXiv, 2019): New sets of parameters.

Further work

- Ongoing work with J.S. Gundersen, D. Ruano, *Squares of Matrix-product Codes* (arXiv, 2019): New sets of parameters.
- I. García-Marco, I. Má rquez-Corbella, D. Ruano,*High dimensional affine codes whose square has a designed minimum distance* (arXiv, 2019).

Further work

- Ongoing work with J.S. Gundersen, D. Ruano, *Squares of Matrix-product Codes* (arXiv, 2019): New sets of parameters.
- I. García-Marco, I. Má rquez-Corbella, D. Ruano,*High dimensional affine codes whose square has a designed minimum distance* (arXiv, 2019).
- Still a lot of work to do:
  - Optimality of constructions
  - Bounds
  - Constructions of cyclic codes with length $n \neq q^k - 1$
  - Other constructions...

Thank you!

Tak! Takk! Tack! Kiitos!

I. Cascudo. "On Squares of Cyclic Codes". *IEEE Transactions of Information Theory*, 65 (2), 1034-1047, 2019.