Codes from G-invariant polynomials, joint work with Mrinmoy Datta

Trygve Johnsen

June 12, 2025

Linear codes

Let $C \subset (\mathbb{F}_q)^n$, for $\mathbb{F}_q$ the field with q elements, for q a prime power. If C is a **vector subspace** of $(\mathbb{F}_q)^n$, then it called a **linear** code.

Linear codes

Let $C \subset (\mathbb{F}_q)^n$, for $\mathbb{F}_q$ the field with q elements, for q a prime power. If C is a **vector subspace** of $(\mathbb{F}_q)^n$, then it called a **linear** code.

The **dimension** k of C is its dimension as vector space over $\mathbb{F}_q$. Clearly $0 \leq k \leq n$.

Linear codes

Let $C \subset (\mathbb{F}_q)^n$, for $\mathbb{F}_q$ the field with q elements, for q a prime power. If C is a **vector subspace** of $(\mathbb{F}_q)^n$, then it called a **linear** code.
The **dimension** k of C is its dimension as vector space over $\mathbb{F}_q$. Clearly $0 \leq k \leq n$.

For an element $\mathbf{x} \in {\mathbb{F}_q}^n$, set $\mathrm{Supp}(\mathbf{x}) = \{i | x_i \neq 0.\}$. For a subset $S \subset {\mathbb{F}_q}^n$, set $\mathrm{Supp}(S) = \cup_{\mathbf{x} \in S} \mathrm{Supp}(\mathbf{x})$.

Linear codes

Let $C \subset (\mathbb{F}_q)^n$, for $\mathbb{F}_q$ the field with q elements, for q a prime power. If C is a **vector subspace** of $(\mathbb{F}_q)^n$, then it called a **linear** code.
The **dimension** k of C is its dimension as vector space over $\mathbb{F}_q$.
Clearly $0 \leq k \leq n$.

For an element $\mathbf{x} \in {\mathbb{F}_q}^n$, set $\mathrm{Supp}(\mathbf{x}) = \{i | x_i \neq 0.\}$. For a subset $S \subset {\mathbb{F}_q}^n$, set $\mathrm{Supp}(S) = \cup_{\mathbf{x} \in S} \mathrm{Supp}(\mathbf{x})$.

Let $w(\mathbf{x}) = |\mathrm{Supp}(\mathbf{x})|$, and $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$. Let

$$d = d(C) = \min d(\mathbf{x}, \mathbf{y}),$$

for $\mathbf{x}, \mathbf{y} \in C$ and $\mathbf{x} \neq \mathbf{y}$.

Higher weights /generalized Hamming weights

From the translation invariance of linear codes,

$$d = d(C) = \min d(\mathbf{x}, \mathbf{0}),$$

for $\mathbf{x} \in C$ and $\mathbf{x} \neq \mathbf{0}$.

Higher weights /generalized Hamming weights

From the translation invariance of linear codes,

$$d = d(C) = \min d(\mathbf{x}, \mathbf{0}),$$

for $\mathbf{x} \in C$ and $\mathbf{x} \neq \mathbf{0}$.
Let $D_h = \{h$-dimensional linear subspaces of $C\}, h = 1, 2, \ldots, k = \dim C$.

Definition

For $h = 1, 2, \ldots, k$, the *h'th higher weight* of C is

$$d_h = \min\{|(\mathrm{Supp}(S)|; S \in D_h\}.$$

We have: $d_1 = d(C)$, which, as before, is called the *minimum distance* of C.

Wei duality

In the same manner we may define dual generalized Hamming weights $d_1^*, \cdots, d_{n-k}^*$ for linear codes C; these are the generalized Hamming weights of the dual code C^*, which is defined to be the orthogonal complement of C in ${\mathbb{F}_q}^n$.

Wei duality

In the same manner we may define dual generalized Hamming weights $d_1^*, \cdots, d_{n-k}^*$ for linear codes C; these are the generalized Hamming weights of the dual code C^*, which is defined to be the orthogonal complement of C in ${\mathbb{F}_q}^n$.
The following result is valid for all linear codes:

Theorem

$$\{d_1, \cdots, d_k\} \cup \{n+1-d_{n-k}^*, \cdots, n+1-d_1^*\} = \{1, 2, \cdots, n\}.$$

Wei duality

In the same manner we may define dual generalized Hamming weights $d_1^*, \cdots, d_{n-k}^*$ for linear codes C; these are the generalized Hamming weights of the dual code C^*, which is defined to be the orthogonal complement of C in ${\mathbb{F}_q}^n$.
The following result is valid for all linear codes:

Theorem

$$\{d_1, \cdots, d_k\} \cup \{n+1-d_{n-k}^*, \cdots, n+1-d_1^*\} = \{1, 2, \cdots, n\}.$$

Corollary

We have: $d_i < d_{i+1}$, *for* $i = 1, \cdots, k-1$.

The d_i (in addition to $d_1 = d$) are important for giving bounds for the complexity of processes like Viterbi decoding. (G. Forney). They also have cryptographical interpretations in cases where the generator matrices of the codes are used in connection with the so-called wire-tap channels of type 2.

Main goal in (linear) coding theory

Given k and n, construct C such that $d_1, d_2, \ldots, d_k$ are as big as possible.

The d_i (in addition to $d_1 = d$) are important for giving bounds for the complexity of processes like Viterbi decoding. (G. Forney). They also have cryptographical interpretations in cases where the generator matrices of the codes are used in connection with the so-called wire-tap channels of type 2.

Main goal in (linear) coding theory

Given k and n, construct C such that $d_1, d_2, \dots, d_k$ are as big as possible.
Or: For classes of codes "that appear in a natural way", and/or are easy to construct; determine $n, k, d = d_1, d_2, \cdots, d_k$, and (higher) weight spectra of the codes.

Today we will define and study a class of Reed-Muller type error-correcting codes obtained from elementary symmetric functions in finitely many variables. We determine the code parameters and higher weight spectra in the simplest cases.

For a positive integer m and a non-negative integer i, we denote by σ_m^i the i-th elementary symmetric polynomial in m variables $x_1, \ldots, x_m$, i.e.

$$\sigma_m^i = \sum_{1 \leq j_1 < \cdots < j_i \leq m} x_{j_1} \cdots x_{j_i}$$

for $1 \leq i \leq m$ and $\sigma_m^0 = 1$.

For a positive integer m and a non-negative integer i, we denote by σ_m^i the i-th elementary symmetric polynomial in m variables $x_1, \ldots, x_m$, i.e.

$$\sigma_m^i = \sum_{1 \leq j_1 < \cdots < j_i \leq m} x_{j_1} \cdots x_{j_i}$$

for $1 \leq i \leq m$ and $\sigma_m^0 = 1$.
Any symmetric polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ can be written as an algebraic expression in $\sigma_m^0, \ldots, \sigma_m^m$.

In this talk we are only interested in symmetric polynomials that are $\mathbb{F}_q$-linear combinations of the σ^i_m.

In this talk we are only interested in symmetric polynomials that are $\mathbb{F}_q$-linear combinations of the σ_m^i.

Let Σ_m be the $\mathbb{F}_q$-linear subspace generated by the elementary symmetric polynomials $\sigma_m^0, \ldots, \sigma_m^m$. Note that $\dim_{\mathbb{F}_q} \Sigma_m = m + 1$.

In this talk we are only interested in symmetric polynomials that are $\mathbb{F}_q$-linear combinations of the σ_m^i.

Let Σ_m be the $\mathbb{F}_q$-linear subspace generated by the elementary symmetric polynomials $\sigma_m^0, \ldots, \sigma_m^m$. Note that $\dim_{\mathbb{F}_q} \Sigma_m = m + 1$.

A point $(a_1, \ldots, a_m) \in \mathbb{A}^m(\mathbb{F}_q)$ is said to be *distinguished* if $a_i \neq a_j$ whenever $i \neq j$.

In this talk we are only interested in symmetric polynomials that are $\mathbb{F}_q$-linear combinations of the σ_m^i.

Let Σ_m be the $\mathbb{F}_q$-linear subspace generated by the elementary symmetric polynomials $\sigma_m^0, \ldots, \sigma_m^m$. Note that $\dim_{\mathbb{F}_q} \Sigma_m = m + 1$.

A point $(a_1, \ldots, a_m) \in \mathbb{A}^m(\mathbb{F}_q)$ is said to be *distinguished* if $a_i \neq a_j$ whenever $i \neq j$.

Let $\mathbb{A}_D(\mathbb{F}_q)^m = \mathbb{A}_D^m$ be the set of all distinguished points of $\mathbb{A}^m(\mathbb{F}_q) = \mathbb{F}_q^m$.

Definition

We fix an ordering $\{P_1, \dots, P_n\}$ of elements in $\mathbb{A}^m_D$. Define an evaluation map

$$\mathrm{ev} : \Sigma_m \to \mathbb{F}_q^n, \quad \text{given by} \quad f \mapsto (f(P_1), \dots, f(P_n)).$$

One sees that ev is a linear map and consequently the image, $\mathcal{C}_m$ of ev is a (linear)code.

We have:

Proposition

If $m \leq q-1$, then the code $\mathcal{C}_m$ is a nondegenerate $[n,k,d]$ code, where $n = \frac{q!}{(q-m)!}$, $k = m+1$ and $d = (q-m)\frac{(q-1)!}{(q-m)!}$. Furthermore, the code $\mathcal{C}_m$ is generated by minimum weight codewords.

We have:

Proposition

If $m \leq q-1$, then the code $\mathcal{C}_m$ is a nondegenerate $[n,k,d]$ code, where $n = \frac{q!}{(q-m)!}$, $k = m+1$ and $d = (q-m)\frac{(q-1)!}{(q-m)!}$. Furthermore, the code $\mathcal{C}_m$ is generated by minimum weight codewords.

Proof: The statement on the length n of the code is trivial, while the fact that the code is non-degenerate follows readily by observing that $\mathrm{ev}(1) = (1,\ldots,1) \in \mathcal{C}_m$.

To show that $\mathcal{C}_m$ is of dimension $m+1$, it is enough to show that the map ev is injective. To this end, let $f \in \Sigma_m$ with $\mathrm{ev}(f) = (0, \ldots, 0)$. Then f has n zeroes in $\mathbb{A}^m_D$. But it can be shown that if $f \neq 0$, then f has at most $m\frac{(q-1)!}{(q-m)!}$ zeroes. And this is a smaller number than n. This also shows that $d \geq n - m\frac{(q-1)!}{(q-m)!}$. We get equality for d, since functions of type

$$f = c(x_1 - b)(x_2 - b) \cdots (x_m - b)$$

have exactly $m\frac{(q-1)!}{(q-m)!}$ zeroes in $\mathbb{A}^m_D$.

To show that $\mathcal{C}_m$ is of dimension $m+1$, it is enough to show that the map ev is injective. To this end, let $f \in \Sigma_m$ with $\mathrm{ev}(f) = (0, \ldots, 0)$. Then f has n zeroes in $\mathbb{A}^m_D$. But it can be shown that if $f \neq 0$, then f has at most $m\frac{(q-1)!}{(q-m)!}$ zeroes. And this is a smaller number than n. This also shows that $d \geq n - m\frac{(q-1)!}{(q-m)!}$. We get equality for d, since functions of type

$$f = c(x_1 - b)(x_2 - b)\cdots(x_m - b)$$

have exactly $m\frac{(q-1)!}{(q-m)!}$ zeroes in $\mathbb{A}^m_D$.

Being generated by minimum weight codewords follows by considering choices of $m+1$ different (and then linearly independent) functions

$$f = c(x_1 - b_i)(x_2 - b_i)\cdots(x_m - b_i).$$

Remark

We note that the relative minimum distance $1 - \frac{m}{q}$ *of* $\mathcal{C}_m$ *is as that of the generalized Reed-Muller codes of order m.*

Proposition

a) An element of Σ_m *is either irreducible, or completely reducible of type* $c(x_1 - b)(x_2 - b) \cdots (x_m - b))$, *for some* c, b.

Remark

We note that the relative minimum distance $1 - \frac{m}{q}$ of $\mathcal{C}_m$ is as that of the generalized Reed-Muller codes of order m.

Proposition

a) An element of Σ_m is either irreducible, or completely reducible of type $c(x_1 - b)(x_2 - b) \cdots (x_m - b))$, for some c, b.

b) If $f \in \Sigma_m$ is irreducible, its number of zeroes in $\mathbb{A}^m_D$ is upper-bounded by $m\frac{(q-1)!}{(q-m)!} - (q - m)\frac{(q-2)!}{(q-m)!}$

Remark

We note that the relative minimum distance $1 - \frac{m}{q}$ of $\mathcal{C}_m$ is as that of the generalized Reed-Muller codes of order m.

Proposition

a) An element of Σ_m is either irreducible, or completely reducible of type $c(x_1 - b)(x_2 - b)\cdots(x_m - b))$, for some c, b.

b) If $f \in \Sigma_m$ is irreducible, its number of zeroes in $\mathbb{A}^m_D$ is upper-bounded by $m\frac{(q-1)!}{(q-m)!} - (q-m)\frac{(q-2)!}{(q-m)!}$

c) The number of codewords of minimal weight is $q(q-1)$

(For c.): There are $(q-1)$ choices of c and q choices of b.)

A sister code $\mathcal{C}_m$

The code $\mathcal{C}_m$ is made by evaluating each of the functions in Σ_m at the points of $\mathbb{A}_D^m$.

A sister code $\mathcal{C}_m$

The code $\mathcal{C}_m$ is made by evaluating each of the functions in Σ_m at the points of $\mathbb{A}^m_D$.

But the points of $\mathbb{A}^m_D$ constitute a disjoint union of S_m-orbits, each of cardinality $m!$, where the symmetric group S_m in m letters acts freely by permuting the coordinates.

A sister code $\mathcal{C}_m$

The code $\mathcal{C}_m$ is made by evaluating each of the functions in Σ_m at the points of $\mathbb{A}^m_D$.

But the points of $\mathbb{A}^m_D$ constitute a disjoint union of S_m-orbits, each of cardinality $m!$, where the symmetric group S_m in m letters acts freely by permuting the coordinates.

We now pick a new ordered set R_D, consisting of one point from each of the S_m orbits mentioned above. say $Q_1, \ldots, Q_N$, where $N = \binom{q}{m}$.
We now consider the evaluation map ev, followed by the projection onto R_D:

$$\mathrm{ev}' : \Sigma_m \to \mathbb{F}_q^N \quad \text{given by} \quad f \mapsto (f(Q_1), \ldots, f(Q_N)).$$

Let $\mathcal{C}'_m$ denote the image of the "orbit slice" R_D under the map ev'. The following proposition follows directly from Proposition 2.1, since the ev-map is constant on the S_m-orbits.

Let $\mathcal{C}'_m$ denote the image of the "orbit slice" R_D under the map ev'. The following proposition follows directly from Proposition 2.1, since the ev-map is constant on the S_m-orbits.

Proposition

If $m < q$, then $\mathcal{C}'_m$ is a nondegenerate $[N, K, D]$ linear code where $N = \binom{q}{m}$, $K = m + 1$ and $D = \binom{q}{m} - \binom{q-1}{m-1}$.

Let $\mathcal{C}'_m$ denote the image of the "orbit slice" R_D under the map ev'. The following proposition follows directly from Proposition 2.1, since the ev-map is constant on the S_m-orbits.

Proposition

If $m < q$, then $\mathcal{C}'_m$ is a nondegenerate $[N, K, D]$ linear code where $N = \binom{q}{m}$, $K = m + 1$ and $D = \binom{q}{m} - \binom{q-1}{m-1}$.

One may work "in parallel" with $\mathcal{C}_m$ and $\mathcal{C}'_m$, and most results in question, for one of these codes, will imply corresponding results for its "sister code".

Proposition

Fix positive integers $1 \leq r < m+1 \leq q$. We have

$$d_r(\mathcal{C}_m) \leq \frac{q!}{(q-m)!} - m!\binom{q-r}{m-r}, \text{ and } d_r(\mathcal{C}'_m) \leq \binom{q}{m} - \binom{q-r}{m-r},$$

$$\text{Moreover } d_m(\mathcal{C}'_m) = \binom{q}{m} - 1, \text{ and } d_{m+1}(\mathcal{C}'_m) = \binom{q}{m}$$

Proposition

Fix positive integers $1 \leq r < m+1 \leq q$. We have

$$d_r(\mathcal{C}_m) \leq \frac{q!}{(q-m)!} - m! \binom{q-r}{m-r}, \text{ and } d_r(\mathcal{C}'_m) \leq \binom{q}{m} - \binom{q-r}{m-r},$$

$$\text{Moreover } d_m(\mathcal{C}'_m) = \binom{q}{m} - 1, \text{ and } d_{m+1}(\mathcal{C}'_m) = \binom{q}{m}$$

The two first(equivalent statements follow by considering choices of r different (and then linearly independent) functions

$$f = c(x_1 - b_i)(x_2 - b_i) \cdots (x_m - b_i).$$

Proposition

Fix positive integers $1 \leq r < m+1 \leq q$. We have

$$d_r(\mathcal{C}_m) \leq \frac{q!}{(q-m)!} - m! \binom{q-r}{m-r}, \text{ and } d_r(\mathcal{C}'_m) \leq \binom{q}{m} - \binom{q-r}{m-r},$$

$$\text{Moreover } d_m(\mathcal{C}'_m) = \binom{q}{m} - 1, \text{ and } d_{m+1}(\mathcal{C}'_m) = \binom{q}{m}$$

The two first(equivalent statements follow by considering choices of r different (and then linearly independent) functions

$$f = c(x_1 - b_i)(x_2 - b_i) \cdots (x_m - b_i).$$

The third statement follows from proving $d((\mathcal{C}'_m)^{\perp}) \geq 3$, since no two columns of a generator matrix for $\mathcal{C}'_m$ are parallel.

By the previous results $\mathcal{C}_2$ for $q \geq 3$, is an $[n, k, d]$ code, where

$$n = q(q-1), \text{ and } k = 3,$$

and

$$(d_1, d_2, d_3) = ((q-1)(q-2), q(q-1)-2, q(q-1)).$$

By the previous results $\mathcal{C}_2$ for $q \geq 3$, is an $[n, k, d]$ code, where

$$n = q(q-1), \text{ and } k = 3,$$

and

$$(d_1, d_2, d_3) = ((q-1)(q-2), q(q-1) - 2, q(q-1)).$$

We now proceed to determine the weight distribution for the code $\mathcal{C}_2$.

Definition

Let w and r be integers satisfying $0 \leq w \leq q(q-1)$ and $1 \leq r \leq 3$. Define

(a) $A_w :=$ the number of codewords of $\mathcal{C}_2$ of Hamming weight w.

(b) $A_w^{(r)} :=$ the number of r-dimensional subcodes of $\mathcal{C}_2$ of support weight w.

We have the following results:

Proposition

If q is odd, and $q \geq 5$, then we have

$$A_w = \begin{cases} 1, & \textit{if } w = 0 \\ q(q-1), & \textit{if } w = (q-1)(q-2) \\ \frac{q(q-1)(q+1)}{2}, & \textit{if } w = q(q-1)-(q-1) \\ \frac{q(q-1)^2}{2}, & \textit{if } w = q(q-1)-(q-3) \\ (q-1), & \textit{if } w = q(q-1) \\ 0, & \textit{otherwise.} \end{cases}$$

We have the following results:

Proposition

If q is odd, and $q \geq 5$, then we have

$$A_w = \begin{cases} 1, & \text{if } w = 0 \\ q(q-1), & \text{if } w = (q-1)(q-2) \\ \frac{q(q-1)(q+1)}{2}, & \text{if } w = q(q-1)-(q-1) \\ \frac{q(q-1)^2}{2}, & \text{if } w = q(q-1)-(q-3) \\ (q-1), & \text{if } w = q(q-1) \\ 0, & \text{otherwise.} \end{cases}$$

For $q = 3$, we have $A_0 = 1, A_1 = 6, A_4 = 12$, and $A_6 = 8$.

Proposition

If q is even, and $q \geq 4$, then we have

$$A_w = \begin{cases} 1, & \text{if } w = 0 \\ q(q-1), & \text{if } w = (q-1)(q-2) \\ q(q-1)^2, & \text{if } w = q(q-1)-(q-2) \\ (q-1)^2, & \text{if } w = q(q-1)-1 \\ 2(q-1), & \text{if } w = q(q-1) \\ 0, & \text{otherwise.} \end{cases}$$

Proposition

If q is even, and $q \geq 4$, then we have

$$A_w = \begin{cases} 1, & \text{if } w = 0 \\ q(q-1), & \text{if } w = (q-1)(q-2) \\ q(q-1)^2, & \text{if } w = q(q-1)-(q-2) \\ (q-1)^2, & \text{if } w = q(q-1)-1 \\ 2(q-1), & \text{if } w = q(q-1) \\ 0, & \text{otherwise.} \end{cases}$$

These results appear as a consequence of a detailed and refined study of the zeroes of the $f \in \Sigma_2$ in odd and even characteristic. This study represents the main work with the article this talk is based on.

We now turn our attention towards computing $A_w^{(i)}$-s for all values of $1 \leq w \leq q(q-1)$ and $i = 1, 2, 3$ for the code $\mathcal{C}_2$. We have the following result:

Proposition

For $1 \leq w \leq q(q-1)$ and $i = 1, 2, 3$ we have

$$A_w^{(i)} = \begin{cases} \frac{A_w}{q-1}, & \textit{if} \quad i = 1 \\ \frac{q(q-1)}{2}, & \textit{if} \quad w = q(q-1) - 2 \textit{ and } i = 2 \\ \frac{q^2+3q+2}{2}, & \textit{if} \quad w = q(q-1) \textit{ and } i = 2 \\ 1, & \textit{if} \quad w = q(q-1) \textit{ and } i = 3, \\ 0, & \textit{otherwise.} \end{cases}$$

Proof.

The assertions concerning the cases when $i = 1$ and $i = 3$ are clear. To prove the claims concerning the cases when $i = 2$, we must analyze the possible number of distinguished points on the intersection of two curves given by the zeroes of two linearly independent functions

$$f_1(x,y) = a_0 + a_1(x+y) + a_2xy \quad \text{and} \quad f_2(x,y) = b_0 + b_1(x+y) + b_2xy.$$

A detailed, somewhat geometrical, proof gives the result. $\square$

The spectra of extension codes

Let $(\mathcal{C}_2)^{(s)} = \mathcal{C}_2 \otimes_{\mathbb{F}_q} \mathbb{F}_{q^s}$ for $s \geqslant 1$. It is a linear code over $\mathbb{F}_Q$, for $Q = q^s$, with the same generator matrix as $\mathcal{C}_2$ itself.

The spectra of extension codes

Let $(\mathcal{C}_2)^{(s)} = \mathcal{C}_2 \otimes_{\mathbb{F}_q} \mathbb{F}_{q^s}$ for $s \geqslant 1$. It is a linear code over $\mathbb{F}_Q$, for $Q = q^s$, with the same generator matrix as $\mathcal{C}_2$ itself. Denote the

number of codewords of weight w for $(\mathcal{C}_2)^{(s)}$ by $P_w(Q)$. Then, by for example Jurrius(2012):

The spectra of extension codes

Let $(\mathcal{C}_2)^{(s)} = \mathcal{C}_2 \otimes_{\mathbb{F}_q} \mathbb{F}_{q^s}$ for $s \geqslant 1$. It is a linear code over $\mathbb{F}_Q$, for $Q = q^s$, with the same generator matrix as $\mathcal{C}_2$ itself. Denote the

number of codewords of weight w for $(\mathcal{C}_2)^{(s)}$ by $P_w(Q)$. Then, by for example Jurrius(2012):

$$P_w(Q) = \sum_{r=0}^{k} A_w^{(r)} \prod_{i=0}^{r-1} (q^s - q^i) = \sum_{r=0}^{k} A_w^{(r)} \prod_{i=0}^{r-1} (Q - q^i).$$

Corollary

For $(\mathcal{C}_2)^{(s)}$ we have, if $q \geq 7$ is odd :

$$P_0(Q) = 1,\ P_{n-2(q-1)}(Q) = q(Q-1),\ P_{n-(q-1)}(Q) = \frac{q^2+q}{2}(Q-1),$$

$$P_{n-(q-3)}(Q) = \frac{q^2-q}{2}(Q-1),\ P_{n-2}(Q) = \frac{q^2-q}{2}(Q-1)(Q-q),$$

$$P_n(Q) = (Q-1)(Q^2 + \frac{-q^2+q+2}{2}Q + \frac{q^3-3q^2-2q+2}{2}).$$

One can find analogous formulas for $q = 3, 5$, and for even $q \geq 4$.

For $m \geq 3$ very little is known about $\mathcal{C}_m$,(as far as we know), other than the values of $n, d_{k-1} = d_m, d_k = d_{m+1}$. For $m = 3$, however, the only unknown d_i is d_2. The only additional, tiny "result" we have about d_2 for $m = 3$, is:

For $m \geq 3$ very little is known about $\mathcal{C}_m$,(as far as we know), other than the values of $n, d_{k-1} = d_m, d_k = d_{m+1}$. For $m = 3$, however, the only unknown d_i is d_2. The only additional, tiny "result" we have about d_2 for $m = 3$, is:

Proposition

For $q = 5$, we have $d_2(\mathcal{C}_3) = 42$, and hence $(d_1, d_2, d_3, d_4) = (24, 42, 54, 60)$, while the corresponding numbers then are $(4, 7, 9, 10)$ for $\mathcal{C}'_3$.

For $m \geq 3$ very little is known about $\mathcal{C}_m$,(as far as we know), other than the values of $n, d_{k-1} = d_m, d_k = d_{m+1}$. For $m = 3$, however, the only unknown d_i is d_2. The only additional, tiny "result" we have about d_2 for $m = 3$, is:

Proposition

For $q = 5$, we have $d_2(\mathcal{C}_3) = 42$, and hence $(d_1, d_2, d_3, d_4) = (24, 42, 54, 60)$, while the corresponding numbers then are $(4, 7, 9, 10)$ for $\mathcal{C}'_3$.

Proof: A "dirty" argument, in part by using computers. The argument was presented in our joint paper just to illustrate the complexity for $m \geq 3$.

Similar codess, including codes from A_m-invariant polynomials.

Giacomo Micheli, Vincenzo Pallozzi Lavorante, and Phillip Waitkevich studied such codes, patterned after the analysis of codes from S_m-invariant polynomials invariant polynomial described above.

Similar codess, including codes from A_m-invariant polynomials.

Giacomo Micheli, Vincenzo Pallozzi Lavorante, and Phillip Waitkevich studied such codes, patterned after the analysis of codes from S_m-invariant polynomials invariant polynomial described above.

An important ingredient is: Let $g \in \overline{\mathbb{F}}[x_1, \cdots, x_m]$ be an A_m-invariant polynomial. Then there exist symmetric polynomials $s_1, s_2 \in \overline{\mathbb{F}}[x_1, \cdots, x_m]$ such that: $g = s_1 + v_m s_2$, for $v_m = \prod_{1 \leq i < j \leq m}(x_i - x_j)$ being the Vandermonde polynomial in m variables. Furthermore, the representation is unique.

Similar codess, including codes from A_m-invariant polynomials.

Barbara Gatti, Gábor Korchmáros, Gábor P. Nagy, Vincenzo Pallozzi Lavorante, and Gioia Schulte studied evaluation codes from linear systems of s_m-invariant polynomials that were themselves homogeneous, but not necessarily linear, in the elementary symmetric functions.

Definition

$S \subset \mathbb{P}^m$ is said to be a k-arc if $|S| = k$, and $|S \cap H| \leq m$ for all hyperplanes H in $\mathbb{P}^m$.

Definition

$S \subset \mathbb{P}^m$ is said to be a k-arc if $|S| = k$, and $|S \cap H| \leq m$ for all hyperplanes H in $\mathbb{P}^m$.
A k-arc is complete if S is not contained in a $(k+1)$-arc.

Definition

$S \subset \mathbb{P}^m$ is said to be a k-arc if $|S| = k$, and $|S \cap H| \leq m$ for all hyperplanes H in $\mathbb{P}^m$.
A k-arc is complete if S is not contained in a $(k+1)$-arc.

Compelete Arc Conjecture

The rational normal curve $C_m \subset \mathbb{P}^m$ is a complete $(q+1)$-arc if $1 \leq m \leq q$, and q odd. It is also complete if q is even and $m = 1$ or $3 \leq m \leq q-3$.

Here $C_m = \{(1, t, \cdots, t^m) | t \in \mathbb{F}_q\} \cup \{(0, 0, \cdots, 0, 1)\}$.

We observe: If $S \subset \mathbb{P}^m$ is a k-arc, with the property that for all $P \in \mathbb{P}^m - S$, there exists a hyperplane H passing through P, such that $|S \cap H| = m$, then S is a complete k-arc.

We observe: If $S \subset \mathbb{P}^m$ is a k-arc, with the property that for all $P \in \mathbb{P}^m - S$, there exists a hyperplane H passing through P, such that $|S \cap H| = m$, then S is a complete k-arc.

Let $P = (a_0, a_1, \cdots, a_m) \in \mathbb{P}^m$. then there exists a hyperplane H passing through P, such that $|S \cap H| = m$ if and only if:

$a_m\sigma_m^0 - a_{m-1}\sigma_m^1 + \cdots + a_m(-1)^m\sigma_m^m$ has a zero in $\mathbb{A}_D^m$, or
$a_{m-1}\sigma_m^0 - a_{m-2}\sigma_m^1 + a_0 \cdots + (-1)^{m-1}\sigma_m^{m-1}$ has a zero in $\mathbb{A}_D^m$.

We observe: If $S \subset \mathbb{P}^m$ is a k-arc, with the property that for all $P \in \mathbb{P}^m - S$, there exists a hyperplane H passing through P, such that $|S \cap H| = m$, then S is a complete k-arc.

Let $P = (a_0, a_1, \cdots, a_m) \in \mathbb{P}^m$. then there exists a hyperplane H passing through P, such that $|S \cap H| = m$ if and only if:

$a_m\sigma_m^0 - a_{m-1}\sigma_m^1 + \cdots + a_m(-1)^m\sigma_m^m$ has a zero in $\mathbb{A}_D^m$, or
$a_{m-1}\sigma_m^0 - a_{m-2}\sigma_m^1 + a_0 \cdots + (-1)^{m-1}\sigma_m^{m-1}$ has a zero in $\mathbb{A}_D^m$.

Hence the study of the complete arc conjecture "runs in parallel" with the study of codewords of $\mathcal{C}_m$. We were not able to solve the conjecture, but obtained results about these codes as a byproduct, and my coauthor Datta has also (at least) reproduced old, partial results related to the conjecture.