Generalized AG-codes from maximal curves

Marco Calderini

12 March 2012

AG-codes

Let $K = \overline{\mathbb{F}_q}$ and $\mathcal{X}$ a non-singular curve defined over $\mathbb{F}_q$.

- $\mathbb{F}_q(\mathcal{X}) = \left\{ \alpha \in K(\mathcal{X}) \middle| \alpha = \frac{F+I(\mathcal{X})}{G+I(\mathcal{X})} \text{ and } F, G \in \mathbb{F}_q[x_0, \dots, x_m] \right\}$
- $\mathcal{X}(\mathbb{F}_q) = \{P \in \mathcal{X} \,|\, \Phi(P) = P\}$, where $\Phi : (a_0 : \dots : a_m) \longmapsto (a_0^q : \dots : a_m^q)$
- $Div_{\mathbb{F}_q}(\mathcal{X}) = \{D \in Div(\mathcal{X}) \,|\, \nu_P(D) = \nu_{\Phi(P)}(D), \forall\, P \in \mathcal{X}\}$
- $\mathcal{L}_{\mathbb{F}_q}(D) = \{\alpha \in \mathbb{F}_q(\mathcal{X})^* \,|\, (\alpha) + D \geq 0\} \cup \{0\}$

AG-codes

- $\mathcal{X}$ algebraic curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_n \in \mathcal{X}(\mathbb{F}_q)$
- Let $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \ldots, P_n\} = \emptyset$

Definition

Consider the $\mathbb{F}_q$-linear map

$$\begin{aligned} ev : \mathcal{L}_{\mathbb{F}_q}(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) . \end{aligned}$$

The image of ev is an algebraic-geometry code, $C(P_1, \ldots, P_n; G) = ev(\mathcal{L}_{\mathbb{F}_q}(G))$.

AG-codes

- $\mathcal{X}$ algebraic curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_n \in \mathcal{X}(\mathbb{F}_q)$
- Let $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \ldots, P_n\} = \emptyset$

Definition

Consider the $\mathbb{F}_q$-linear map

$$\begin{aligned} ev : \mathcal{L}_{\mathbb{F}_q}(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) . \end{aligned}$$

The image of ev is an algebraic-geometry code, $C(P_1, \ldots, P_n; G) = ev(\mathcal{L}_{\mathbb{F}_q}(G))$.

AG-codes

- $\mathcal{X}$ algebraic curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_n \in \mathcal{X}(\mathbb{F}_q)$
- Let $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \ldots, P_n\} = \emptyset$

Definition

Consider the $\mathbb{F}_q$-linear map

$$\begin{aligned} ev : \mathcal{L}_{\mathbb{F}_q}(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) . \end{aligned}$$

The image of ev is an algebraic-geometry code, $C(P_1, \ldots, P_n; G) = ev(\mathcal{L}_{\mathbb{F}_q}(G))$.

AG-codes

- $\mathcal{X}$ algebraic curve of genus g over $\mathbb{F}_q$
- $P_1, \dots, P_n \in \mathcal{X}(\mathbb{F}_q)$
- Let $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \dots, P_n\} = \emptyset$

Definition

Consider the $\mathbb{F}_q$*-linear map*

$$\begin{aligned} ev : \mathcal{L}_{\mathbb{F}_q}(G) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \dots, f(P_n)) . \end{aligned}$$

The image of ev *is an algebraic-geometry code,* $C(P_1, \dots, P_n; G) = ev(\mathcal{L}_{\mathbb{F}_q}(G))$.

AG-codes

Theorem

If G has degree less than n, then $C(P_1, \ldots, P_n; G)$ is an $[n, k, d]_q$-code with

$$k \geq \deg(G) - g + 1 \quad d \geq n - \deg(G).$$

AG-codes

Remark

Let C be a linear code $[n, k, d]_q$.
Relative Singleton defect:

$$\Delta = 1 + \frac{1}{n} - (R + \delta),$$

where $R = \frac{k}{n}$ and $\delta = \frac{d}{n}$.

Goal: to minimize relative Singleton defect of the code.

AG-codes

Remark

For an AG-code we have

$$k + d \geq n - g + 1$$

so the relative Singleton defect is

$$\Delta \leq \frac{g}{\#\mathcal{X}(\mathbb{F}_q)}.$$

Good curves for codes: those with many $\mathbb{F}_q$-rational points with respect to their genus.

Theorem (Hasse-Weil Bound)

The $\mathbb{F}_q$-rational points of a non-singular curve $\mathcal{X}$ satisfy

$$\#\mathcal{X}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

Definition

A curve $\mathcal{X}$ that satisfy the equality in the Hasse-Weil bound is called $\mathbb{F}_q$-maximal.

Remark

If we have a maximal curve s.t. $\#\mathcal{X}(\mathbb{F}_q) = n$, then the AG-code, of length n, obtained from this curve has better parameters than other AG-codes of the same length, which are constructed from another curve.

Maximal Curves

Theorem (Hasse-Weil Bound)

The $\mathbb{F}_q$-rational points of a non-singular curve $\mathcal{X}$ satisfy

$$\#\mathcal{X}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

Definition

A curve $\mathcal{X}$ that satisfy the equality in the Hasse-Weil bound is called $\mathbb{F}_q$-maximal.

Remark

If we have a maximal curve s.t. $\#\mathcal{X}(\mathbb{F}_q) = n$, then the AG-code, of length n, obtained from this curve has better parameters than other AG-codes of the same length, which are constructed from another curve.

Maximal Curves

Theorem (Hasse-Weil Bound)

The $\mathbb{F}_q$-rational points of a non-singular curve $\mathcal{X}$ satisfy

$$\#\mathcal{X}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

Definition

A curve $\mathcal{X}$ that satisfy the equality in the Hasse-Weil bound is called $\mathbb{F}_q$-maximal.

Remark

If we have a maximal curve s.t. $\#\mathcal{X}(\mathbb{F}_q) = n$, then the AG-code, of length n, obtained from this curve has better parameters than other AG-codes of the same length, which are constructed from another curve.

GAG-codes

Definition

Let $P \in \mathcal{X}$ (curve defined over $\mathbb{F}_q$), we define

$$\deg P = \min\{r \mid P \in \mathcal{X}(\mathbb{F}_{q^r})\}.$$

Definition

Let $P \in \mathcal{X}$ be a point of degree r. Then the closed point of P is the set

$$\mathcal{O}(P) = \{P, \Phi(P), \Phi^2(P), \ldots, \Phi^{r-1}(P)\}.$$

GAG-codes

Definition

Let $P \in \mathcal{X}$ (curve defined over $\mathbb{F}_q$), we define

$$\deg P = \min\{r |\, P \in \mathcal{X}(\mathbb{F}_{q^r})\}.$$

Definition

Let $P \in \mathcal{X}$ be a point of degree r. Then the closed point of P is the set

$$\mathcal{O}(P) = \{P, \Phi(P), \Phi^2(P), \dots, \Phi^{r-1}(P)\}.$$

GAG-codes

- $\mathcal{X}$ curve of genus g over $\mathbb{F}_q$
- $P_1, \dots, P_r \in \mathcal{X}$ with $\deg P_i = k_i$ for $1 \le i \le r$ and $\mathcal{O}(P_i) \cap \mathcal{O}(P_j) = \emptyset$ for $i \neq j$
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \dots, P_r\} = \emptyset$
- for $1 \le i \le r$ fix C_i, $[n_i, k_i, d_i]_q$-code, and $\pi_i : \mathbb{F}_{q^{k_i}} \longrightarrow C_i$, $\mathbb{F}_q$-linear isomorphism.

Definition

Let $n = \sum_{i=1}^{r} n_i$ *and consider the* $\mathbb{F}_q$*-linear map*

$$\pi : \begin{cases} \mathcal{L}_{\mathbb{F}_q}(G) & \rightarrow & \mathbb{F}_q^n \\ f & \mapsto & (\pi_1(f(P_1)), \dots, \pi_r(f(P_r))) \end{cases}$$

The image of π *is a generalized AG-code*

$$C(P_1, \dots, P_r; G; C_1, \dots, C_r) = \pi(\mathcal{L}_{\mathbb{F}_q}(G)).$$

GAG-codes

- $\mathcal{X}$ curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_r \in \mathcal{X}$ with $\deg P_i = k_i$ for $1 \leq i \leq r$ and $\mathcal{O}(P_i) \cap \mathcal{O}(P_j) = \emptyset$ for $i \neq j$
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \ldots, P_r\} = \emptyset$
- for $1 \leq i \leq r$ fix C_i, $[n_i, k_i, d_i]_q$-code, and $\pi_i : \mathbb{F}_{q^{k_i}} \longrightarrow C_i$, $\mathbb{F}_q$-linear isomorphism.

Definition

Let $n = \sum_{i=1}^{r} n_i$ and consider the $\mathbb{F}_q$-linear map

$$\pi : \begin{cases} \mathcal{L}_{\mathbb{F}_q}(G) & \rightarrow & \mathbb{F}_q^n \\ f & \mapsto & (\pi_1(f(P_1)), \ldots, \pi_r(f(P_r))) \end{cases}$$

The image of π is a generalized AG-code

$$C(P_1, \ldots, P_r; G; C_1, \ldots, C_r) = \pi(\mathcal{L}_{\mathbb{F}_q}(G)).$$

GAG-codes

- $\mathcal{X}$ curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_r \in \mathcal{X}$ with $\deg P_i = k_i$ for $1 \leq i \leq r$ and $\mathcal{O}(P_i) \cap \mathcal{O}(P_j) = \emptyset$ for $i \neq j$
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \ldots, P_r\} = \emptyset$
- for $1 \leq i \leq r$ fix C_i, $[n_i, k_i, d_i]_q$-code, and $\pi_i : \mathbb{F}_{q^{k_i}} \longrightarrow C_i$, $\mathbb{F}_q$-linear isomorphism.

Definition

Let $n = \sum_{i=1}^{r} n_i$ *and consider the* $\mathbb{F}_q$*-linear map*

$$\pi : \begin{cases} \mathcal{L}_{\mathbb{F}_q}(G) & \to & \mathbb{F}_q^n \\ f & \mapsto & (\pi_1(f(P_1)), \ldots, \pi_r(f(P_r))) \end{cases}$$

The image of π *is a generalized AG-code*

$$C(P_1, \ldots, P_r; G; C_1, \ldots, C_r) = \pi(\mathcal{L}_{\mathbb{F}_q}(G)).$$

- $\mathcal{X}$ curve of genus g over $\mathbb{F}_q$
- $P_1, \ldots, P_r \in \mathcal{X}$ with $\deg P_i = k_i$ for $1 \leq i \leq r$ and $\mathcal{O}(P_i) \cap \mathcal{O}(P_j) = \emptyset$ for $i \neq j$
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \ldots, P_r\} = \emptyset$
- for $1 \leq i \leq r$ fix C_i, $[n_i, k_i, d_i]_q$-code, and $\pi_i : \mathbb{F}_{q^{k_i}} \longrightarrow C_i$, $\mathbb{F}_q$-linear isomorphism.

Definition

Let $n = \sum_{i=1}^{r} n_i$ and consider the $\mathbb{F}_q$-linear map

$$\pi : \begin{cases} \mathcal{L}_{\mathbb{F}_q}(G) & \rightarrow & \mathbb{F}_q^n \\ f & \mapsto & (\pi_1(f(P_1)), \ldots, \pi_r(f(P_r))) \end{cases}$$

The image of π is a generalized AG-code

$$C(P_1, \ldots, P_r; G; C_1, \ldots, C_r) = \pi(\mathcal{L}_{\mathbb{F}_q}(G)).$$

GAG-codes

- $\mathcal{X}$ curve of genus g over $\mathbb{F}_q$
- $P_1, \dots, P_r \in \mathcal{X}$ with $\deg P_i = k_i$ for $1 \leq i \leq r$ and $\mathcal{O}(P_i) \cap \mathcal{O}(P_j) = \emptyset$ for $i \neq j$
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \dots, P_r\} = \emptyset$
- for $1 \leq i \leq r$ fix C_i, $[n_i, k_i, d_i]_q$-code, and $\pi_i : \mathbb{F}_{q^{k_i}} \longrightarrow C_i$, $\mathbb{F}_q$-linear isomorphism.

Definition

Let $n = \sum_{i=1}^{r} n_i$ *and consider the* $\mathbb{F}_q$*-linear map*

$$\pi : \begin{cases} \mathcal{L}_{\mathbb{F}_q}(G) & \rightarrow & \mathbb{F}_q^n \\ f & \mapsto & (\pi_1(f(P_1)), \dots, \pi_r(f(P_r))) \end{cases}$$

The image of π *is a generalized AG-code*

$$C(P_1, \dots, P_r; G; C_1, \dots, C_r) = \pi(\mathcal{L}_{\mathbb{F}_q}(G)).$$

GAG-codes

Theorem (Xing, Niederreiter, Lam)

If $\deg(G) < \sum_{i=1}^{r} k_i$, $d_i \leq k_i$ *for* $1 \leq i \leq r$. *Then* $C(P_1, \ldots, P_r; G; C_1, \ldots, C_r)$ *is an* $[n, k, d]_q$*-code with*

$$n = \sum_{i=1}^{r} n_i, \quad k \geq \deg(G) - g + 1, \quad d \geq \sum_{i=1}^{r} d_i - \deg(G).$$

Remark

If we use $P_1, \ldots, P_r$ *rational points of the curve* $\mathcal{X}$ *and we fix* $[1, 1, 1]_q$ *as code* C_i *for* $1 \leq i \leq r$*, then the GAG-code is an AG-code.*

New GAG-codes from maximal curves

Why maximal curves?

Theorem

For all $r \geq 2$,

$$B_r = \frac{1}{r} \sum_{d|r} \mu\left(\frac{r}{d}\right) \left(\#\mathcal{X}(\mathbb{F}_{q^d})\right),$$

$\mu : \mathbb{N} \to \{0, 1, -1\}$ *is the Möbius function*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } \exists\, k > 1 \text{ s.t. } k^2 \mid n, \\ (-1)^h & \text{if } n \text{ is the product of } h \text{ prime numbers.} \end{cases}$$

Remark

If $\mathcal{X}$ is a maximal curve of genus g, then
$\#\mathcal{X}(\mathbb{F}_{q^r}) = q^r + 1 + (-1)^{r+1} 2g q^{r/2}$.

New GAG-codes from maximal curves

Why maximal curves?

Theorem

For all $r \geq 2$,

$$B_r = \frac{1}{r} \sum_{d|r} \mu\left(\frac{r}{d}\right)\left(\#\mathcal{X}(\mathbb{F}_{q^d})\right),$$

$\mu : \mathbb{N} \to \{0, 1, -1\}$ is the Möbius function

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } \exists\, k > 1 \text{ s.t. } k^2 \mid n, \\ (-1)^h & \text{if } n \text{ is the product of } h \text{ prime numbers.} \end{cases}$$

Remark

If $\mathcal{X}$ is a maximal curve of genus g, then
$\#\mathcal{X}(\mathbb{F}_{q^r}) = q^r + 1 + (-1)^{r+1} 2g q^{r/2}$.

New GAG-codes from maximal curves

We construct 2895 new GAG-codes over $\mathbb{F}_{25}, \mathbb{F}_{49}, \mathbb{F}_{64}, \mathbb{F}_{81}$.
These codes are new in the sense that for same length and dimension, their minimum distance exceeds the one given in the tables of MinT.

Maximal-*d*-Table for Linear [*n*, *k*, *d*]-Codes over F_{25} — Arbitrary

$n =$	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
$k = 0$	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
$k = 1$	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
$k = 2$	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	50	51	52	53	54	55	56	57
$k = 3$	28	29	30	31	32	33	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	48	49	50	51	52	53	54	55
$k = 4$	27	28	29	30	31	32	32	33	34	35	36	37	38	39	40	41	41	42	43	44	45	46	47	48	49	50	50	51	52	53
$k = 5$	26	27	28	29	30	31	31	32	33	34	35	36	37	38	39	40	40	41	42	43	44	45	46	47	48	49	49	50	51	52
$k = 6$	25	26	27	28	29	30	30	31	32	33	34	35	36	37	38	39	39	40	41	42	43	44	45	46	47	48	48	49	50	51
$k = 7$	24	25	26	27	28	29	29	30	31	32	33	34	35	36	37	38	38	39	40	41	42	43	44	45	46	47	47	48	49	50
$k = 8$	23	24	25	26	27	28	28	29	30	31	32	33	34	35	36	37	37	38	39	40	41	42	43	44	45	46	46	47	48	49
$k = 9$	22	23	24	25	26	27	27	28	29	30	31	32	33	34	35	36	36	37	38	39	40	41	42	43	44	45	45	46	47	48
$k = 10$	21	22	23	24	25	26	26	27	28	29	30	31	32	33	34	35	35	36	37	38	39	40	41	42	43	44	44	45	46	47
$k = 11$	20	21	22	23	24	25	25	26	27	28	29	30	31	32	33	34	34	35	36	37	38	39	40	41	42	43	43	44	45	46
$k = 12$	19	20	21	22	23	24	24	25	26	27	28	29	30	31	32	33	33	34	35	36	37	38	39	40	41	42	42	43	44	45
$k = 13$	18	19	20	21	22	23	23	24	25	26	27	28	29	30	31	32	32	33	34	35	36	37	38	39	40	41	41	42	43	44
$k = 14$	17	18	19	20	21	22	22	23	24	25	26	27	28	29	30	31	31	32	33	34	35	36	37	38	39	40	40	41	42	43
$k = 15$	16	17	18	19	20	21	21	22	23	24	25	26	27	28	29	30	30	31	32	33	34	35	36	37	38	39	39	40	41	42
$k = 16$	15	16	17	18	19	20	20	21	22	23	24	25	26	27	28	29	29	30	31	32	33	34	35	36	37	38	38	39	40	41
$k = 17$	14	15	16	17	18	19	19	20	21	22	23	24	25	26	27	28	28	29	30	31	32	33	34	35	36	37	37	38	39	40

New GAG-codes from maximal curves

$\Gamma(\mathbb{F}_q) = \{g | \exists\, \mathcal{X}\, \mathbb{F}_q\text{-maximal}\}$.

- $\Gamma(\mathbb{F}_{25}) = \{0, 1, 2, 3, 4, 10\}$;
- $\Gamma(\mathbb{F}_{49}) = \{0, 1, 2, 3, 5, 7, 9, 21\}$;
- $\Gamma(\mathbb{F}_{64}) \supseteq \{0, 1, 2, 3, 4, 6, 7, 9, 10, 12, 28\}$;
- $\Gamma(\mathbb{F}_{81}) \supseteq \{0, 1, 2, 3, 4, 6, 8, 9, 12, 16, 36\}$.

$\Gamma(\mathbb{F}_q) = \{g \mid \exists\, \mathcal{X}\ \mathbb{F}_q\text{-maximal}\}$.

- $\Gamma(\mathbb{F}_{25}) = \{0, 1, 2, 3, 4, 10\}$;
- $\Gamma(\mathbb{F}_{49}) = \{0, 1, 2, 3, 5, 7, 9, 21\}$;
- $\Gamma(\mathbb{F}_{64}) \supseteq \{0, 1, 2, 3, 4, 6, 7, 9, 10, 12, 28\}$;
- $\Gamma(\mathbb{F}_{81}) \supseteq \{0, 1, 2, 3, 4, 6, 8, 9, 12, 16, 36\}$.

New GAG-codes from maximal curves

Consider for $j = 1, \dots, 5$ the MDS code C_j over $\mathbb{F}_q$, $[2j-1, j, j]$.
For a curve $\mathcal{X}$ defined over $\mathbb{F}_q$, we have the GAG-code $C(P_1, \dots, P_r; G; C_1, \dots, C_r)$ denoted by

$$C(k, A_1, A_2, A_3, A_4, A_5)$$

were:

- $\deg(G) = k + g - 1$;
- $r = A_1 + A_2 + A_3 + A_4 + A_5$;
- A_j is the number of points in $\{P_1, \dots, P_r\}$ with degree j.

Remark

$C(k, A_1, A_2, A_3, A_4, A_5)$ is an $[n, k', d]$ code with $n = \sum_{i=1}^{5}(2j-1)A_j$, $k' \geq k$, $d \geq \sum_{i=1}^{5} jA_j - (k+g-1)$. By passing to a k-dimensional subspace of $C(k, A_1, A_2, A_3, A_4, A_5)$, an $[n, k, d]$ code can be obtained.

New GAG-codes from maximal curves

Consider for $j = 1, \dots, 5$ the MDS code C_j over $\mathbb{F}_q$, $[2j-1, j, j]$.
For a curve $\mathcal{X}$ defined over $\mathbb{F}_q$, we have the GAG-code $C(P_1, \dots, P_r; G; C_1, \dots, C_r)$ denoted by

$$C(k, A_1, A_2, A_3, A_4, A_5)$$

were:

- $\deg(G) = k + g - 1$;
- $r = A_1 + A_2 + A_3 + A_4 + A_5$;
- A_j is the number of points in $\{P_1, \dots, P_r\}$ with degree j.

Remark

$C(k, A_1, A_2, A_3, A_4, A_5)$ is an $[n, k', d]$ code with $n = \sum_{i=1}^{5}(2j-1)A_j$, $k' \geq k$, $d \geq \sum_{i=1}^{5} jA_j - (k+g-1)$. By passing to a k-dimensional subspace of $C(k, A_1, A_2, A_3, A_4, A_5)$, an $[n, k, d]$ code can be obtained.

New GAG-codes from maximal curves

$q = 49,\ g = 9 \quad \mathcal{X}\colon\ Y^4 = X^7 + X$
$B_1 = 176,\ B_i > 3$ for $i = 2, 3, 4, 5$.

Code	k	Parameters	d_{MinT}
$C(k; 176, 1, 0, 0, 0)$	$124 \leq k \leq 155$	$[179, k, d \geq 170 - k]$	$\leq 169 - k$
$C(k; 176, 2, 0, 0, 0)$	$127 \leq k \leq 156$	$[182, k, d \geq 172 - k]$	$\leq 171 - k$
$C(k; 176, 3, 0, 0, 0)$	$130 \leq k \leq 155$	$[185, k, d \geq 174 - k]$	$\leq 173 - k$
$C(k; 176, 4, 0, 0, 0)$	$133 \leq k \leq 156$	$[188, k, d \geq 176 - k]$	$\leq 175 - k$
$C(k; 176, 0, 1, 0, 0)$	$126 \leq k \leq 154$	$[181, k, d \geq 171 - k]$	$\leq 170 - k$
$C(k; 176, 0, 2, 0, 0)$	$131 \leq k \leq 154$	$[186, k, d \geq 174 - k]$	$\leq 173 - k$
$C(k; 176, 0, 0, 1, 0)$	$128 \leq k \leq 153$	$[183, k, d \geq 172 - k]$	$\leq 171 - k$
$C(k; 176, 0, 0, 2, 0)$	$135 \leq k \leq 153$	$[190, k, d \geq 176 - k]$	$\leq 175 - k$
$C(k; 176, 1, 1, 0, 0)$	$129 \leq k \leq 154$	$[184, k, d \geq 173 - k]$	$\leq 172 - k$
$C(k; 176, 1, 1, 1, 0)$	$136 \leq k \leq 154$	$[191, k, d \geq 177 - k]$	$\leq 176 - k$

Asymptotically good families of GAG-codes

Definition

A sequence of linear codes over $\mathbb{F}_q$, $(C_i)_i$, s.t. $n(C_i) \longrightarrow +\infty$, is asymptotically good if $R_i \longrightarrow R$ and $\delta_i \longrightarrow \delta$ for $i \longrightarrow +\infty$ are s.t. $R\delta > 0$, R_i is the information rate and δ_i the relative distance of C_n.

Goal: to determinate an explicit asymptotically good family of codes.

Asymptotically good families of GAG-codes

Lemma

Let m and r be positive integers with $r \leq m$. Then there exists a family of $q^m - 1$ injective $\mathbb{F}_q$-linear maps

$$\{\psi_w : \mathbb{F}_q^r \to \mathbb{F}_q^{m+r} \mid w \in \mathbb{F}_q^m, w \neq (0, \ldots, 0)\}$$

whose images have pairwise trivial intersection.

Fix $r > 0$, $\sigma : \mathbb{F}_{q^r} \to \mathbb{F}_q^r$ $\mathbb{F}_q$-linear isomorphism and a total order on $\mathbb{F}_q^r$, so $\mathbb{F}_q^r = \{0, w_1, \dots, w_{q^r-1}\}$.

- $\mathcal{X}$ curve of genus g
- $P_1, \dots, P_s \in \mathcal{X}$, $\deg P_i = r$ for all i
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \dots, P_s\} = \emptyset$
- C_i be the $[2r, r, d]$-code consisting of the vectors of $Im(\psi_{w_i})$
- $\pi_i : \mathbb{F}_{q^r} \to C_i$ be the $\mathbb{F}_q$-linear isomorphism mapping $\alpha \in \mathbb{F}_{q^r}$ to $\psi_{w_i}(\sigma(\alpha))$.

Asymptotically good families of GAG-codes

Fix $r > 0$, $\sigma : \mathbb{F}_{q^r} \to \mathbb{F}_q^r$ $\mathbb{F}_q$-linear isomorphism and a total order on $\mathbb{F}_q^r$, so $\mathbb{F}_q^r = \{0, w_1, \dots, w_{q^r-1}\}$.

- $\mathcal{X}$ curve of genus g
- $P_1, \dots, P_s \in \mathcal{X}$, $\deg P_i = r$ for all i
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \dots, P_s\} = \emptyset$
- C_i be the $[2r, r, d]$-code consisting of the vectors of $Im(\psi_{w_i})$
- $\pi_i : \mathbb{F}_{q^r} \to C_i$ be the $\mathbb{F}_q$-linear isomorphism mapping $\alpha \in \mathbb{F}_{q^r}$ to $\psi_{w_i}(\sigma(\alpha))$.

Asymptotically good families of GAG-codes

Fix $r > 0$, $\sigma : \mathbb{F}_{q^r} \to \mathbb{F}_q^r$ $\mathbb{F}_q$-linear isomorphism and a total order on $\mathbb{F}_q^r$, so $\mathbb{F}_q^r = \{0, w_1, \ldots, w_{q^r-1}\}$.

- $\mathcal{X}$ curve of genus g
- $P_1, \ldots, P_s \in \mathcal{X}$, $\deg P_i = r$ for all i
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \ldots, P_s\} = \emptyset$
- C_i be the $[2r, r, d]$-code consisting of the vectors of $Im(\psi_{w_i})$
- $\pi_i : \mathbb{F}_{q^r} \to C_i$ be the $\mathbb{F}_q$-linear isomorphism mapping $\alpha \in \mathbb{F}_{q^r}$ to $\psi_{w_i}(\sigma(\alpha))$.

Asymptotically good families of GAG-codes

Fix $r > 0$, $\sigma : \mathbb{F}_{q^r} \to \mathbb{F}_q^r$ $\mathbb{F}_q$-linear isomorphism and a total order on $\mathbb{F}_q^r$, so $\mathbb{F}_q^r = \{0, w_1, \ldots, w_{q^r-1}\}$.

- $\mathcal{X}$ curve of genus g
- $P_1, \ldots, P_s \in \mathcal{X}$, $\deg P_i = r$ for all i
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \ldots, P_s\} = \emptyset$
- C_i be the $[2r, r, d]$-code consisting of the vectors of $Im(\psi_{w_i})$
- $\pi_i : \mathbb{F}_{q^r} \to C_i$ be the $\mathbb{F}_q$-linear isomorphism mapping $\alpha \in \mathbb{F}_{q^r}$ to $\psi_{w_i}(\sigma(\alpha))$.

Asymptotically good families of GAG-codes

Fix $r > 0$, $\sigma : \mathbb{F}_{q^r} \to \mathbb{F}_q^r$ $\mathbb{F}_q$-linear isomorphism and a total order on $\mathbb{F}_q^r$, so $\mathbb{F}_q^r = \{0, w_1, \dots, w_{q^r-1}\}$.

- $\mathcal{X}$ curve of genus g
- $P_1, \dots, P_s \in \mathcal{X}$, $\deg P_i = r$ for all i
- $G \in Div_{\mathbb{F}_q}(\mathcal{X})$ s.t. $Supp(G) \cap \{P_1, \dots, P_s\} = \emptyset$
- C_i be the $[2r, r, d]$-code consisting of the vectors of $Im(\psi_{w_i})$
- $\pi_i : \mathbb{F}_{q^r} \to C_i$ be the $\mathbb{F}_q$-linear isomorphism mapping $\alpha \in \mathbb{F}_{q^r}$ to $\psi_{w_i}(\sigma(\alpha))$.

Asymptotically good families of GAG-codes

Theorem

Let q be any prime power. Let λ be any rational number such that $0 < \lambda < H_q^{-1}(1/2)$, fix $2H_q(\lambda) < \alpha < 1$. Put $s = q^{\alpha r}$ and $\deg(G) = sMr$ for some M with $0 < M < 1$. Defining with $C(\mathcal{X}, r, \alpha, M)$ the GAG-code

$$C(P_1, \dots, P_s; G; C_1, \dots, C_s).$$

Then

$$\mathcal{C} = \{C(\mathcal{X}, r, \alpha, M) \mid rM, r\lambda, q^{\alpha r} \text{ are all integers}\}$$

contains an asymptotically good family of q-ary GAG-codes with asymptotic rate $R \geq M/2$ and asymptotic relative distance $\delta \geq \lambda(1 - M)$.

Asymptotically good families of GAG-codes

Remark

With the AG-codes it is possible to determinate asymptotically good families of codes, whose parameters are better than the asymptotic Gilbert-Varshamov bound, but to construct a family of AG-codes it is necessary to determinate a family of curves which permit to construct the family.
Using the GAG-codes we can fix the curves and increase only the degree of the points.

Thank you for your attention!