Numerical Semigroups and Alegebraic Geometry Codes

Maria Bras-Amorós

CIMPA Research School
Algebraic Methods in Coding Theory
Ubatuba, July 3-7, 2017

Contents

One-point codes and their decoding

Linear codes

A linear code C of length n over the alphabet $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$.

Linear codes

A linear code C of length n over the alphabet $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$.

Its elements are called code words.

Linear codes

A linear code C of length n over the alphabet $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$.

Its elements are called code words.

The dimension k of the code is the dimension of C as a subspace of $\mathbb{F}_q^n$.

Linear codes

A linear code C of length n over the alphabet $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$.

Its elements are called code words.

The dimension k of the code is the dimension of C as a subspace of $\mathbb{F}_q^n$.

The dual code of C is $C^\perp = \{v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ for all } c \in C\}$.

Linear codes

A linear code C of length n over the alphabet $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$.

Its elements are called code words.

The dimension k of the code is the dimension of C as a subspace of $\mathbb{F}_q^n$.

The dual code of C is $C^\perp = \{v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ for all } c \in C\}$.

The Hamming distance between two vectors of the same length is the number of positions in which they differ.

Linear codes

A linear code C of length n over the alphabet $\mathbb{F}_q$ is a vector subspace of $\mathbb{F}_q^n$.

Its elements are called code words.

The dimension k of the code is the dimension of C as a subspace of $\mathbb{F}_q^n$.

The dual code of C is $C^\perp = \{v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ for all } c \in C\}$.

The Hamming distance between two vectors of the same length is the number of positions in which they differ.

The weight of a vector is the number of its non-zero components or, equivalently, its Hamming distance to the zero vector.

Linear codes

The minimum distance d of a linear code C is the minimum Hamming distance between two code words in C.

Linear codes

The minimum distance d of a linear code C is the minimum Hamming distance between two code words in C.

Equivalently, it is the minimum weight of all code words in C.

Linear codes

The minimum distance d of a linear code C is the minimum Hamming distance between two code words in C.

Equivalently, it is the minimum weight of all code words in C.

The correction capability of a code is the maximum number of errors that can be added to any code word, with the code word being still uniquely identifiable.

Linear codes

The minimum distance d of a linear code C is the minimum Hamming distance between two code words in C.

Equivalently, it is the minimum weight of all code words in C.

The correction capability of a code is the maximum number of errors that can be added to any code word, with the code word being still uniquely identifiable.

The correction capability of a linear code with minimum distance d is $\lfloor \frac{d-1}{2} \rfloor$.

One-point codes

Let $\mathcal{X}_F$ be defined over $\mathbb{F}_q$.

One-point codes

Let $\mathcal{X}_F$ be defined over $\mathbb{F}_q$.

Let $P \in \mathcal{X}_F$,

One-point codes

Let $\mathcal{X}_F$ be defined over $\mathbb{F}_q$.

Let $P \in \mathcal{X}_F$, with Weierstrass semigroup $\Lambda = \{\lambda_0 = 0, \lambda_1, \ldots\}$.

One-point codes

Let $\mathcal{X}_F$ be defined over $\mathbb{F}_q$.

Let $P \in \mathcal{X}_F$, with Weierstrass semigroup $\Lambda = \{\lambda_0 = 0, \lambda_1, \ldots\}$.

Let $A = \bigcup_{m \geqslant 0} L(mP)$.

One-point codes

Let $\mathcal{X}_F$ be defined over $\mathbb{F}_q$.

Let $P \in \mathcal{X}_F$, with Weierstrass semigroup $\Lambda = \{\lambda_0 = 0, \lambda_1, \dots\}$.

Let $A = \bigcup_{m \geqslant 0} L(mP)$.

The order of $f \in A \setminus \{0\}$ is $\rho(f) = s$ if $v_P(f) = -\lambda_s$

One-point codes

Let $\mathcal{X}_F$ be defined over $\mathbb{F}_q$.

Let $P \in \mathcal{X}_F$, with Weierstrass semigroup $\Lambda = \{\lambda_0 = 0, \lambda_1, \dots\}$.

Let $A = \bigcup_{m \geqslant 0} L(mP)$.

The order of $f \in A \setminus \{0\}$ is $\rho(f) = s$ if $v_P(f) = -\lambda_s$
($\rho(0) = -1$).

One-point codes

Let $\mathcal{X}_F$ be defined over $\mathbb{F}_q$.

Let $P \in \mathcal{X}_F$, with Weierstrass semigroup $\Lambda = \{\lambda_0 = 0, \lambda_1, \ldots\}$.

Let $A = \bigcup_{m \geqslant 0} L(mP)$.

The order of $f \in A \setminus \{0\}$ is $\rho(f) = s$ if $v_P(f) = -\lambda_s$
$(\rho(0) = -1)$.

There exists an infinite basis $z_0, z_1, \ldots$ of A with $v_P(z_i) = -\lambda_i$
$(\rho(z_i) = i)$.

One-point codes

Let $\mathcal{X}_F$ be defined over $\mathbb{F}_q$.

Let $P \in \mathcal{X}_F$, with Weierstrass semigroup $\Lambda = \{\lambda_0 = 0, \lambda_1, \dots\}$.

Let $A = \bigcup_{m \geqslant 0} L(mP)$.

The order of $f \in A \setminus \{0\}$ is $\rho(f) = s$ if $v_P(f) = -\lambda_s$
($\rho(0) = -1$).

There exists an infinite basis $z_0, z_1, \dots$ of A with $v_P(z_i) = -\lambda_i$
($\rho(z_i) = i$).

For $P_1, \dots, P_n \in \mathcal{X}_F \setminus P$ let

$$\begin{array}{rccc} ev: & A & \longrightarrow & \mathbb{F}_q{}^n \\ & ev(f) & = & (f(P_1), \dots, f(P_n)) \end{array}$$

Exercise

Consider the Hermitian curve $\mathcal{H}_2$

- What is the Weierstrass semigroup at P_∞?
- Find a basis $z_0, z_1, \ldots$ of A with $v_P(z_i) = -\lambda_i$
- Find the matrix $\begin{pmatrix} ev(z_0) \\ ev(z_1) \\ ev(z_2) \\ \vdots \end{pmatrix}$ for the points $P_1 = (0:0:1) \equiv (0,0), P_2 = (0:1:1) \equiv (0,1), P_3 = (1:\alpha:1) \equiv (1,\alpha), P_4 = (1:\alpha^2:1) \equiv (1,\alpha^2), P_5 = (\alpha:\alpha:1) \equiv (\alpha,\alpha), P_6 = (\alpha:\alpha^2:1) \equiv (\alpha,\alpha^2), P_7 = (\alpha^2:\alpha:1) \equiv (\alpha^2,\alpha), P_8 = (\alpha^2:\alpha^2:1) \equiv (\alpha^2,\alpha^2)$

Exercise

Consider the Hermitian curve $\mathcal{H}_2$

- What is the Weierstrass semigroup at P_∞? $\{0, 2, 3, 4, 5 \dots\}$
- Find a basis $z_0, z_1, \dots$ of A with $v_P(z_i) = -\lambda_i$
  $z_0 = 1, z_1 = x, z_2 = y, z_3 = x^2, z_4 = xy, z_5 = x^3, z_6 = x^2y, z_7 = x^4, z_8 = x^3y, z_9 = x^5, \dots$
- Find the matrix $\begin{pmatrix} ev(z_0) \\ ev(z_1) \\ ev(z_2) \\ \vdots \end{pmatrix}$ for the points
  $P_1 = (0:0:1) \equiv (0,0), P_2 = (0:1:1) \equiv (0,1), P_3 = (1:\alpha:1) \equiv (1,\alpha), P_4 = (1:\alpha^2:1) \equiv (1,\alpha^2), P_5 = (\alpha:\alpha:1) \equiv (\alpha,\alpha), P_6 = (\alpha:\alpha^2:1) \equiv (\alpha,\alpha^2), P_7 = (\alpha^2:\alpha:1) \equiv (\alpha^2,\alpha), P_8 = (\alpha^2:\alpha^2:1) \equiv (\alpha^2,\alpha^2)$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha^2 & \alpha & \alpha \\ 0 & 0 & \alpha & \alpha^2 & \alpha^2 & 1 & 1 & \alpha \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ & & & \vdots & & & & \end{pmatrix}$$

One-point codes

For $W \subseteq \mathbb{N}_0$ define the one-point code

$$C_W = < ev(z_i) : i \in W >^{\perp} = < (z_i(P_1), \ldots, z_i(P_n)) : i \in W >^{\perp} .$$

One-point codes

For $W \subseteq \mathbb{N}_0$ define the one-point code

$$C_W = < ev(z_i) : i \in W >^{\perp} = < (z_i(P_1), \ldots, z_i(P_n)) : i \in W >^{\perp} .$$

We say that W is the set of parity checks of C_W.

One-point codes

For $W \subseteq \mathbb{N}_0$ define the one-point code

$$C_W =< ev(z_i) : i \in W >^{\perp} =< (z_i(P_1), \dots, z_i(P_n)) : i \in W >^{\perp} .$$

We say that W is the set of parity checks of C_W.

Example

Following the previous exercise, $C_{\{0,2,5\}}$ is the linear code over $\mathbb{F}_4$ with parity check matrix $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha^2 & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$

One-point codes

For $W \subseteq \mathbb{N}_0$ define the one-point code

$$C_W =< ev(z_i) : i \in W >^{\perp} =< (z_i(P_1), \ldots, z_i(P_n)) : i \in W >^{\perp} .$$

We say that W is the set of parity checks of C_W.

Example

Following the previous exercise, $C_{\{0,2,5\}}$ is the linear code over $\mathbb{F}_4$ with parity check matrix $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha^2 & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$

The one-point codes for which $W = \{0, 1, \ldots, m\}$ are called classical one-point codes. In this case we write C_m for C_W.

Decoding one-point codes

Let $c \in C_W$, $u = c + e$, $t = \text{weight}(e)$.

Decoding one-point codes

Let $c \in C_W$, $u = c + e$, $t = \text{weight}(e)$.

Definition

A polynomial f is an error-locator of e if $f(P_i) = 0$ whenever $e_i \neq 0$.

Decoding one-point codes

Let $c \in C_W$, $u = c + e$, $t = \text{weight}(e)$.

Definition

A polynomial f is an error-locator of e if $f(P_i) = 0$ whenever $e_i \neq 0$.

The footprint of e is the set $\Delta_e = \mathbb{N}_0 \setminus \{\rho(f) : f \text{ is an error-locator}\}$.

Decoding one-point codes

Let $c \in C_W$, $u = c + e$, $t = \text{weight}(e)$.

Definition

A polynomial f is an error-locator of e if $f(P_i) = 0$ whenever $e_i \neq 0$.

The footprint of e is the set $\Delta_e = \mathbb{N}_0 \setminus \{\rho(f) : f \text{ is an error-locator}\}$.

Lemma

$\#\Delta_e = t$.

Decoding one-point codes

Definition

The kth syndrome of e is the vector e times the kth row of the parity check matrix, that is,

$$s_k = \begin{pmatrix} z_k(P_1) & z_k(P_2) & \dots & z_k(P_n) \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = \sum_{l=1}^{n} z_k(P_l) e_l.$$

Decoding one-point codes

Definition

The kth syndrome of e is the vector e times the kth row of the parity check matrix, that is,

$$s_k = \begin{pmatrix} z_k(P_1) & z_k(P_2) & \dots & z_k(P_n) \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = \sum_{l=1}^{n} z_k(P_l) e_l.$$

For correcting u we need a number of syndromes.

Decoding one-point codes

If $k \in W$, then s_k is known since

$$s_k = \sum_{l=1}^{n} z_k(P_l)e_l = \sum_{l=1}^{n} z_k(P_l)u_l - \sum_{l=1}^{n} z_k(P_l)c_l = \sum_{l=1}^{n} z_k(P_l)u_l.$$

Decoding one-point codes

If $k \in W$, then s_k is known since

$$s_k = \sum_{l=1}^{n} z_k(P_l)e_l = \sum_{l=1}^{n} z_k(P_l)u_l - \sum_{l=1}^{n} z_k(P_l)c_l = \sum_{l=1}^{n} z_k(P_l)u_l.$$

Otherwise, s_k can be obtained through the so-called majority voting if the majority voting condition holds:

$$\nu_k > 2\#(D(k) \cap \Delta_e),$$

where $D(k) = \{j \in \mathbb{N}_0 : \lambda_k - \lambda_j \in \Lambda\}$ $(\#D(k) = \nu_k)$.

Decoding one-point codes

If $k \in W$, then s_k is known since

$$s_k = \sum_{l=1}^{n} z_k(P_l)e_l = \sum_{l=1}^{n} z_k(P_l)u_l - \sum_{l=1}^{n} z_k(P_l)c_l = \sum_{l=1}^{n} z_k(P_l)u_l.$$

Otherwise, s_k can be obtained through the so-called majority voting if the majority voting condition holds:

$$\nu_k > 2\#(D(k) \cap \Delta_e),$$

where $D(k) = \{j \in \mathbb{N}_0 : \lambda_k - \lambda_j \in \Lambda\}$ $(\#D(k) = \nu_k)$.

Theorem

If $\nu_i > 2\#(D(i) \cap \Delta_e)$ for all $i \notin W$ then e is correctable by C_W.

The ν sequence, classical codes, and Feng-Rao improved codes

Order bound on the minimum distance

From the equality $\#\Delta_e = t$ we deduce the next lemma.

Lemma

If the number t of errors in e satisfies $t \leqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$, then $\nu_i > 2\#(D(i) \cap \Delta_e)$.

Order bound on the minimum distance

From the equality $\#\Delta_e = t$ we deduce the next lemma.

Lemma

If the number t of errors in e satisfies $t \leqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$, then $\nu_i > 2\#(D(i) \cap \Delta_e)$.

Definition

The order (or Feng-Rao) bound on the minimum distance of C_m is

$$d_{ORD}(C_m) = \min\{\nu_i : i > m\}.$$

Order bound on the minimum distance

From the equality $\#\Delta_e = t$ we deduce the next lemma.

Lemma

If the number t of errors in e satisfies $t \leqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$, then $\nu_i > 2\#(D(i) \cap \Delta_e)$.

Definition

The order (or Feng-Rao) bound on the minimum distance of C_m is

$$d_{ORD}(C_m) = \min\{\nu_i : i > m\}.$$

Lemma

$$d(C_m) \geqslant d_{ORD}(C_m).$$

Order bound on the minimum distance

Definition

A refined version of the order bound is

$$d_{ORD}^{P_1,\ldots,P_n}(C_m) = \min\{\nu_i : i > m, C_i \neq C_{i+1}\}.$$

Order bound on the minimum distance

Definition

A refined version of the order bound is

$$d_{ORD}^{P_1,\dots,P_n}(C_m) = \min\{\nu_i : i > m, C_i \neq C_{i+1}\}.$$

While d_{ORD} only depends on the Weierstrass semigroup, $d_{ORD}^{P_1,\dots,P_n}$ depends also on the points $P_1, \dots, P_n$.

Order bound on the minimum distance

Lemma

If $i \geqslant 2c - g - 1$ *(equiv. to lambda*$_i \geqslant 2c - 1$*), then* $\nu_{i+1} \leqslant \nu_{i+2}$.

Order bound on the minimum distance

Lemma

If $i \geqslant 2c - g - 1$ (equiv. to lambda$_i \geqslant 2c - 1$), then $\nu_{i+1} \leqslant \nu_{i+2}$.

Consequently, $d_{ORD}(C_i) = \nu_{i+1}$ for all $i \geqslant 2c - g - 1$.

Order bound on the minimum distance

Aim: smallest m for which $d_{ORD}(C_i) = \nu_{i+1}$ for all $i \geqslant m$.

Order bound on the minimum distance

Aim: smallest m for which $d_{ORD}(C_i) = \nu_{i+1}$ for all $i \geqslant m$.

For a non-ordinary semigroup $\Lambda = [0] \cup [c_k, d_k] \cup \cdots \cup [c_1, d_1] \cup [c_0, \infty)$ define the conductor $c = c_0$, the subconductor $c' = c_1$, the dominant $d = d_1$, and the subdominant $d' = d_2$.

Order bound on the minimum distance

Aim: smallest m for which $d_{ORD}(C_i) = \nu_{i+1}$ for all $i \geqslant m$.

For a non-ordinary semigroup $\Lambda = [0] \cup [c_k, d_k] \cup \cdots \cup [c_1, d_1] \cup [c_0, \infty)$ define the conductor $c = c_0$, the subconductor $c' = c_1$, the dominant $d = d_1$, and the subdominant $d' = d_2$.

Theorem

Let Λ be a non-ordinary acute semigroup and let

$$m = \min\{\lambda^{-1}(c + c' - 2), \lambda^{-1}(2d)\}. \quad (1)$$

Then,

1. $\nu_m > \nu_{m+1}$
2. $\nu_i \leqslant \nu_{i+1}$ *for all* $i > m$.

Order bound on the minimum distance

Corollary

Let Λ be a non-ordinary acute numerical semigroup and let

$$m = \min\{\lambda^{-1}(c + c' - 2), \lambda^{-1}(2d)\}.$$

Then, m is the smallest integer for which

$$d_{ORD}(C_i) = \nu_{i+1}$$

for all $i \geqslant m$.

Example with the Klein quartic

i	λ_i	ν_i	$d_{ORD}(C_i)$
0	0	1	2
1	3	2	2
2	5	2	2
3	6	3	2
4	7	2	4
5	8	4	4
6	9	4	5
7	10	5	6
8	11	6	7
9	12	7	8

Example with the Klein quartic

i	λ_i	ν_i	$d_{ORD}(C_i)$
0	0	1	2
1	3	2	2
2	5	2	2
3	6	3	2
4	7	2	4
5	8	4	4
6	9	4	5
7	10	5	6
8	11	6	7
9	12	7	8

In this example, $c = 5$, $d = 3$ and $c' = 3$.

Example with the Klein quartic

i	λ_i	ν_i	$d_{ORD}(C_i)$
0	0	1	2
1	3	2	2
2	5	2	2
3	6	3	2
4	7	2	4
5	8	4	4
6	9	4	5
7	10	5	6
8	11	6	7
9	12	7	8

In this example, $c = 5$, $d = 3$ and $c' = 3$.

So, $\lambda^{-1}(c + c' - 2) = \lambda^{-1}(2d) = 3$

Example with the Klein quartic

i	λ_i	ν_i	$d_{ORD}(C_i)$
0	0	1	2
1	3	2	2
2	5	2	2
3	6	3	2
4	7	2	4
5	8	4	4
6	9	4	5
7	10	5	6
8	11	6	7
9	12	7	8

In this example, $c = 5$, $d = 3$ and $c' = 3$.

So, $\lambda^{-1}(c + c' - 2) = \lambda^{-1}(2d) = 3$

and $m = \min\{\lambda^{-1}(c + c' - 2), \lambda^{-1}(2d)\} = 3$.

Example with the Hermitian curve

i	λ_i	ν_i	$d_{ORD}(C_i)$
0	0	1	2
1	4	2	2
2	5	2	3
3	8	3	3
4	9	4	3
5	10	3	4
6	12	4	4
7	13	6	4
8	14	6	4
9	15	4	5
10	16	5	8
11	17	8	8
12	18	9	8
13	19	8	9
14	20	9	10
15	21	10	12
16	22	12	12
17	23	12	13
18	24	13	14
19	25	14	15
20	26	15	16

In this case $c = 12$, $d = 10$, $c' = 8$. $\lambda^{-1}(c + c' - 2) = 12$ and $\lambda^{-1}(2d) = 14$. So $m = 12$ is largest with $\nu_m > \nu_{m+1}$ and with $d_{ORD}(C_i) = \nu_{i+1}$ for all $i \geqslant m$.

Extending to near-acute semigroups

Munuera and Torres, and Oneto and Tamone proved that for *any* numerical semigroup

$$m \leqslant \min\{\lambda^{-1}(c + c' - 2 - g), \lambda^{-1}(2d - g)\}.$$

Extending to near-acute semigroups

Munuera and Torres, and Oneto and Tamone proved that for *any* numerical semigroup

$$m \leqslant \min\{\lambda^{-1}(c+c'-2-g), \lambda^{-1}(2d-g)\}.$$

Notice that for acute semigroups this inequality is an equality.

Extending to near-acute semigroups

Munuera and Torres, and Oneto and Tamone proved that for *any* numerical semigroup

$$m \leqslant \min\{\lambda^{-1}(c + c' - 2 - g), \lambda^{-1}(2d - g)\}.$$

Notice that for acute semigroups this inequality is an equality.

Munuera and Torres proved that the formula $m = \min\{\lambda^{-1}(c + c' - 2 - g), \lambda^{-1}(2d - g)\}$ not only applies for acute semigroups but also for near-acute semigroups.

Definition

[Munuera, Torres] A numerical semigroup with conductor c, dominant d and subdominant d' is said to be a near-acute semigroup if either $c - d \leqslant d - d'$ or $2d - c + 1 \notin \Lambda$.

Extending to near-acute semigroups

Oneto and Tamone proved that
$m = \min\{\lambda^{-1}(c + c' - 2 - g), \lambda^{-1}(2d - g)\}$ if and *only if* $c + c' - 2 \leqslant 2d$ or $2d - c + 1 \notin \Lambda$.

Extending to near-acute semigroups

Oneto and Tamone proved that
$m = \min\{\lambda^{-1}(c + c' - 2 - g), \lambda^{-1}(2d - g)\}$ if and *only if* $c + c' - 2 \leqslant 2d$ or $2d - c + 1 \notin \Lambda$.

Lemma

For a numerical semigroup the following are equivalent

1. $c - d \leqslant d - d'$ *or* $2d - c + 1 \notin \Lambda$ *(near-acute condition),*
2. $c + c' - 2 \leqslant 2d$ *or* $2d - c + 1 \notin \Lambda$.

Extending to near-acute semigroups

Oneto and Tamone proved that
$m = \min\{\lambda^{-1}(c + c' - 2 - g), \lambda^{-1}(2d - g)\}$ if and *only if* $c + c' - 2 \leqslant 2d$ or $2d - c + 1 \notin \Lambda$.

Lemma

For a numerical semigroup the following are equivalent

1. $c - d \leqslant d - d'$ *or* $2d - c + 1 \notin \Lambda$ *(near-acute condition)*,
2. $c + c' - 2 \leqslant 2d$ *or* $2d - c + 1 \notin \Lambda$.

Proof: Let us see first that (1) implies (2). If $2d - c + 1 \notin \Lambda$ then it is obvious. Otherwise the condition $c - d \leqslant d - d'$ is equivalent to $d' \leqslant 2d - c$ which, together with $2d - c + 1 \in \Lambda$ implies $c' \leqslant 2d - c + 1$ by definition of c'. This in turn implies that $c + c' - 2 < c + c' - 1 \leqslant 2d$.

To see that (1) is a consequence of (2) notice that by definition, $d' \leqslant c' - 2$. Then, if $c + c' - 2 \leqslant 2d$, we have $d - d' \geqslant d - c' + 2 \geqslant c - d$.
□

Extending to near-acute semigroups

One concludes the next theorem.

Theorem (Munuera, Torres, Oneto, Tamone)

1. *For* any *numerical semigroup* $m \leqslant \min\{\lambda^{-1}(c+c'-2-g), \lambda^{-1}(2d-g)\}$.
2. $m = \min\{\lambda^{-1}(c+c'-2-g), \lambda^{-1}(2d-g)\}$ *if and only if the corresponding numerical semigroup is near-acute.*

Extending to near-acute semigroups

One concludes the next theorem.

Theorem (Munuera, Torres, Oneto, Tamone)

1. *For* any *numerical semigroup* $m \leqslant \min\{\lambda^{-1}(c + c' - 2 - g), \lambda^{-1}(2d - g)\}$.
2. $m = \min\{\lambda^{-1}(c + c' - 2 - g), \lambda^{-1}(2d - g)\}$ *if and only if the corresponding numerical semigroup is near-acute.*

Conjecture (Oneto, Tamone)

For any numerical semigroup,

$$m \geqslant \lambda^{-1}(c + d - g - \lambda_1).$$

Feng-Rao improved codes

Recall that if $t \leqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all $i \notin W$ then e is correctable by C_W.

Definition

Given a rational point P of an algebraic smooth curve $\mathcal{X}_F$ defined over $\mathbb{F}_q$ with Weierstrass semigroup Λ and sequence ν with associated basis $z_0, z_1, \ldots$ and given n other different points $P_1, \ldots, P_n$ of $\mathcal{X}_F$, the associated Feng-Rao improved code guaranteeing correction of t errors is defined as

$$C_{\tilde{R}(t)} = < (z_i(P_1), \ldots, z_i(P_n)) : i \in \tilde{R}(t) >^{\perp},$$

where

$$\tilde{R}(t) = \{i \in \mathbb{N}_0 : \nu_i < 2t + 1\}.$$

Feng-Rao improved codes

Recall that if $t \leqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all $i \notin W$ then e is correctable by C_W.

Definition

Given a rational point P of an algebraic smooth curve $\mathcal{X}_F$ defined over $\mathbb{F}_q$ with Weierstrass semigroup Λ and sequence ν with associated basis $z_0, z_1, \ldots$ and given n other different points $P_1, \ldots, P_n$ of $\mathcal{X}_F$, the associated Feng-Rao improved code guaranteeing correction of t errors is defined as

$$C_{\tilde{R}(t)} = < (z_i(P_1), \ldots, z_i(P_n)) : i \in \tilde{R}(t) >^{\perp},$$

where

$$\tilde{R}(t) = \{i \in \mathbb{N}_0 : \nu_i < 2t + 1\}.$$

Feng-Rao improved codes will actually improve classical codes only if ν_i is decreasing at some i. So, we are interested in the monotonicity of ν_i.

Lemma

If Λ is an ordinary numerical semigroup with enumeration λ then

$$\nu_i = \begin{cases} 1 & \text{if } i = 0, \\ 2 & \text{if } 1 \leqslant i \leqslant \lambda_1, \\ i - \lambda_1 + 2 & \text{if } i > \lambda_1. \end{cases}$$

Lemma

If Λ is an ordinary numerical semigroup with enumeration λ then

$$\nu_i = \begin{cases} 1 & \text{if } i = 0, \\ 2 & \text{if } 1 \leqslant i \leqslant \lambda_1, \\ i - \lambda_1 + 2 & \text{if } i > \lambda_1. \end{cases}$$

Proof: It is obvious that $\nu_0 = 1$ and that $\nu_i = 2$ whenever $0 < \lambda_i < 2\lambda_1$. So, since $2\lambda_1 = \lambda_{\lambda_1+1}$, we have that $\nu_i = 2$ for all $1 \leqslant i \leqslant \lambda_1$. Finally, if $\lambda_i \geqslant 2\lambda_1$ then all non-gaps up to $\lambda_i - \lambda_1$ are in $D(i)$ as well as λ_i, and none of the remaining non-gaps are in $D(i)$. Now, if the genus of Λ is g, then $\nu_i = \lambda_i - \lambda_1 + 2 - g$ and $\lambda_i = i + g$. So, $\nu_i = i - \lambda_1 + 2$. □

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Notice that if **(i)** is satisfied for all i, then $\{j \in \mathbb{N}_0 : j \leqslant i\} \subseteq D(\lambda^{-1}(2\lambda_i))$ for all i, and hence Λ is Arf (Campillo, Farran, Munuera).

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

If $i = 0$ ok.

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Suppose $i > 0$.

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Suppose $i > 0$. By the induction hypothesis, $\nu_{\lambda^{-1}(\lambda_{i-1}+\lambda_i)} = 2i$.

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Suppose $i > 0$. By the induction hypothesis, $\nu_{\lambda^{-1}(\lambda_{i-1}+\lambda_i)} = 2i$.

(ν_i) not decreasing and $2\lambda_i > \lambda_{i-1} + \lambda_i$, $\Rightarrow \nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i$.

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Suppose $i > 0$. By the induction hypothesis, $\nu_{\lambda^{-1}(\lambda_{i-1}+\lambda_i)} = 2i$.

(ν_i) not decreasing and $2\lambda_i > \lambda_{i-1} + \lambda_i$, $\Rightarrow \nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i$.

If $j \leqslant k$ satisfy $\lambda_j + \lambda_k = 2\lambda_i$ then $\lambda_j \leqslant \lambda_i$ and $\lambda_k \geqslant \lambda_i$.

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Suppose $i > 0$. By the induction hypothesis, $\nu_{\lambda^{-1}(\lambda_{i-1}+\lambda_i)} = 2i$.

(ν_i) not decreasing and $2\lambda_i > \lambda_{i-1} + \lambda_i$, $\Rightarrow \nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i$.

If $j \leqslant k$ satisfy $\lambda_j + \lambda_k = 2\lambda_i$ then $\lambda_j \leqslant \lambda_i$ and $\lambda_k \geqslant \lambda_i$.

Consequently, $\lambda(D(\lambda^{-1}(2\lambda_i))) \subseteq \{\lambda_j : 0 \leqslant j \leqslant i\} \sqcup \{2\lambda_i - \lambda_j : 0 \leqslant j < i\}$ and

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Suppose $i > 0$. By the induction hypothesis, $\nu_{\lambda^{-1}(\lambda_{i-1}+\lambda_i)} = 2i$.

(ν_i) not decreasing and $2\lambda_i > \lambda_{i-1} + \lambda_i$, $\Rightarrow \nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i$.

If $j \leqslant k$ satisfy $\lambda_j + \lambda_k = 2\lambda_i$ then $\lambda_j \leqslant \lambda_i$ and $\lambda_k \geqslant \lambda_i$.

Consequently, $\lambda(D(\lambda^{-1}(2\lambda_i))) \subseteq \{\lambda_j : 0 \leqslant j \leqslant i\} \sqcup \{2\lambda_i - \lambda_j : 0 \leqslant j < i\}$ and

$\nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i \Leftrightarrow D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$.

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

(i) $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,

(ii) $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Suppose $i > 0$. By the induction hypothesis, $\nu_{\lambda^{-1}(\lambda_{i-1}+\lambda_i)} = 2i$.

(ν_i) not decreasing and $2\lambda_i > \lambda_{i-1} + \lambda_i, \Rightarrow \nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i$.

If $j \leqslant k$ satisfy $\lambda_j + \lambda_k = 2\lambda_i$ then $\lambda_j \leqslant \lambda_i$ and $\lambda_k \geqslant \lambda_i$.

Consequently, $\lambda(D(\lambda^{-1}(2\lambda_i))) \subseteq \{\lambda_j : 0 \leqslant j \leqslant i\} \sqcup \{2\lambda_i - \lambda_j : 0 \leqslant j < i\}$ and

$\nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i \Leftrightarrow D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$.

This proves **(i)**.

On the improvement of Feng-Rao improved codes

Lemma

If ν is non-decreasing then Λ is Arf.

Proof: Let λ be the enumeration of Λ. Let us see by induction on i that

- **(i)** $D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$,
- **(ii)** $D(\lambda^{-1}(\lambda_i + \lambda_{i+1})) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(\lambda_i + \lambda_{i+1} - \lambda_j) : 0 \leqslant j \leqslant i\}$.

Suppose $i > 0$. By the induction hypothesis, $\nu_{\lambda^{-1}(\lambda_{i-1}+\lambda_i)} = 2i$.

(ν_i) not decreasing and $2\lambda_i > \lambda_{i-1} + \lambda_i$, $\Rightarrow \nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i$.

If $j \leqslant k$ satisfy $\lambda_j + \lambda_k = 2\lambda_i$ then $\lambda_j \leqslant \lambda_i$ and $\lambda_k \geqslant \lambda_i$.

Consequently, $\lambda(D(\lambda^{-1}(2\lambda_i))) \subseteq \{\lambda_j : 0 \leqslant j \leqslant i\} \sqcup \{2\lambda_i - \lambda_j : 0 \leqslant j < i\}$ and

$\nu_{\lambda^{-1}(2\lambda_i)} \geqslant 2i \Leftrightarrow D(\lambda^{-1}(2\lambda_i)) = \{j \in \mathbb{N}_0 : j \leqslant i\} \sqcup \{\lambda^{-1}(2\lambda_i - \lambda_j) : 0 \leqslant j < i\}$.

This proves **(i)**.

Finally, **(i)** implies $\nu_{\lambda^{-1}(2\lambda_i)} = 2i + 1$ and **(ii)** follows by an analogous argumentation.

Theorem

The unique numerical semigroups for which the ν sequence is non-decreasing are ordinary numerical semigroups.

On the improvement of Feng-Rao improved codes

Theorem

The unique numerical semigroups for which the ν sequence is non-decreasing are ordinary numerical semigroups.

Corollary

The unique numerical semigroup for which the ν sequence is strictly increasing is the trivial numerical semigroup.

On the improvement of Feng-Rao improved codes

Theorem

The unique numerical semigroups for which the ν sequence is non-decreasing are ordinary numerical semigroups.

Corollary

The unique numerical semigroup for which the ν sequence is strictly increasing is the trivial numerical semigroup.

The unique numerical semigroups for which the associated classical codes are not improved by the Feng-Rao improved codes, at least for one value of t, are the ordinary semigroups.

The τ sequence and codes guaranteeing correction of generic errors

Generic errors

Definition

The points $P_{i_1}, \ldots, P_{i_t}$ are generically distributed if no element $f \in A$, $f \neq 0$ generated by $z_0, \ldots, z_{t-1}$ vanishes in all of them.

Generic errors

Definition

The points $P_{i_1}, \ldots, P_{i_t}$ are generically distributed if no element $f \in A$, $f \neq 0$ generated by $z_0, \ldots, z_{t-1}$ vanishes in all of them.

Generic errors are those errors whose non-zero positions correspond to generically distributed points.

Generic errors

Definition

The points $P_{i_1}, \dots, P_{i_t}$ are generically distributed if no element $f \in A$, $f \neq 0$ generated by $z_0, \dots, z_{t-1}$ vanishes in all of them.

Generic errors are those errors whose non-zero positions correspond to generically distributed points.

Equivalently, e is generic if and only if $\Delta_e = \Delta_t := \{0, \dots, t-1\}$.

Generic errors

Definition

The points $P_{i_1}, \ldots, P_{i_t}$ are generically distributed if no element $f \in A$, $f \neq 0$ generated by $z_0, \ldots, z_{t-1}$ vanishes in all of them.

Generic errors are those errors whose non-zero positions correspond to generically distributed points.

Equivalently, e is generic if and only if $\Delta_e = \Delta_t := \{0, \ldots, t-1\}$.

Generic errors of weight t can be a very large portion of all possible errors of weight t [Hansen, 2001].

Generic errors

Definition

The points $P_{i_1}, \dots, P_{i_t}$ are generically distributed if no element $f \in A$, $f \neq 0$ generated by $z_0, \dots, z_{t-1}$ vanishes in all of them.

Generic errors are those errors whose non-zero positions correspond to generically distributed points.

Equivalently, e is generic if and only if $\Delta_e = \Delta_t := \{0, \dots, t-1\}$.

Generic errors of weight t can be a very large portion of all possible errors of weight t [Hansen, 2001].

By restricting the errors to be corrected to generic errors the decoding requirements become weaker and we are still able to correct almost all errors.

Example: generic sets of points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Recall $\mathcal{H}_q$ has affine equation $x^{q+1} = y^q + y$.

Example: generic sets of points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Recall $\mathcal{H}_q$ has affine equation $x^{q+1} = y^q + y$.

The unique point at infinity is $P_\infty = (0 : 1 : 0)$.

Example: generic sets of points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Recall $\mathcal{H}_q$ has affine equation $x^{q+1} = y^q + y$.

The unique point at infinity is $P_\infty = (0 : 1 : 0)$.

$b \in \mathbb{F}_q \Rightarrow b^q + b = Tr(b) = 0 \Rightarrow$ the unique affine point with $y = b$ is $(0, b)$.
There are a total of q points (a, b) with $b \in \mathbb{F}_q$.

Example: generic sets of points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Recall $\mathcal{H}_q$ has affine equation $x^{q+1} = y^q + y$.

The unique point at infinity is $P_\infty = (0:1:0)$.

$b \in \mathbb{F}_q \Rightarrow b^q + b = Tr(b) = 0 \Rightarrow$ the unique affine point with $y = b$ is $(0, b)$.
There are a total of q points (a, b) with $b \in \mathbb{F}_q$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow b^q + b = Tr(b) \in \mathbb{F}_q \setminus \{0\} \Rightarrow$ there are $q+1$ solutions of $x^{q+1} = b^q + b$.

Example: generic sets of points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Recall $\mathcal{H}_q$ has affine equation $x^{q+1} = y^q + y$.

The unique point at infinity is $P_\infty = (0:1:0)$.

$b \in \mathbb{F}_q \Rightarrow b^q + b = Tr(b) = 0 \Rightarrow$ the unique affine point with $y = b$ is $(0, b)$.
There are a total of q points (a, b) with $b \in \mathbb{F}_q$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow b^q + b = Tr(b) \in \mathbb{F}_q \setminus \{0\} \Rightarrow$ there are $q+1$ solutions of $x^{q+1} = b^q + b$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow$ there are $q+1$ different affine points with $y = b$.

Example: generic sets of points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Recall $\mathcal{H}_q$ has affine equation $x^{q+1} = y^q + y$.

The unique point at infinity is $P_\infty = (0 : 1 : 0)$.

$b \in \mathbb{F}_q \Rightarrow b^q + b = Tr(b) = 0 \Rightarrow$ the unique affine point with $y = b$ is $(0, b)$.
There are a total of q points (a, b) with $b \in \mathbb{F}_q$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow b^q + b = Tr(b) \in \mathbb{F}_q \setminus \{0\} \Rightarrow$ there are $q + 1$ solutions of $x^{q+1} = b^q + b$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow$ there are $q + 1$ different affine points with $y = b$.

There are a total of $(q^2 - q)(q + 1)$ points (a, b) with $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Example: generic sets of points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Recall $\mathcal{H}_q$ has affine equation $x^{q+1} = y^q + y$.

The unique point at infinity is $P_\infty = (0 : 1 : 0)$.

$b \in \mathbb{F}_q \Rightarrow b^q + b = Tr(b) = 0 \Rightarrow$ the unique affine point with $y = b$ is $(0, b)$.
There are a total of q points (a, b) with $b \in \mathbb{F}_q$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow b^q + b = Tr(b) \in \mathbb{F}_q \setminus \{0\} \Rightarrow$ there are $q + 1$ solutions of $x^{q+1} = b^q + b$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow$ there are $q + 1$ different affine points with $y = b$.

There are a total of $(q^2 - q)(q + 1)$ points (a, b) with $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Total number of affine points $= q + (q^2 - q)(q + 1) = q^3$.

Example: generic sets of points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Recall $\mathcal{H}_q$ has affine equation $x^{q+1} = y^q + y$.

The unique point at infinity is $P_\infty = (0 : 1 : 0)$.

$b \in \mathbb{F}_q \Rightarrow b^q + b = Tr(b) = 0 \Rightarrow$ the unique affine point with $y = b$ is $(0, b)$.
There are a total of q points (a, b) with $b \in \mathbb{F}_q$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow b^q + b = Tr(b) \in \mathbb{F}_q \setminus \{0\} \Rightarrow$ there are $q + 1$ solutions of $x^{q+1} = b^q + b$.

$b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \Rightarrow$ there are $q + 1$ different affine points with $y = b$.

There are a total of $(q^2 - q)(q + 1)$ points (a, b) with $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Total number of affine points $= q + (q^2 - q)(q + 1) = q^3$.

If we distinguish the point P_∞, we can take $z_0 = 1, z_1 = x, z_2 = y$, $z_3 = x^2, z_4 = xy, z_5 = y^2 \ldots$

Example: generic sets of TWO points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Non-generic sets of two points are pairs of points satisfying $x^{q+1} = y^q + y$ and simultaneously vanishing at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$.

Example: generic sets of TWO points in $\mathcal{H}_q$ $(x^{q+1} = y^q + y)$

Non-generic sets of two points are pairs of points satisfying $x^{q+1} = y^q + y$ and simultaneously vanishing at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$.

$x + a$ represents a line with q points.

Example: generic sets of TWO points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Non-generic sets of two points are pairs of points satisfying $x^{q+1} = y^q + y$ and simultaneously vanishing at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$.

$x + a$ represents a line with q points.

There are q^2 such lines.

Example: generic sets of TWO points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Non-generic sets of two points are pairs of points satisfying $x^{q+1} = y^q + y$ and simultaneously vanishing at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$.

$x + a$ represents a line with q points.

There are q^2 such lines.

There are a total of $q^2\binom{q}{2}$ pairs of colinear points over lines of the form $x + a$ and so $q^2\binom{q}{2}$ non-generic errors.

Example: generic sets of TWO points in $\mathcal{H}_q$ $(x^{q+1} = y^q + y)$

Non-generic sets of two points are pairs of points satisfying $x^{q+1} = y^q + y$ and simultaneously vanishing at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$.

$x + a$ represents a line with q points.

There are q^2 such lines.

There are a total of $q^2\binom{q}{2}$ pairs of colinear points over lines of the form $x + a$ and so $q^2\binom{q}{2}$ non-generic errors.

Consequently, the portion of non-generic errors of weight 2 is

$$\frac{q^2\binom{q}{2}}{\binom{q^3}{2}} = \frac{1}{q^2 + q + 1}.$$

Example: generic sets of THREE points in $\mathcal{H}_q$ $(x^{q+1} = y^q + y)$

A set of three points is non-generic if the points satisfy $x^{q+1} = y^q + y$ and simultaneously vanish at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$ or at $f = z_2 + az_1 + bz_0 = y + ax + b$ for some $a, b \in \mathbb{F}_{q^2}$.

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

A set of three points is non-generic if the points satisfy $x^{q+1} = y^q + y$ and simultaneously vanish at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$ or at $f = z_2 + az_1 + bz_0 = y + ax + b$ for some $a, b \in \mathbb{F}_{q^2}$.

lines of type 1:	$x + a$
number of lines of type 1:	q^2
number of points per line of type 1:	q

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

A set of three points is non-generic if the points satisfy $x^{q+1} = y^q + y$ and simultaneously vanish at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$ or at $f = z_2 + az_1 + bz_0 = y + ax + b$ for some $a, b \in \mathbb{F}_{q^2}$.

lines of type 1:	$x + a$
number of lines of type 1:	q^2
number of points per line of type 1:	q
lines of type 2:	$y + ax + b$ with $a^{q+1} = b^q + b$
number of lines of type 2:	q^3
number of points per line of type 2:	

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

A set of three points is non-generic if the points satisfy $x^{q+1} = y^q + y$ and simultaneously vanish at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$ or at $f = z_2 + az_1 + bz_0 = y + ax + b$ for some $a, b \in \mathbb{F}_{q^2}$.

lines of type 1:	$x + a$
number of lines of type 1:	q^2
number of points per line of type 1:	q
lines of type 2:	$y + ax + b$ with $a^{q+1} = b^q + b$
number of lines of type 2:	q^3
number of points per line of type 2:	
lines of type 3:	$y + ax + b$ with $a^{q+1} \neq b^q + b$
number of lines of type 3:	$q^4 - q^3$
number of points per line of type 3:	

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 2? ($y + ax + b$ with $a^{q+1} = b^q + b$)

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 2? ($y + ax + b$ with $a^{q+1} = b^q + b$)

A point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy
$x^{q+1} = (-ax - b)^q + (-ax - b) = -(ax)^q - ax - a^{q+1}$.

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 2? ($y + ax + b$ with $a^{q+1} = b^q + b$)

A point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy
$x^{q+1} = (-ax - b)^q + (-ax - b) = -(ax)^q - ax - a^{q+1}$.

Notice that
$(x+a^q)^{q+1} = (x+a^q)^q(x+a^q) = (x^q+a)(x+a^q) = x^{q+1}+x^qa^q+ax+a^{q+1}$.

Example: generic sets of THREE points in $\mathcal{H}_q$ $(x^{q+1} = y^q + y)$

Number of points of lines of type 2? $(y + ax + b$ with $a^{q+1} = b^q + b)$

A point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy
$x^{q+1} = (-ax - b)^q + (-ax - b) = -(ax)^q - ax - a^{q+1}$.

Notice that
$(x+a^q)^{q+1} = (x+a^q)^q(x+a^q) = (x^q+a)(x+a^q) = x^{q+1}+x^q a^q+ax+a^{q+1}$.

So, $x = -a^q$ is the unique solution to $x^{q+1} = -(ax)^q - ax - a^{q+1}$ and so the unique point of $\mathcal{H}_q$ on the line $y + ax + b$ is $(-a^q, a^{q+1} - b)$.

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 2? ($y + ax + b$ with $a^{q+1} = b^q + b$)

A point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy
$x^{q+1} = (-ax - b)^q + (-ax - b) = -(ax)^q - ax - a^{q+1}$.

Notice that
$(x+a^q)^{q+1} = (x+a^q)^q(x+a^q) = (x^q+a)(x+a^q) = x^{q+1}+x^q a^q+ax+a^{q+1}$.

So, $x = -a^q$ is the unique solution to $x^{q+1} = -(ax)^q - ax - a^{q+1}$ and so the unique point of $\mathcal{H}_q$ on the line $y + ax + b$ is $(-a^q, a^{q+1} - b)$.

Lines of type 2 have 1 point

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

A set of three points is non-generic if the points satisfy $x^{q+1} = y^q + y$ and simultaneously vanish at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$ or at $f = z_2 + az_1 + bz_0 = y + ax + b$ for some $a, b \in \mathbb{F}_{q^2}$.

lines of type 1:	$x + a$
number of lines of type 1:	q^2
number of points per line of type 1:	q
lines of type 2:	$y + ax + b$ with $a^{q+1} = b^q + b$
number of lines of type 2:	q^3
number of points per line of type 2:	1
lines of type 3:	$y + ax + b$ with $a^{q+1} \neq b^q + b$
number of lines of type 3:	$q^4 - q^3$
number of points per line of type 3:	

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 3? ($y + ax + b$ with $a^{q+1} \neq b^q + b$)

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 3? ($y + ax + b$ with $a^{q+1} \neq b^q + b$)

Counting argument:

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 3? ($y + ax + b$ with $a^{q+1} \neq b^q + b$)

Counting argument:

On one hand, a point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy $x^{q+1} = -(ax)^q - ax - b^q - b \Rightarrow$ at most $q + 1$ points.

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 3? ($y + ax + b$ with $a^{q+1} \neq b^q + b$)

Counting argument:

On one hand, a point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy $x^{q+1} = -(ax)^q - ax - b^q - b \Rightarrow$ at most $q + 1$ points.

On the other hand there are a total of $\binom{q^3}{2}$ pairs of affine points.

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 3? ($y + ax + b$ with $a^{q+1} \neq b^q + b$)

Counting argument:

On one hand, a point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy $x^{q+1} = -(ax)^q - ax - b^q - b \Rightarrow$ at most $q + 1$ points.

On the other hand there are a total of $\binom{q^3}{2}$ pairs of affine points.

Each pair meets only in one line.

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 3? ($y + ax + b$ with $a^{q+1} \neq b^q + b$)

Counting argument:

On one hand, a point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy $x^{q+1} = -(ax)^q - ax - b^q - b \Rightarrow$ at most $q + 1$ points.

On the other hand there are a total of $\binom{q^3}{2}$ pairs of affine points.

Each pair meets only in one line.

The number of pairs sharing lines of type 1 is $q^2\binom{q}{2}$, the number of pairs sharing lines of type 2 is 0 and the number of pairs sharing lines of type 3 is at most $q^3(q-1)\binom{q+1}{2}$, with equality only if all lines of type 3 have $q + 1$ points.

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

Number of points of lines of type 3? ($y + ax + b$ with $a^{q+1} \neq b^q + b$)

Counting argument:

On one hand, a point on $\mathcal{H}_q$ and on the line $y + ax + b$ must satisfy $x^{q+1} = -(ax)^q - ax - b^q - b \Rightarrow$ at most $q + 1$ points.

On the other hand there are a total of $\binom{q^3}{2}$ pairs of affine points.

Each pair meets only in one line.

The number of pairs sharing lines of type 1 is $q^2\binom{q}{2}$, the number of pairs sharing lines of type 2 is 0 and the number of pairs sharing lines of type 3 is at most $q^3(q-1)\binom{q+1}{2}$, with equality only if all lines of type 3 have $q + 1$ points.

Since $q^2\binom{q}{2} + q^3(q-1)\binom{q+1}{2} = \binom{q^3}{2}$, we deduce that all the lines of type 3 must have $q + 1$ points.

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

A set of three points is non-generic if the points satisfy $x^{q+1} = y^q + y$ and simultaneously vanish at $f = z_1 + az_0 = x + a$ for some $a \in \mathbb{F}_{q^2}$ or at $f = z_2 + az_1 + bz_0 = y + ax + b$ for some $a, b \in \mathbb{F}_{q^2}$.

lines of type 1:	$x + a$
number of lines of type 1:	q^2
number of points per line of type 1:	q
lines of type 2:	$y + ax + b$ with $a^{q+1} = b^q + b$
number of lines of type 2:	q^3
number of points per line of type 2:	1
lines of type 3:	$y + ax + b$ with $a^{q+1} \neq b^q + b$
number of lines of type 3:	$q^4 - q^3$
number of points per line of type 3:	$q + 1$

Example: generic sets of THREE points in $\mathcal{H}_q$ ($x^{q+1} = y^q + y$)

There are $q^2\binom{q}{3}$ sets of three points sharing a line of type 1 and $(q^4 - q^3)\binom{q+1}{3}$ sets of three points sharing a line of type 3.

The portion of non-generic errors of weight 3 is then

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

Conditions for correcting generic errors

Lemma

The following conditions are equivalent.

1. $\nu_k > 2\#(D(k) \cap \Delta_t)$,
2. $\tau_k \geqslant t$.

Conditions for correcting generic errors

Lemma

The following conditions are equivalent.

1. $\nu_k > 2\#(D(k) \cap \Delta_t)$,
2. $\tau_k \geqslant t$.

Proof: Suppose $D_{k,j} < t \leqslant D_{k,j+1}$

If $\tau_k < t$

$$D(k) = \{\underbrace{\overbrace{D_{k,1} < D_{k,2} < \cdots < D_{k,i} = \tau_k}^{\lceil \frac{\nu_k}{2} \rceil} \leqslant D_{k,i+1} < \cdots < D_{k,j}}_{D(k)\cap\Delta_t} < D_{k,j+1} \cdots < D_{k,\nu_k}\}$$

If $\tau_k \geqslant t$

$$D(k) = \{\underbrace{\overbrace{D_{k,1} < D_{k,2} < \cdots < D_{k,j}}_{D(k)\cap\Delta_t} < D_{k,j+1} \cdots < D_{k,i} = \tau_k}^{\lceil \frac{\nu_k}{2} \rceil} \leqslant \overbrace{D_{k,i+1} < \cdots < D_{k,\nu_k}}^{\lfloor \frac{\nu_k}{2} \rfloor}\}$$

Codes guaranteeing correction of generic errors

We have seen that if $t \leqslant \tau_i$ for all $i \notin W$ then e is correctable by C_W.

Codes guaranteeing correction of generic errors

We have seen that if $t \leqslant \tau_i$ for all $i \notin W$ then e is correctable by C_W.

Definition

Given a rational point P of an algebraic smooth curve $\mathcal{X}_F$ defined over $\mathbb{F}_q$ with Weierstrass semigroup Λ and sequence ν with associated basis $z_0, z_1, \ldots$ and given n other different points $P_1, \ldots, P_n$ of $\mathcal{X}_F$, the associated improved code guaranteeing correction of t generic errors is defined as

$$C_{\tilde{R}^*(t)} = < (z_i(P_1), \ldots, z_i(P_n)) : i \in \tilde{R}^*(t) >^{\perp},$$

where

$$\tilde{R}^*(t) = \{i \in \mathbb{N}_0 : \tau_i < t\}.$$

Comparison of improved codes and classical codes correcting generic errors

Definition

The classical evaluation code with maximum dimension correcting t generic errors is defined by the set of checks

$$R^*(t) = \{i \in \mathbb{N}_0 : i \leqslant m(t)\}$$

where $m(t) = \max\{i \in \mathbb{N}_0 : \tau_i < t\}$.

Comparison of improved codes and classical codes correcting generic errors

Definition

The classical evaluation code with maximum dimension correcting t generic errors is defined by the set of checks

$$R^*(t) = \{i \in \mathbb{N}_0 : i \leqslant m(t)\}$$

where $m(t) = \max\{i \in \mathbb{N}_0 : \tau_i < t\}$.

By studying the monotonicity of the τ sequence we can compare $\widetilde{R}^*(t)$ and $R^*(t)$ and the associated codes.

Monotonicity of τ

The τ sequence of $\mathbb{N}_0$ is

$$0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, \ldots$$

Monotonicity of τ

The τ sequence of $\mathbb{N}_0$ is

$$0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, \ldots$$

The τ sequence of the semigroup $\{0\} \cup [c, \infty)$ with $c > 0$ is

$$\overbrace{0, \ldots, 0}^{(c+1)}, 1, 1, 2, 2, 3, 3, 4, 4, \ldots$$

Monotonicity of τ

The τ sequence of $\mathbb{N}_0$ is

$$0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, \ldots$$

The τ sequence of the semigroup $\{0\} \cup [c, \infty)$ with $c > 0$ is

$$\overbrace{0, \ldots, 0}^{(c+1)}, 1, 1, 2, 2, 3, 3, 4, 4, \ldots$$

Lemma

For a non-ordinary semigroup with conductor c, genus g and dominant d (non-gap previous to c) let $m = \lambda^{-1}(2d)$. Then

- $\tau_m = c - g - 1 > \tau_{m+1}$
- $\tau_i \leqslant \tau_{i+1}$ *for all* $i > m$.

Comparison of improved codes and classical codes correcting generic errors

Corollary

1. *The unique numerical semigroups with non-decreasing τ sequence are ordinary semigroups.*

Comparison of improved codes and classical codes correcting generic errors

Corollary

1. *The unique numerical semigroups with non-decreasing τ sequence are ordinary semigroups.*
2. $\widetilde{R}^*(t) = R^*(t)$ *for all* $t \in \mathbb{N}_0$ *if and only if the associated numerical semigroup is ordinary.*

Comparison of improved codes correcting generic errors and Feng-Rao improved codes

Feng-Rao improved code correcting t errors:

$$C_{\tilde{R}(t)} =< (z_i(P_1), \ldots, z_i(P_n)) : i \in \tilde{R}(t) >^{\perp},$$

where

$$\tilde{R}(t) = \{i \in \mathbb{N}_0 : \left\lfloor \frac{\nu_i - 1}{2} \right\rfloor < t\}.$$

Comparison of improved codes correcting generic errors and Feng-Rao improved codes

Feng-Rao improved code correcting t errors:

$$C_{\tilde{R}(t)} = <(z_i(P_1), \ldots, z_i(P_n)) : i \in \tilde{R}(t) >^{\perp},$$

where

$$\tilde{R}(t) = \{i \in \mathbb{N}_0 : \left\lfloor \frac{\nu_i - 1}{2} \right\rfloor < t\}.$$

Improved code correcting t *generic* errors: is defined as

$$C_{\tilde{R}^*(t)} = <(z_i(P_1), \ldots, z_i(P_n)) : i \in \tilde{R}^*(t) >^{\perp},$$

where

$$\tilde{R}^*(t) = \{i \in \mathbb{N}_0 : \tau_i < t\}.$$

Comparing ν and τ

Lemma

- $\tau_i \geqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \in \mathbb{N}_0$
- $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \geqslant 2c - g - 1$
- $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \in \mathbb{N}_0$ *if and only if* Λ *is Arf.*

Comparing ν and τ

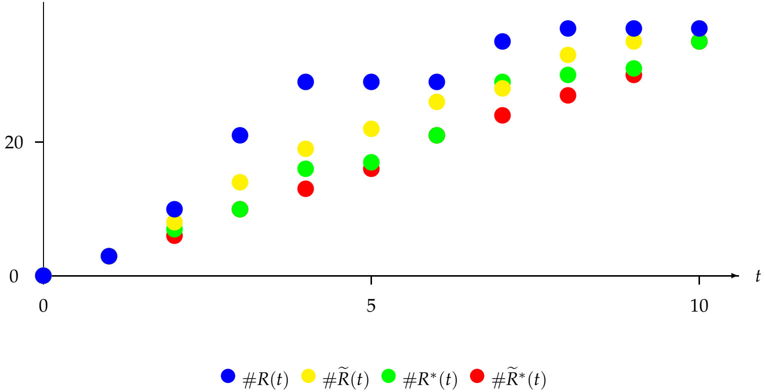
Lemma

- $\tau_i \geqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \in \mathbb{N}_0$
- $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \geqslant 2c - g - 1$
- $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \in \mathbb{N}_0$ *if and only if* Λ *is Arf.*

Corollary

1. $\widetilde{R}^*(t) \subseteq \widetilde{R}(t)$ *for all* $t \in \mathbb{N}_0$.
2. $\widetilde{R}^*(t) = \widetilde{R}(t)$ *for all* t *large enough.*
3. $\widetilde{R}^*(t) = \widetilde{R}(t)$ *for all* $t \in \mathbb{N}_0$ *if and only if the associated numerical semigroup is Arf.*

Hermitian Codes Redundancy ($\mathbb{F}_{7^2}$)



Exercise

Consider the numerical semigroup
$H = \{0, 12, 19, 24, 28, 31, 34, 36, 38, 40, 42, 43, 45, 46, 47, \ldots\}$.

Check that

- $\tau_i \geqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all $i \in \mathbb{N}_0$
- $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all $i \geqslant 2c - g - 1$

Exercise

Consider the numerical semigroup
$H = \{0, 12, 19, 24, 28, 31, 34, 36, 38, 40, 42, 43, 45, 46, 47, \ldots\}$.

Check that

- $\tau_i \geqslant \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all $i \in \mathbb{N}_0$
- $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all $i \geqslant 2c - g - 1$

i	λ_i	$\{\lambda_j : \lambda_i - \lambda_j \in \Lambda\}$	ν	τ
0	0	{0}	1	0
1	12	{0, 12}	2	0
2	19	{0, 19}	2	0
3	24	{0, 12, 24}	3	1
4	28	{0, 28}	2	0
5	31	{0, 12, 19, 31}	4	1
6	34	{0, 34}	2	0
7	36	{0, 12, 24, 36}	4	1
8	38	{0, 19, 38}	3	2
9	40	{0, 12, 28, 40}	4	1
10	42	{0, 42}	2	0
11	43	{0, 12, 19, 24, 31, 43}	6	2
12	45	{0, 45}	2	0
13	46	{0, 12, 34, 46}	4	1
14	47	{0, 19, 28, 47}	4	2
15	48	{0, 12, 24, 36, 48}	5	3
16	49	{0, 49}	2	0
17	50	{0, 12, 19, 31, 38, 50}	6	2
18	51	{0, 51}	2	0
19	52	{0, 12, 24, 28, 40, 52}	6	3
20	53	{0, 19, 34, 53}	4	2
21	54	{0, 12, 42, 54}	4	1
22	55	{0, 12, 19, 24, 31, 36, 43, 55}	8	3
23	56	{0, 28, 56}	3	4