Semigroup Ideals and Generalized Hamming Weights

Maria Bras-Amorós

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

Contents

Main reference

The results in this talk can be found in

M. Bras-Amorós, K. Lee, A. Vico-Oton:
New Lower Bounds on the Generalized Hamming Weights of AG Codes,
IEEE Transactions on Information Theory, vol. 60, n. 10, pp. 5930-5937, October 2014. ISSN: 0018-9448.

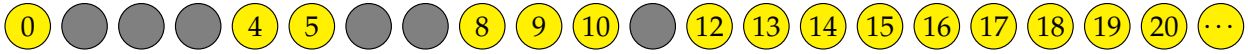
Maximum integer not in an ideal

Max integer not in a semigroup (Frobenius number)

Max integer not in a semigroup (Frobenius number)

A numerical semigroup Λ is a subset of $\mathbb{N}_0$ such that

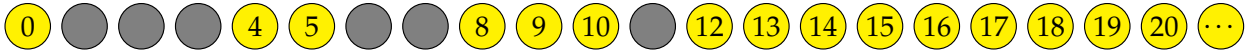
- Λ contains 0,
- Λ is closed under addition,
- Λ has a finite complement in $\mathbb{N}_0$.



Max integer not in a semigroup (Frobenius number)

A numerical semigroup Λ is a subset of $\mathbb{N}_0$ such that

- Λ contains 0,
- Λ is closed under addition,
- Λ has a finite complement in $\mathbb{N}_0$.



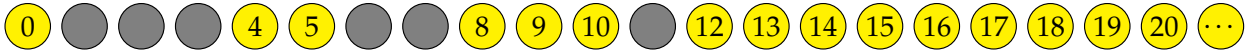
The elements in this complement are called the gaps of the semigroup and the number of gaps is the genus.

The maximum gap is the Frobenius number of the semigroup and the conductor is the Frobenius number plus one.

Max integer not in a semigroup (Frobenius number)

A numerical semigroup Λ is a subset of $\mathbb{N}_0$ such that

- Λ contains 0,
- Λ is closed under addition,
- Λ has a finite complement in $\mathbb{N}_0$.



The elements in this complement are called the gaps of the semigroup and the number of gaps is the genus.

The maximum gap is the Frobenius number of the semigroup and the conductor is the Frobenius number plus one.

Lemma

1. $F \leqslant 2g - 1$ *(pigeonhole principle)*
2. $F = 2g - 1 \iff \Lambda$ *symmetric (that is,* $i \in \Lambda \iff F - i \notin \Lambda$*).*

Maximun integer not in an ideal

Maximun integer not in an ideal

Ideals of a numerical semigroup

A subset $I \subseteq \Lambda$ is an ideal of a numerical semigroup if and only if

$$I + \Lambda \subseteq I.$$

In particular, $\Lambda \setminus I$ is finite.

Maximun integer not in an ideal

Ideals of a numerical semigroup

A subset $I \subseteq \Lambda$ is an ideal of a numerical semigroup if and only if

$$I + \Lambda \subseteq I.$$

In particular, $\Lambda \setminus I$ is finite.

Goal: $\max(\mathbb{N}_0 \setminus I)$.

Maximun integer not in an ideal

Ideals of a numerical semigroup

A subset $I \subseteq \Lambda$ is an ideal of a numerical semigroup if and only if

$$I + \Lambda \subseteq I.$$

In particular, $\Lambda \setminus I$ is finite.

Goal: $\max(\mathbb{N}_0 \setminus I)$.

Example

If $I = \Lambda$ then $\max(\mathbb{N}_0 \setminus I) = F$. In particular,

1. $\max(\mathbb{N}_0 \setminus I) \leqslant 2g - 1$
2. $\max(\mathbb{N}_0 \setminus I) = 2g - 1 \iff \Lambda$ symmetric.

Preliminaries: Barucci's theorem

Preliminaries: Barucci's theorem

Suppose $\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \dots\}$.

Divisors of λ_i: $D(i) = \{\lambda_j \leqslant \lambda_i : \lambda_i - \lambda_j \in \Lambda\}$, and we set $\nu_i = \#D(i)$

Preliminaries: Barucci's theorem

Suppose $\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \dots\}$.

Divisors of λ_i: $D(i) = \{\lambda_j \leqslant \lambda_i : \lambda_i - \lambda_j \in \Lambda\}$, and we set $\nu_i = \#D(i)$ (*different than yesterday!*)

Preliminaries: Barucci's theorem

Suppose $\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \dots\}$.

Divisors of λ_i: $D(i) = \{\lambda_j \leqslant \lambda_i : \lambda_i - \lambda_j \in \Lambda\}$, and we set $\nu_i = \#D(i)$ *(different than yesterday!)*

Example

In $\Lambda = \{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, D(6) = \{0, 4, 8, 12\}, \nu_6 = 4$.

Preliminaries: Barucci's theorem

Suppose $\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \dots\}$.

Divisors of λ_i: $D(i) = \{\lambda_j \leqslant \lambda_i : \lambda_i - \lambda_j \in \Lambda\}$, and we set $\nu_i = \#D(i)$ *(different than yesterday!)*

Example

In $\Lambda = \{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, D(6) = \{0, 4, 8, 12\}, \nu_6 = 4$.

Theorem (Barucci)

Any ideal of a numerical semigroup is an intersection of irreducible ideals and irreducible ideals have the form $\Lambda \setminus D(i)$ for some i.

Preliminaries: Barucci's theorem

Suppose $\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \dots\}$.

Divisors of λ_i: $D(i) = \{\lambda_j \leqslant \lambda_i : \lambda_i - \lambda_j \in \Lambda\}$, and we set $\nu_i = \#D(i)$ *(different than yesterday!)*

Example

In $\Lambda = \{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, D(6) = \{0, 4, 8, 12\}, \nu_6 = 4$.

Theorem (Barucci)

Any ideal of a numerical semigroup is an intersection of irreducible ideals and irreducible ideals have the form $\Lambda \setminus D(i)$ for some i.

Example

$\Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ is an irreducible ideal of Λ.

Preliminaries: Hoholdt, van Lint, Pellikaan's Lemma

Preliminaries: Hoholdt, van Lint, Pellikaan's Lemma

$G(i)$: number of pairs of gaps adding up to λ_i.

Preliminaries: Hoholdt, van Lint, Pellikaan's Lemma

$G(i)$: number of pairs of gaps adding up to λ_i.

Example

In $\{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, G(6) = 3$ since $\lambda_6 = 12 = 1 + 11 = 6 + 6 = 11 + 1$.

Preliminaries: Hoholdt, van Lint, Pellikaan's Lemma

$G(i)$: number of pairs of gaps adding up to λ_i.

Example

In $\{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, G(6) = 3$ since $\lambda_6 = 12 = 1 + 11 = 6 + 6 = 11 + 1$.

$g(i)$: number of gaps smaller than λ_i.

Preliminaries: Hoholdt, van Lint, Pellikaan's Lemma

$G(i)$: number of pairs of gaps adding up to λ_i.

Example

In $\{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, G(6) = 3$ since $\lambda_6 = 12 = 1 + 11 = 6 + 6 = 11 + 1$.

$g(i)$: number of gaps smaller than λ_i.

Example

In $\{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, g(3) = \#\{\text{gaps smaller than } \lambda_3 (= 8)\} = 5$.

Preliminaries: Hoholdt, van Lint, Pellikaan's Lemma

$G(i)$: number of pairs of gaps adding up to λ_i.

Example

In $\{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, G(6) = 3$ since $\lambda_6 = 12 = 1 + 11 = 6 + 6 = 11 + 1$.

$g(i)$: number of gaps smaller than λ_i.

Example

In $\{0, 4, 5, 8, 9, 10, 12, \rightarrow\}, g(3) = \#\{\text{gaps smaller than } \lambda_3 (= 8)\} = 5$.

Lemma (Hoholdt, van Lint, Pellikaan)

$$\nu_i = i - g(i) + G(i) + 1$$

Bound

Difference of I: $\#(\Lambda \setminus I)$

Theorem

The maximum integer not belonging to an ideal I of a semigroup Λ of genus g with difference d is at most $d + 2g - 1$. That is, $d + 2g + i \in I$ for all $i \geqslant 0$.

Bound

Difference of I: $\#(\Lambda \setminus I)$

Theorem

The maximum integer not belonging to an ideal I of a semigroup Λ of genus g with difference d is at most $d + 2g - 1$. That is, $d + 2g + i \in I$ for all $i \geqslant 0$.

Proof: If I, I' satisfy the result then $I \cap I'$ also satisfies it.

By Barucci's Theorem it is then enough to prove the result for $I = \Lambda \setminus D(i)$.

In this case $\begin{cases} d = \nu_i \\ \max(\mathbb{N}_0 \setminus I) = \max\{c-1, \lambda_i\}. \end{cases}$

We need to see that $\nu_i + 2g \geqslant \max\{c, \lambda_i + 1\}$ (c the conductor).

If $c \geqslant \lambda_i + 1$ then we are done since $2g \geqslant c$.

If $c < \lambda_i + 1$ then $g(i) = g$, $\lambda_i = i + g$, and hence, by HvLP's Lemma,
$\nu_i + 2g = (i - g + G(i) + 1) + 2g = i + g + 1 + G(i) = \lambda_i + 1 + G(i) \geqslant \lambda_i + 1.$ □

Characterization of ideals attaining the bound

Lemma

If $G(i) = 0$ *then* $\lambda_i \geqslant c$.

Characterization of ideals attaining the bound

Lemma

If $G(i) = 0$ *then* $\lambda_i \geqslant c$.

Proof: Suppose $G(i) = 0$. Then, $1, \ldots, \lambda_1 - 1$ gaps $\Longrightarrow \lambda_i - \lambda_1 + 1, \ldots, \lambda_i - 1$ non-gaps.

But $\lambda_i \in \Lambda \Longrightarrow [\lambda_i - \lambda_1 + 1, \ldots, \lambda_i] \subseteq \Lambda$.

Now, by adding multiples of λ_1 to the elements in this interval we get the whole set of integers $\lambda_i + k$ with $k \geqslant 0$.

Then $\lambda_i \geqslant c$. □

Characterization of ideals attaining the bound

Theorem

The next statements are equivalent:

1. *The maximum integer not belonging to I is exactly $d + 2g - 1$.*
2. $I = \Lambda \setminus D(i)$ *for some i with* $G(i) = 0$.

Characterization of ideals attaining the bound

Theorem

The next statements are equivalent:

1. *The maximum integer not belonging to* I *is exactly* $d + 2g - 1$.
2. $I = \Lambda \setminus D(i)$ *for some* i *with* $G(i) = 0$.

Proof: Suppose first that $I = \Lambda \setminus D(i)$ for some i with $G(i) = 0$.

Then $d = \nu_i$.

Also, $G(i) = 0 \Longrightarrow \lambda_i \geqslant c$ and so

- $g(i) = g$
- $\lambda_i = i + g$

Now, by HvLP's Lemma,
$d + 2g - 1 = (i - g(i) + G(i) + 1) + 2g - 1 = i - g + 0 + 1 + 2g - 1 = i + g = \lambda_i \notin I$.

□

Characterization of ideals attaining the bound

Theorem

The next statements are equivalent:

1. *The maximum integer not belonging to I is exactly $d + 2g - 1$.*
2. $I = \Lambda \setminus D(i)$ *for some i with* $G(i) = 0$.

Proof:

Conversely, suppose that the maximum integer not belonging to I is $d + 2g - 1$.

If $I = I' \cap I''$, with I', I'' ideals, $d' = \#(\Lambda \setminus I')$, $d'' = \#(\Lambda \setminus I'')$, and $I', I'' \neq I$, then $d = \#(\Lambda \setminus I) > d', d''$.

If $d + 2g - 1 \notin I$ then $d + 2g - 1 \notin I'$ or $d + 2g - 1 \notin I''$, but $d + 2g - 1 > d' + 2g - 1, d'' + 2g - 1$, contradicting the previous bound.

By Barucci's Theorem, $I = \Lambda \setminus D(i)$ for some i. Also, $d = \nu_i$.

If $\lambda_i < c$, then $\nu_i + 2g - 1 \geqslant 1 + 2g - 1 = 2g \geqslant c$ and so $d + 2g - 1 \in I$, a contradiction.

Therefore $\lambda_i \geqslant c$. Then $\nu_i = i - g + G(i) + 1$ by HvLP's Lemma.
So $d + 2g - 1 = i + g + G(i) = \lambda_i + G(i)$. But $d + 2g - 1 \notin I \Longrightarrow G(i) = 0$. □

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ has difference equal to $\nu_6 = 4$,

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ has difference equal to $\nu_6 = 4$, but

$$d + 2g - 1 = 4 + 12 - 1 = 15 \in I.$$

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ has difference equal to $\nu_6 = 4$, but

$$d + 2g - 1 = 4 + 12 - 1 = 15 \in I.$$

This is because, as already seen, $G(6) \neq 0$.

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ has difference equal to $\nu_6 = 4$, but

$$d + 2g - 1 = 4 + 12 - 1 = 15 \in I.$$

This is because, as already seen, $G(6) \neq 0$.

The ideal $I = \Lambda \setminus D(9) = \{4, 8, 9, 12, 13, 14, 16, \rightarrow\}$

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ has difference equal to $\nu_6 = 4$, but

$$d + 2g - 1 = 4 + 12 - 1 = 15 \in I.$$

This is because, as already seen, $G(6) \neq 0$.

The ideal $I = \Lambda \setminus D(9) = \{4, 8, 9, 12, 13, 14, 16, \rightarrow\}$ has difference equal to $\nu_9 = \#\{0, 5, 10, 15\} = 4$,

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ has difference equal to $\nu_6 = 4$, but

$$d + 2g - 1 = 4 + 12 - 1 = 15 \in I.$$

This is because, as already seen, $G(6) \neq 0$.

The ideal $I = \Lambda \setminus D(9) = \{4, 8, 9, 12, 13, 14, 16, \rightarrow\}$ has difference equal to $\nu_9 = \#\{0, 5, 10, 15\} = 4$, and

$$d + 2g - 1 = 4 + 12 - 1 = 15 \notin I.$$

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ has difference equal to $\nu_6 = 4$, but

$$d + 2g - 1 = 4 + 12 - 1 = 15 \in I.$$

This is because, as already seen, $G(6) \neq 0$.

The ideal $I = \Lambda \setminus D(9) = \{4, 8, 9, 12, 13, 14, 16, \rightarrow\}$ has difference equal to $\nu_9 = \#\{0, 5, 10, 15\} = 4$, and

$$d + 2g - 1 = 4 + 12 - 1 = 15 \notin I.$$

This is because $G(9) = 0$. Indeed, $\{15 - 1 = 14, 15 - 2 = 13, 15 - 3 = 12, 15 - 6 = 9, 15 - 7 = 8, 15 - 11 = 4\} \subseteq \Lambda$.

Characterization of ideals attaining the bound

Theorem

The next statements are equivalent:

1. *The maximum integer not belonging to I is exactly $d + 2g - 1$.*
2. $I = \Lambda \setminus D(i)$ *for some* i *with* $G(i) = 0$.
3. $\Lambda \setminus I = \Lambda \cap ((d + 2g - 1) - \Lambda) = \{\lambda \in \Lambda : d + 2g - 1 - \lambda \in \Lambda\}$
4. $I = \{\lambda_i - h : h \in \mathbb{Z} \setminus \Lambda\}$ *for some* i *with* $G(i) = 0$.
5. $\{a + h : h \notin \Lambda, F - h \notin \Lambda\} \subseteq \Lambda$ *and* $I = (a + \Lambda) \cup \{a + h : h \notin \Lambda, F - h \notin \Lambda\}$ *for some* $a \in \Lambda$, $a > 0$.

Characterization of ideals attaining the bound

We call the ideals of the form $a + \Lambda$ for some $a \in \Lambda$ principal ideals.

Characterization of ideals attaining the bound

We call the ideals of the form $a + \Lambda$ for some $a \in \Lambda$ principal ideals.

Corollary

Let Λ be a symmetric numerical semigroup of genus g. Suppose that I is an ideal of Λ with difference d. Then the largest integer not belonging to I is $d + 2g - 1$ if and only if I is principal.

Characterization of ideals attaining the bound

Example

Consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, \rightarrow\}.$$

The ideal $I = \Lambda \setminus D(6) = \{5, 9, 10, 13, \rightarrow\}$ has difference equal to $\nu_6 = 4$, but

$$d + 2g - 1 = 4 + 12 - 1 = 15 \in I.$$

This is because, as already seen, $G(6) \neq 0$.

The ideal $I = \Lambda \setminus D(9) = \{4, 8, 9, 12, 13, 14, 16, \rightarrow\}$ has difference equal to $\nu_9 = \#\{0, 5, 10, 15\} = 4$, and

$$d + 2g - 1 = 4 + 12 - 1 = 15 \notin I.$$

This is because $G(9) = 0$. Indeed, $\{15 - 1 = 14, 15 - 2 = 13, 15 - 3 = 12, 15 - 6 = 9, 15 - 7 = 8, 15 - 11 = 4\} \subseteq \Lambda$.

Sequences of pairwise isometric one-point AG codes

Sequences of pairwise isometric one-point AG codes

Two codes $C, D \subseteq \mathbb{F}_q^n$ are said to be x-isometric, for $x \in (\mathbb{F}_q^*)^n$ if

$$D = \{x * c = (x_1c_1, \ldots, x_nc_n) : c \in C\}.$$

Sequences of pairwise isometric one-point AG codes

Two codes $C, D \subseteq \mathbb{F}_q^n$ are said to be x-isometric, for $x \in (\mathbb{F}_q^*)^n$ if

$$D = \{x * c = (x_1c_1, \ldots, x_nc_n) : c \in C\}.$$

Example

Consider the double-repetition code in $\mathbb{F}^{*4}_3$
$C = \{(0,0,0,0),(0,0,1,1),(0,0,2,2),(1,1,0,0),(1,1,1,1),(1,1,2,2),(2,2,0,0),(2,2,1,1),(2,2,2,2)\}$

and the code

$D = \{(0,0,0,0),(0,0,1,2),(0,0,2,1),(1,2,0,0),(1,2,1,2),(1,2,2,1),(2,1,0,0),(2,1,1,2),(2,1,2,1)\}$

One can check that D is $(1,2,1,2)$-isometric to C.

Sequences of pairwise isometric one-point AG codes

Two codes $C, D \subseteq \mathbb{F}_q^n$ are said to be x-isometric, for $x \in (\mathbb{F}_q^*)^n$ if

$$D = \{x * c = (x_1 c_1, \ldots, x_n c_n) : c \in C\}.$$

Example

Consider the double-repetition code in $\mathbb{F}{*}_3^4$

$C = \{(0,0,0,0), (0,0,1,1), (0,0,2,2), (1,1,0,0), (1,1,1,1), (1,1,2,2), (2,2,0,0), (2,2,1,1), (2,2,2,2)\}$

and the code

$D = \{(0,0,0,0), (0,0,1,2), (0,0,2,1), (1,2,0,0), (1,2,1,2), (1,2,2,1), (2,1,0,0), (2,1,1,2), (2,1,2,1)\}$

One can check that D is $(1,2,1,2)$-isometric to C.

A sequence of codes $(C_i)_{i=0,\ldots,n}$ is said to satisfy the isometry-dual condition if there exists $x \in (\mathbb{F}_q^*)^n$ such that C_i is x-isometric to $C_{n-i}^{\perp}$ for all $i = 0, \ldots, n$.

Sequences of pairwise isometric one-point AG codes

Let $P_1, \ldots, P_n, Q$ be different rational points of a (projective, non-singular, geometrically irreducible) curve with genus g and define

$$C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\} \textit{(different than yesterday!)}$$

Sequences of pairwise isometric one-point AG codes

Let $P_1, \ldots, P_n, Q$ be different rational points of a (projective, non-singular, geometrically irreducible) curve with genus g and define

$$C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\} \text{(\textit{different than yesterday!})}$$

$$W = \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\} \text{(Weierstrass semigroup)},$$

Sequences of pairwise isometric one-point AG codes

Let $P_1, \dots, P_n, Q$ be different rational points of a (projective, non-singular, geometrically irreducible) curve with genus g and define

$$C_m = \{(f(P_1), \dots, f(P_n)) : f \in L(mQ)\} \text{(different than yesterday!)}$$

$$\begin{aligned} W &= \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\} \text{(Weierstrass semigroup)}, \\ W^* &= \{0\} \cup \{m \in \mathbb{N} : C_m \neq C_{m-1}\} = \{m_1 = 0, m_2, \dots, m_n\}. \end{aligned}$$

Sequences of pairwise isometric one-point AG codes

Let $P_1, \ldots, P_n, Q$ be different rational points of a (projective, non-singular, geometrically irreducible) curve with genus g and define

$$C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\}\text{(different than yesterday!)}$$

$$W = \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\}\text{(Weierstrass semigroup)},$$

$$W^* = \{0\} \cup \{m \in \mathbb{N} : C_m \neq C_{m-1}\} = \{m_1 = 0, m_2, \ldots, m_n\}.$$

Theorem (Geil, Munuera, Ruano, Torres)

- *$W \setminus W^*$ is an ideal of W,*
- *$\{0\}, C_{m_1}, \ldots, C_{m_n}$ satisfies the isometry-dual condition $\Leftrightarrow \#W^* + 2g - 1 \in W^*$.*

Feng-Rao numbers and generalized Hamming weights

Generalized Hamming weights

The generalized Hamming weights of a linear code are, for each given dimension, the minimum size of the support of the linear subspaces of that dimension.

Generalized Hamming weights

The generalized Hamming weights of a linear code are, for each given dimension, the minimum size of the support of the linear subspaces of that dimension.

Example

$C = \{(0,0,0,0),(0,0,1,1),(0,0,2,2),(1,1,0,0),(1,1,1,1),(1,1,2,2),(2,2,0,0),(2,2,1,1),(2,2,2,2)\}$

Subspaces of dimension 1:

- $\langle(1,1,0,0)\rangle$ supported on 2 coordinates
- $\langle(0,0,1,1)\rangle$ supported on 2 coordinates
- $\langle(1,1,1,1)\rangle$ supported on 4 coordinates

So, generalized Hamming weight of dimension 1 (= minimum distance) is 2.

Subspaces of dimension 2:

- $\langle(1,1,0,0),(0,0,1,1)\rangle$ supported on 4 coordinates

So, generalized Hamming weight of dimension 2 is 4.

Generalized Hamming weights

Generalized Hamming weights are used in

- the wire-tap channel of type II
- t-resilient functions
- network coding
- list decoding
- bounding the covering radius of linear codes
- secure secret sharing based on linear codes

Order bounds for algebraic geometry codes

Algebraic geometry codes

Let $P_1, \ldots, P_n, Q$ be different rational points of a (projective, non-singular, geometrically irreducible) curve with genus g and define

$$\begin{aligned} C_m &= \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\} \\ W &= \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\} \text{(Weierstrass semigr.)} \end{aligned}$$

Order bounds for algebraic geometry codes

Algebraic geometry codes

Let $P_1, \ldots, P_n, Q$ be different rational points of a (projective, non-singular, geometrically irreducible) curve with genus g and define

$$\begin{aligned} C_m &= \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\} \\ W &= \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\} \text{(Weierstrass semigr.)} \end{aligned}$$

Order bound on the minimum distance

The minimum distance of $C_{\lambda_m}^{\perp}$ is lower bounded by the order bound:

$$\delta(m) = \min\{\nu_i : i > m\}$$

Order bounds for algebraic geometry codes

Define $D(i)$ as before and $D(i_1, \ldots, i_r) = D(i_1) \cup \cdots \cup D(i_r)$.

Order bounds for algebraic geometry codes

Define $D(i)$ as before and $D(i_1, \ldots, i_r) = D(i_1) \cup \cdots \cup D(i_r)$.

Order bound on generalized Hamming weights

The r-th generalized Hamming weight of $C_{\lambda_m}^{\perp}$ is lower bounded by the r-th order bound:

$$\delta_r(m) = \min\{\#D(i_1, \ldots, i_r) : i_1, \ldots, i_r > m\}.$$

Farrán-Munuera's Feng-Rao numbers

Theorem (Farrán-Munuera)

For each numerical semigroup Λ *and each integer* $r \geqslant 2$ *there exists a constant* $E_r = E(\Lambda, r)$*, called r-th Feng-Rao number, such that*

1. $\delta_r(m) = m + 2 - g + E_r$ *for all m such that* $\lambda_m \geqslant 2c - 2$*,*
2. $\delta_r(m) \geqslant m + 2 - g + E_r$ *for any m such that* $\lambda_m \geqslant c$*,*

where c and g are respectively the conductor and the genus of Λ*.*

Farrán-Munuera's Feng-Rao numbers

Theorem (Farrán-Munuera)

For each numerical semigroup Λ and each integer $r \geqslant 2$ there exists a constant $E_r = E(\Lambda, r)$, called r-th Feng-Rao number, such that

1. $\delta_r(m) = m + 2 - g + E_r$ *for all m such that* $\lambda_m \geqslant 2c - 2$,
2. $\delta_r(m) \geqslant m + 2 - g + E_r$ *for any m such that* $\lambda_m \geqslant c$,

where c and g are respectively the conductor and the genus of Λ.

This is an extension of the Goppa bound for $r = 1$, with $E_r = 0$.

Farrán-Munuera's Feng-Rao numbers

Theorem (Farrán-Munuera)

For each numerical semigroup Λ and each integer $r \geqslant 2$ there exists a constant $E_r = E(\Lambda, r)$, called r-th Feng-Rao number, such that

1. $\delta_r(m) = m + 2 - g + E_r$ *for all* m *such that* $\lambda_m \geqslant 2c - 2$,
2. $\delta_r(m) \geqslant m + 2 - g + E_r$ *for any* m *such that* $\lambda_m \geqslant c$,

where c *and* g *are respectively the conductor and the genus of* Λ.

This is an extension of the Goppa bound for $r = 1$, with $E_r = 0$.

Furthermore,

3. $r \leqslant E_r \leqslant \lambda_{r-1}$ if $g > 0$ (and $r \geqslant 2$),
4. $E_r = \lambda_{r-1}$ if $r \geqslant c$,
5. $E_r = r - 1$ if $g = 0$.

The perspective of ideals

Recall, $\delta_r(m) = \min\{\#D(i_1, \ldots, i_r) : i_1, \ldots, i_r > m\}$.

The perspective of ideals

Recall, $\delta_r(m) = \min\{\#D(i_1, \ldots, i_r) : i_1, \ldots, i_r > m\}$.

By Farrán-Munuera's theorem, $\delta_r(m) = m + 2 - g + E_r$ for all m such that $\lambda_m \geqslant 2c - 2$.

The perspective of ideals

Recall, $\delta_r(m) = \min\{\#D(i_1, \ldots, i_r) : i_1, \ldots, i_r > m\}$.

By Farrán-Munuera's theorem, $\delta_r(m) = m + 2 - g + E_r$ for all m such that $\lambda_m \geqslant 2c - 2$.

Suppose $m < i_1 < \cdots < i_r$ are such that $\delta_r(m) = \#D(i_1, \ldots, i_r)$.

The perspective of ideals

Recall, $\delta_r(m) = \min\{\#D(i_1, \dots, i_r) : i_1, \dots, i_r > m\}$.

By Farrán-Munuera's theorem, $\delta_r(m) = m + 2 - g + E_r$ for all m such that $\lambda_m \geqslant 2c - 2$.

Suppose $m < i_1 < \cdots < i_r$ are such that $\delta_r(m) = \#D(i_1, \dots, i_r)$.

Then
$\Lambda \setminus D(i_1, \dots, i_r) = \Lambda \setminus (D(i_1) \cup \cdots \cup D(i_r)) = (\Lambda \setminus D(i_1)) \cap \cdots \cap (\Lambda \setminus D(i_r))$

The perspective of ideals

Recall, $\delta_r(m) = \min\{\#D(i_1, \dots, i_r) : i_1, \dots, i_r > m\}$.

By Farrán-Munuera's theorem, $\delta_r(m) = m + 2 - g + E_r$ for all m such that $\lambda_m \geqslant 2c - 2$.

Suppose $m < i_1 < \cdots < i_r$ are such that $\delta_r(m) = \#D(i_1, \dots, i_r)$.

Then
$\Lambda \setminus D(i_1, \dots, i_r) = \Lambda \setminus (D(i_1) \cup \cdots \cup D(i_r)) = (\Lambda \setminus D(i_1)) \cap \cdots \cap (\Lambda \setminus D(i_r))$
is an ideal with

- difference: $\#D(i_1, \dots, i_r) = \delta_r(m) = m + 2 - g + E_r$

The perspective of ideals

Recall, $\delta_r(m) = \min\{\#D(i_1, \dots, i_r) : i_1, \dots, i_r > m\}$.

By Farrán-Munuera's theorem, $\delta_r(m) = m + 2 - g + E_r$ for all m such that $\lambda_m \geqslant 2c - 2$.

Suppose $m < i_1 < \cdots < i_r$ are such that $\delta_r(m) = \#D(i_1, \dots, i_r)$.

Then
$\Lambda \setminus D(i_1, \dots, i_r) = \Lambda \setminus (D(i_1) \cup \cdots \cup D(i_r)) = (\Lambda \setminus D(i_1)) \cap \cdots \cap (\Lambda \setminus D(i_r))$
is an ideal with

- difference: $\#D(i_1, \dots, i_r) = \delta_r(m) = m + 2 - g + E_r$
- maximum integer not belonging to it: λ_{i_r}

The perspective of ideals

Recall, $\delta_r(m) = \min\{\#D(i_1, \ldots, i_r) : i_1, \ldots, i_r > m\}$.

By Farrán-Munuera's theorem, $\delta_r(m) = m + 2 - g + E_r$ for all m such that $\lambda_m \geqslant 2c - 2$.

Suppose $m < i_1 < \cdots < i_r$ are such that $\delta_r(m) = \#D(i_1, \ldots, i_r)$.

Then
$\Lambda \setminus D(i_1, \ldots, i_r) = \Lambda \setminus (D(i_1) \cup \cdots \cup D(i_r)) = (\Lambda \setminus D(i_1)) \cap \cdots \cap (\Lambda \setminus D(i_r))$
is an ideal with

- difference: $\#D(i_1, \ldots, i_r) = \delta_r(m) = m + 2 - g + E_r$
- maximum integer not belonging to it: λ_{i_r}

So, $\lambda_{i_r} \leqslant (m + 2 - g + E_r) + 2g - 1 = m + g + 1 + E_r = \lambda_{m+1} + E_r \Longrightarrow$

The perspective of ideals

Recall, $\delta_r(m) = \min\{\#D(i_1, \ldots, i_r) : i_1, \ldots, i_r > m\}$.

By Farrán-Munuera's theorem, $\delta_r(m) = m + 2 - g + E_r$ for all m such that $\lambda_m \geqslant 2c - 2$.

Suppose $m < i_1 < \cdots < i_r$ are such that $\delta_r(m) = \#D(i_1, \ldots, i_r)$.

Then $\Lambda \setminus D(i_1, \ldots, i_r) = \Lambda \setminus (D(i_1) \cup \cdots \cup D(i_r)) = (\Lambda \setminus D(i_1)) \cap \cdots \cap (\Lambda \setminus D(i_r))$ is an ideal with

- difference: $\#D(i_1, \ldots, i_r) = \delta_r(m) = m + 2 - g + E_r$
- maximum integer not belonging to it: λ_{i_r}

So, $\lambda_{i_r} \leqslant (m + 2 - g + E_r) + 2g - 1 = m + g + 1 + E_r = \lambda_{m+1} + E_r \Longrightarrow$

$$E_r \geqslant \lambda_{i_r} - \lambda_{m+1} = i_r - i_1.$$

Bound on the Feng-Rao numbers

Theorem

Suppose that n_ℓ is the number of intervals of at least ℓ gaps of Λ. Then

$$E_r \geqslant \min\{r - 2 + \left\lceil \frac{r}{\ell - 1} \right\rceil, r - 1 + \left\lceil \frac{(\ell - 1)n_{\ell-1}}{\ell} \right\rceil\}.$$

In particular, if n is the number of intervals of Λ then

$$E_r \geqslant \min\{2(r-1), r - 1 + \lceil n/2 \rceil\}.$$

Bound on the Feng-Rao numbers

Theorem

Suppose that n_ℓ is the number of intervals of at least ℓ gaps of Λ. Then

$$E_r \geqslant \min\{r - 2 + \left\lceil \frac{r}{\ell - 1} \right\rceil, r - 1 + \left\lceil \frac{(\ell - 1)n_{\ell-1}}{\ell} \right\rceil\}.$$

In particular, if n is the number of intervals of Λ then

$$E_r \geqslant \min\{2(r-1), r - 1 + \lceil n/2 \rceil\}.$$

Remark

If $r = 2$ or $n_1 \leqslant 2$ then our bound equals $E_r \geqslant r$. In any other case our bound is better.

Bound on the generalized Hamming weights

Corollary

Let m be such that $\lambda_m \geqslant c$ and let $\ell \geqslant 2$. Then

$$\delta_r(m) \geqslant m + 2 - g + \min\{r - 2 + \left\lceil \frac{r}{\ell - 1} \right\rceil, r - 1 + \left\lceil \frac{(\ell - 1)n_{\ell-1}}{\ell} \right\rceil\}.$$

Corollary

If Λ is a semigroup with conductor c and n intervals of gaps then, for any m with $\lambda_m \geqslant c$,

$$\delta_r(m) \geqslant \begin{cases} m - g + 2r & \text{if } r \leqslant \lceil n/2 \rceil + 1, \\ m - g + r + \lceil n/2 \rceil + 1 & \text{otherwise.} \end{cases}$$

Exercise

1. Prove the Lemma by Hoholdt, van Lint, and Pellikaan stating $\nu_i = i - g(i) + G(i) + 1$, where $g(i)$ is the number of gaps smaller than λ_i and $G(i)$ is the number of pairs of gaps adding up to λ_i.
2. Find W^* in the case of Hermitian codes.
   - Check that $W \setminus W^*$ is an ideal.
   - Prove that Hermitian codes satisfy the isoemtry dual property.