Numerical semigroups, conjectures, algorithms, and applications

Maria Bras-Amorós

3a Jornada IMTech

13 de novembre, 2026

Contents

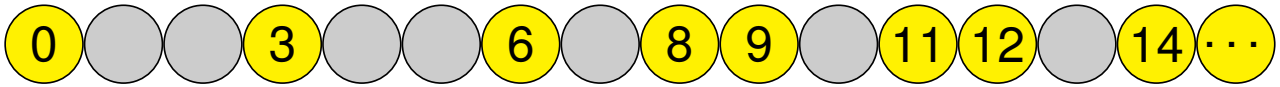
1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus
2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ
3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

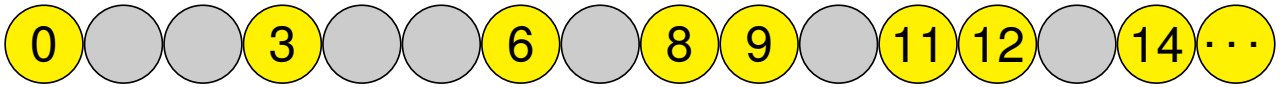
Numerical semigroups



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

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite

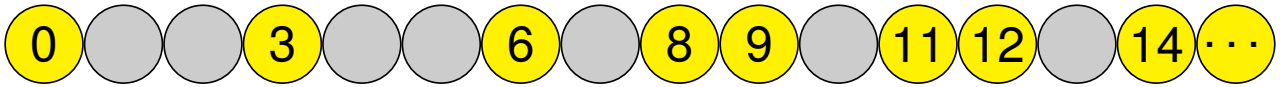
Numerical semigroups



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

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite (genus:=g= $\#(\mathbb{N}_0 \setminus \Lambda)$)

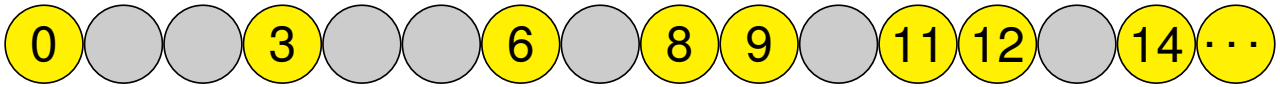
Numerical semigroups



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

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite (genus:=g= $\#(\mathbb{N}_0 \setminus \Lambda)$)
  $\Rightarrow$ there exists the Frobenius number := largest gap F

Numerical semigroups

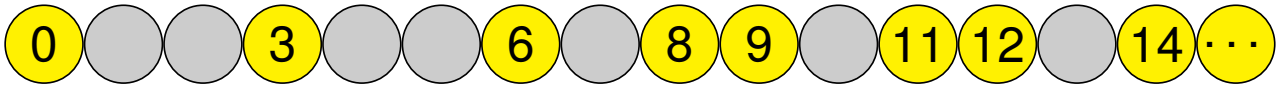


A numerical semigroup is a subset Λ of $\mathbb{N}_0$ satisfying

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite (genus:=g= $\#(\mathbb{N}_0 \setminus \Lambda)$)
  $\Rightarrow$ there exists the Frobenius number := largest gap F

gaps: $\mathbb{N}_0 \setminus \Lambda$
non-gaps: Λ

Numerical semigroups

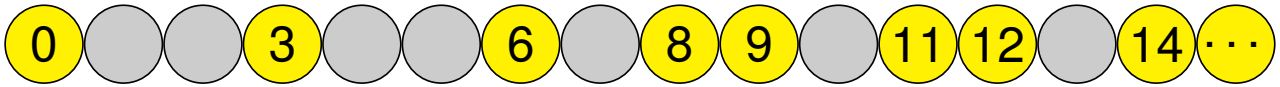


A numerical semigroup is a subset Λ of $\mathbb{N}_0$ satisfying

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite (genus:=g= $\#(\mathbb{N}_0 \setminus \Lambda)$)
  $\Rightarrow$ there exists the Frobenius number := largest gap F

gaps: $\mathbb{N}_0 \setminus \Lambda$
non-gaps: Λ
Left elements: $L(\Lambda) = \Lambda \cap [0, \ldots, F]$

Numerical semigroups

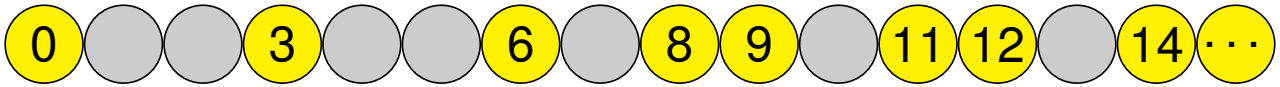


A numerical semigroup is a subset Λ of $\mathbb{N}_0$ satisfying

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite (genus:=g= $\#(\mathbb{N}_0 \setminus \Lambda)$)
  $\Rightarrow$ there exists the Frobenius number := largest gap F

gaps: $\mathbb{N}_0 \setminus \Lambda$
non-gaps: Λ
Left elements: $L(\Lambda) = \Lambda \cap [0, \ldots, F]$
Multiplicity: $\min(\Lambda^*)$

Numerical semigroups

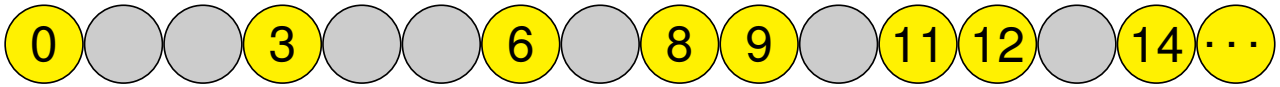


A numerical semigroup is a subset Λ of $\mathbb{N}_0$ satisfying

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite (genus:=g= $\#(\mathbb{N}_0 \setminus \Lambda)$)
  $\Rightarrow$ there exists the Frobenius number := largest gap F

gaps: $\mathbb{N}_0 \setminus \Lambda$
non-gaps: Λ
Left elements: $L(\Lambda) = \Lambda \cap [0, \ldots, F]$
Multiplicity: $\min(\Lambda^*)$
Minimal generators: $\Lambda^* \setminus (\Lambda^* + \Lambda^*)$

Numerical semigroups

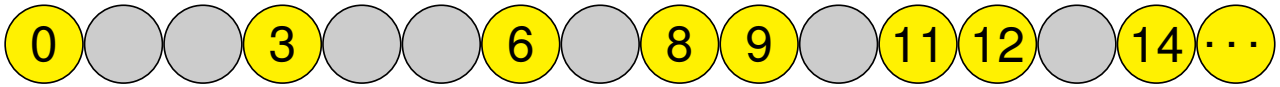


A numerical semigroup is a subset Λ of $\mathbb{N}_0$ satisfying

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite (genus:=g= $\#(\mathbb{N}_0 \setminus \Lambda)$)
  $\Rightarrow$ there exists the Frobenius number := largest gap F

gaps: $\mathbb{N}_0 \setminus \Lambda$
non-gaps: Λ
Left elements: $L(\Lambda) = \Lambda \cap [0, \ldots, F]$
Multiplicity: $\min(\Lambda^*)$
Minimal generators: $\Lambda^* \setminus (\Lambda^* + \Lambda^*)$ (necessarily coprime)

Numerical semigroups



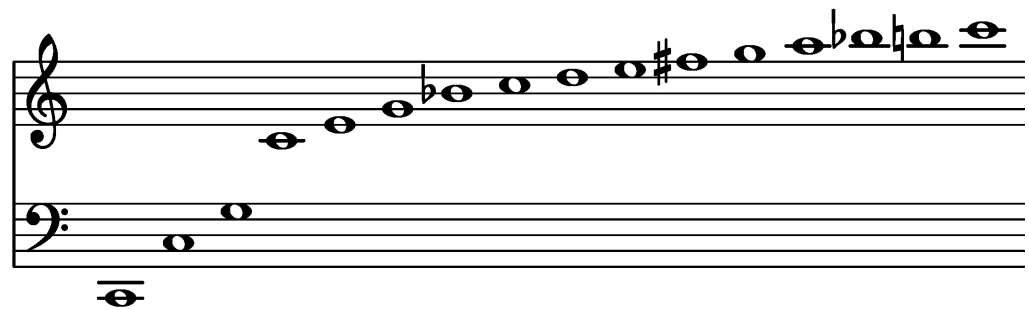
A numerical semigroup is a subset Λ of $\mathbb{N}_0$ satisfying

- $0 \in \Lambda$
- $\Lambda + \Lambda \subseteq \Lambda$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ is finite (genus:=g= $\#(\mathbb{N}_0 \setminus \Lambda)$)
  $\Rightarrow$ there exists the Frobenius number := largest gap F

gaps: $\mathbb{N}_0 \setminus \Lambda$
non-gaps: Λ
Left elements: $L(\Lambda) = \Lambda \cap [0, \ldots, F]$
Multiplicity: $\min(\Lambda^*)$
Minimal generators: $\Lambda^* \setminus (\Lambda^* + \Lambda^*)$ (necessarily coprime)
Embedding dimension: $e(\Lambda)$ = number of minimal generators

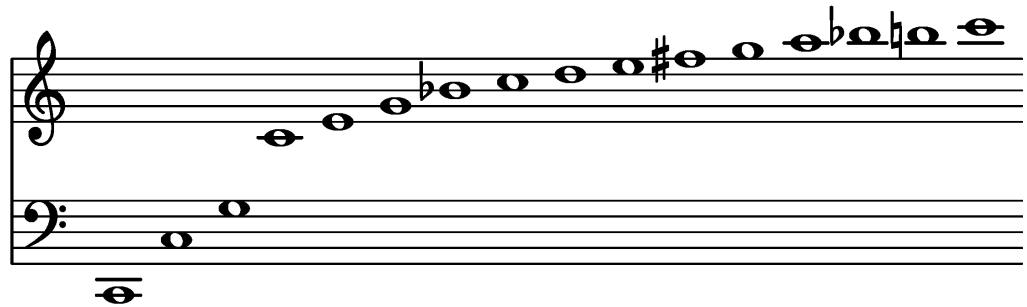
Harmonics: a sound example



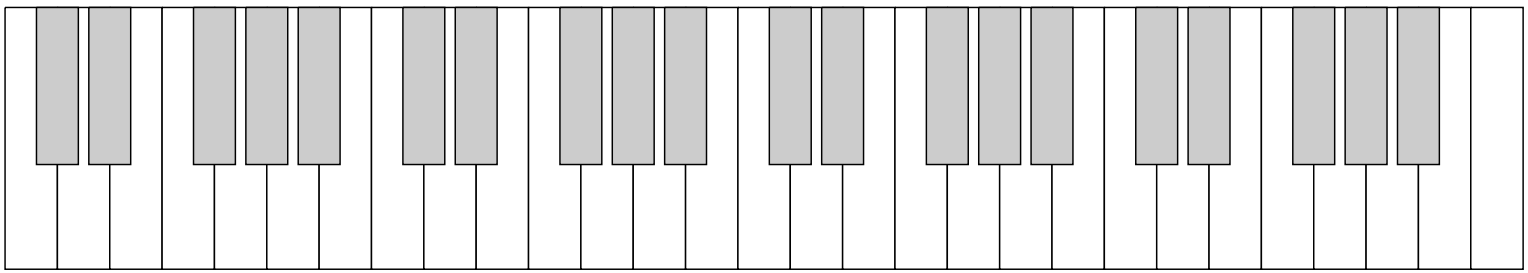


Harmonics: a sound example



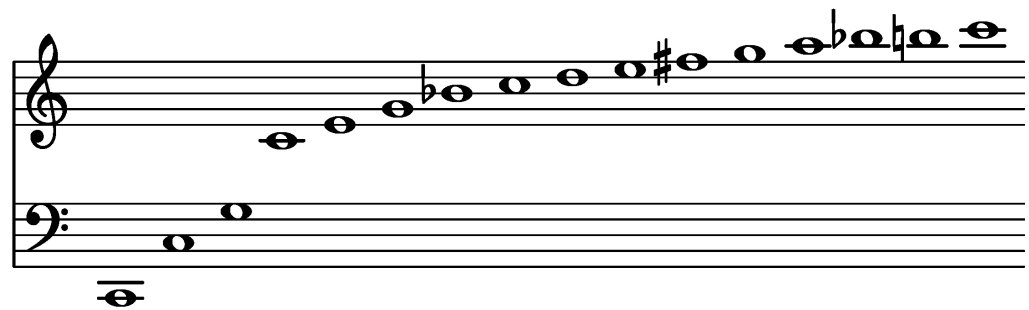


Divide the octave into 12 equal semitones.

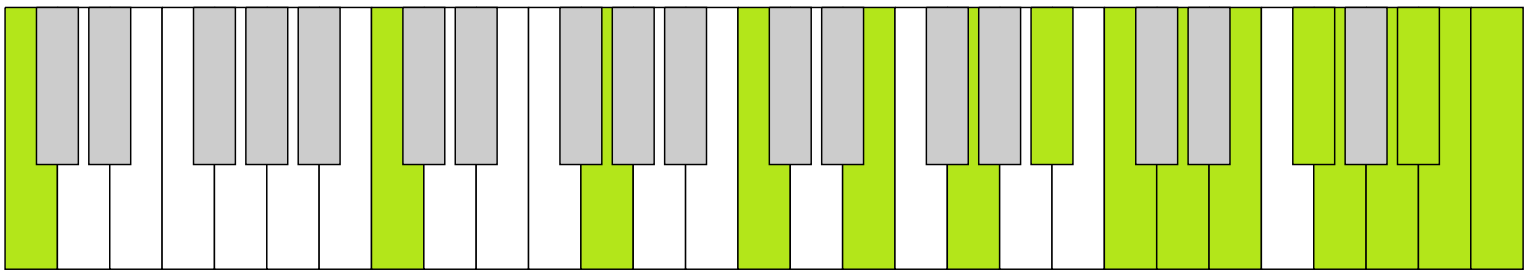


Harmonics: a sound example





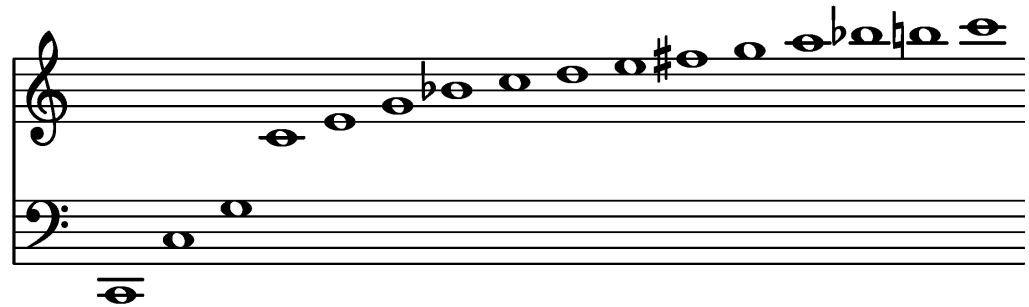
Divide the octave into 12 equal semitones.



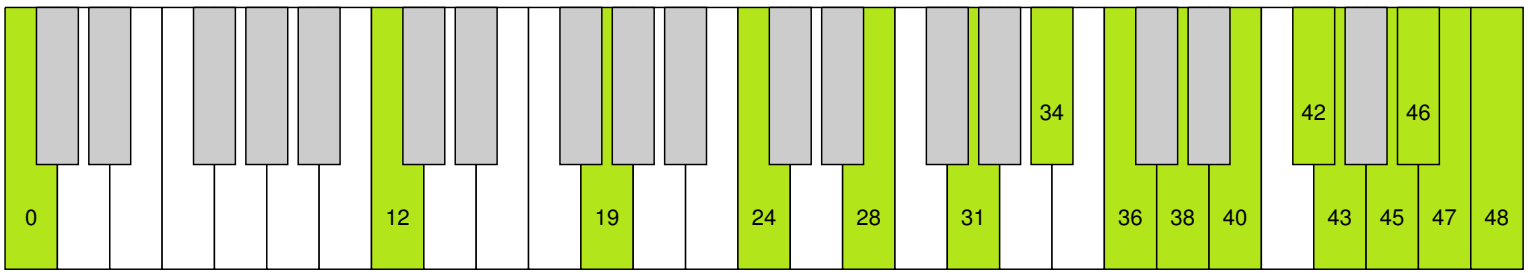
What semitone interval corresponds to each harmonic?

Harmonics: a sound example





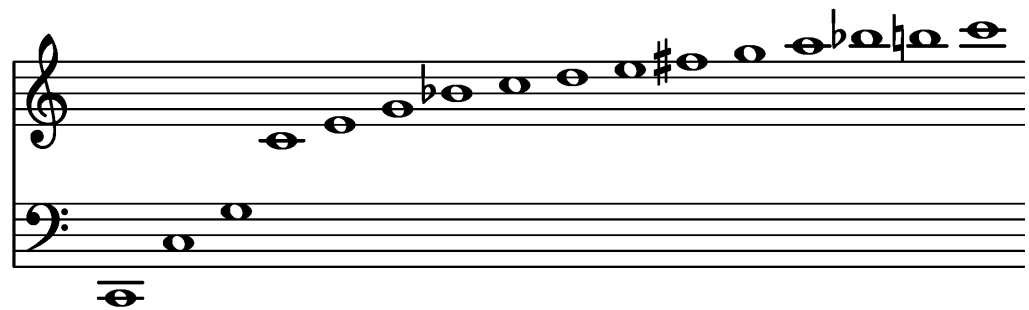
Divide the octave into 12 equal semitones.



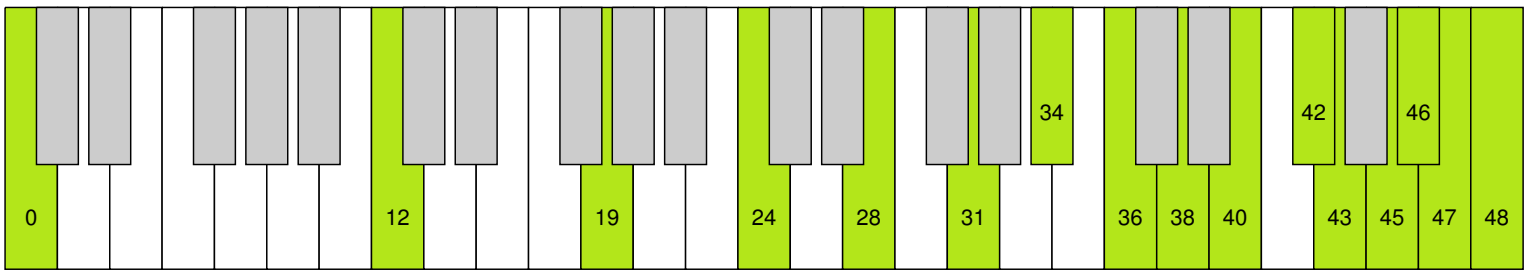
What semitone interval corresponds to each harmonic?

Harmonics: a sound example





Divide the octave into 12 equal semitones.



What semitone interval corresponds to each harmonic?

$$H = \{0, 12, 19, 24, 28, 31, 34, 36, 38, 40, 42, 43, 45, 46, 47, 48, 49, 50, \rightarrow\}.$$

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus
2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ
3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Definition

A gapset is a finite subset G of $\mathbb{N}_0$ satisfying

$$\left.\begin{array}{l} a, b \in \mathbb{N}_0 \\ \\ a+b \in G \end{array}\right\} \Longrightarrow a \in G \text{ or } b \in G.$$

Definition

A gapset is a finite subset G of $\mathbb{N}_0$ satisfying

$$\left.\begin{array}{l} a, b \in \mathbb{N}_0 \\ \\ a + b \in G \end{array}\right\} \Longrightarrow a \in G \text{ or } b \in G.$$

$$G \text{ gapset} \Longleftrightarrow \mathbb{N}_0 \setminus G \text{ numerical semigroup.}$$

S. Eliahou, J. Fromentin. Gapsets and numerical semigroups, Journal of Combinatorial Theory, Series A., 2020

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Weierstrass semigroup

$\mathcal{X}$: projective, non-singular, geometrically irreducible curve

P: rational point of $\mathcal{X}$

Weierstrass semigroup

$\mathcal{X}$: projective, non-singular, geometrically irreducible curve

P: rational point of $\mathcal{X}$

A: the ring of functions on $\mathcal{X}$ with poles only at P

Weierstrass semigroup

$\mathcal{X}$: projective, non-singular, geometrically irreducible curve

P: rational point of $\mathcal{X}$

A: the ring of functions on $\mathcal{X}$ with poles only at P

$\Lambda = \{-v_P(f) : f \in A \setminus \{0\}\}$ the pole orders of A at P

Weierstrass semigroup

$\mathcal{X}$: projective, non-singular, geometrically irreducible curve

P: rational point of $\mathcal{X}$

A: the ring of functions on $\mathcal{X}$ with poles only at P

$\Lambda = \{-v_p(f) : f \in A \setminus \{0\}\}$ the pole orders of A at P

It holds

- $0 = -v_P(1) \in \Lambda$

Weierstrass semigroup

$\mathcal{X}$: projective, non-singular, geometrically irreducible curve

P: rational point of $\mathcal{X}$

A: the ring of functions on $\mathcal{X}$ with poles only at P

$\Lambda = \{-v_p(f) : f \in A \setminus \{0\}\}$ the pole orders of A at P

It holds

- $0 = -v_P(1) \in \Lambda$
- $(-v_P(f)) + (-v_P(g)) = (-v_P(fg)) \in \Lambda$ for all $f, g \in A$

Weierstrass semigroup

$\mathcal{X}$: projective, non-singular, geometrically irreducible curve

P: rational point of $\mathcal{X}$

A: the ring of functions on $\mathcal{X}$ with poles only at P

$\Lambda = \{-v_p(f) : f \in A \setminus \{0\}\}$ the pole orders of A at P

It holds

- $0 = -v_P(1) \in \Lambda$
- $(-v_P(f)) + (-v_P(g)) = (-v_P(fg)) \in \Lambda$ for all $f, g \in A$
- $\#(\mathbb{N}_0 \setminus \Lambda)$ = genus of $\mathcal{X}$ (finite)

Example

Klein quartic

$\chi : x^3y + y^3 + x = 0$

P : rational point with affine coordinates $x = 0, y = 0$

i	λ_i
0	0
1	3
2	5
3	6
4	7
5	8
6	9
7	10
8	11
⋮	⋮

Example

Hermitian curve over $\mathbb{F}_4$

$\chi : x^5 = y^4 + y$

P : the unique point at infinity

i	λ_i
0	0
1	4
2	5
3	8
4	9
5	10
6	12
7	13
⋮	⋮

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus
2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ
3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Frobenius' problem

Suppose we have coins of denominations $a_1, \ldots, a_n$



What is the largest monetary amount that can not be obtained using these coins?

Frobenius' problem

Suppose we have coins of denominations $a_1, \ldots, a_n$



What is the largest monetary amount that can not be obtained using these coins?

$n = 2$: Sylvester's formula $a_1 a_2 - a_1 - a_2$.

$n > 2$?

Frobenius' problem

Suppose we have coins of denominations $a_1, \ldots, a_n$



What is the largest monetary amount that can not be obtained using these coins?

$n = 2$: Sylvester's formula $a_1 a_2 - a_1 - a_2$.

$n > 2$?

Theorem (Curtis)

For $n \geq 3$, there is no simple closed-form algebraic formula for the Frobenius number.

F. Curtis, On formulas for the Frobenius number of a numerical semigroup, Mathematica Scandinavica, 1990.

Wilf's conjecture (1978)

$$c(\Lambda) \leqslant e(\Lambda) \cdot \#L(\Lambda)$$

H.S. Wilf. A Circle-Of-Lights Algorithm for the "Money-Changing Problem", The American Mathematical Monthly, 1978

... and many important contributions of Eliahou, Zhai, Dobbs, Matthews, Kaplan, Sammartano, Moscariello, Delgado, Fromentin, among others.

Wilf's conjecture (1978)

$$c(\Lambda) \leqslant e(\Lambda) \cdot \#L(\Lambda)$$

H.S. Wilf. A Circle-Of-Lights Algorithm for the "Money-Changing Problem", The American Mathematical Monthly, 1978

... and many important contributions of Eliahou, Zhai, Dobbs, Matthews, Kaplan, Sammartano, Moscariello, Delgado, Fromentin, among others.

The Eliahou constant of a semigroup S is $E(S) = k\#L(S) - qs + \rho$, if the Frobenius number of S is $qm - \rho - 1$ with $0 \leqslant \rho < m$, and the number of right minimum generators is $m - s$.

Any counterexample of the Wilf's conjecture would satisfy $E(S) < 0$.

S. Eliahou, Wilf 's conjecture and Macaulay's theorem, J. Eur. Math. Soc., 2018.

Wilf's conjecture (1978)

$$c(\Lambda) \leqslant e(\Lambda) \cdot \#L(\Lambda)$$

H.S. Wilf. A Circle-Of-Lights Algorithm for the "Money-Changing Problem", The American Mathematical Monthly, 1978

... and many important contributions of Eliahou, Zhai, Dobbs, Matthews, Kaplan, Sammartano, Moscariello, Delgado, Fromentin, among others.

The Eliahou constant of a semigroup S is $E(S) = k\#L(S) - qs + \rho$, if the Frobenius number of S is $qm - \rho - 1$ with $0 \leqslant \rho < m$, and the number of right minimum generators is $m - s$.

Any counterexample of the Wilf's conjecture would satisfy $E(S) < 0$.

S. Eliahou, Wilf 's conjecture and Macaulay's theorem, J. Eur. Math. Soc., 2018.

Semigroups with $E(S) < 0$ are extremely rare, but they exist (Only 7 semigroups of genus at most 65, being $n_{65} = 14386348925550$. The first one appears at genus 43).

Wilf's conjecture (1978)

$$c(\Lambda) \leqslant e(\Lambda) \cdot \#L(\Lambda)$$

H.S. Wilf. A Circle-Of-Lights Algorithm for the "Money-Changing Problem", The American Mathematical Monthly, 1978

... and many important contributions of Eliahou, Zhai, Dobbs, Matthews, Kaplan, Sammartano, Moscariello, Delgado, Fromentin, among others.

The Eliahou constant of a semigroup S is $E(S) = k\#L(S) - qs + \rho$, if the Frobenius number of S is $qm - \rho - 1$ with $0 \leqslant \rho < m$, and the number of right minimum generators is $m - s$.

Any counterexample of the Wilf's conjecture would satisfy $E(S) < 0$.

S. Eliahou, Wilf 's conjecture and Macaulay's theorem, J. Eur. Math. Soc., 2018.

Semigroups with $E(S) < 0$ are extremely rare, but they exist (Only 7 semigroups of genus at most 65, being $n_{65} = 14386348925550$. The first one appears at genus 43).

Researchers focused on the search of Eliahou counterexamples.

... and more contributions by Eliahou, Delgado, Fromentin, B., Marín

Hurwitz problems (1893)

- Determining whether there exist non-Weierstrass numerical semigroups, (Buchweitz, 1980, gave one)
- Characterizing Weierstrass semigroups

A. Hurwitz, “Über algebraische Gebilde mit eindeutigen Transformationen in sich”, Mathematische Annalen, 1893

Hurwitz problems (1893)

- Determining whether there exist non-Weierstrass numerical semigroups, (Buchweitz, 1980, gave one)
- Characterizing Weierstrass semigroups

  A. Hurwitz, “Über algebraische Gebilde mit eindeutigen Transformationen in sich”, Mathematische Annalen, 1893

- Unknown $\lim_{g\to\infty} \frac{W(g)}{n_g}$ (could be 0, 1, or any other constant, ...)
- All semigroups of genus $\leqslant 12$ are Weierstrass, there exists a non-Weierstrass semigroup of genus 13. (Eisenbud, Schreyer).

F. Torres. On certain N -sheeted coverings of curves and numerical semigroups which cannot be realized as Weierstrass semigroups. Comm. Algebra, 1995.

S.J. Kim. Semigroups which are not Weierstrass semigroups. Bull. Korean Math. Soc., 1996.

J. Komeda. Non-Weierstrass numerical semigroups. Semigroup Forum, 1998.

N. Kaplan and L. Ye. The proportion of Weierstrass semigroups, J. Algebra 2013.

D. Eisenbud and F.-O. Schreyer. Minimal non-Weierstrass semigroups, 2026.

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus
2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ
3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Counting semigroups by genus

Let n_g denote the number of numerical semigroups of genus g.

Counting semigroups by genus

Let n_g denote the number of numerical semigroups of genus g.

- $n_0 = 1$, since the unique numerical semigroup of genus 0 is $\mathbb{N}_0$

Counting semigroups by genus

Let n_g denote the number of numerical semigroups of genus g.

- $n_0 = 1$, since the unique numerical semigroup of genus 0 is $\mathbb{N}_0$
- $n_1 = 1$, since the unique numerical semigroup of genus 1 is



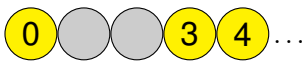
Counting semigroups by genus

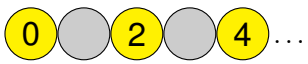
Let n_g denote the number of numerical semigroups of genus g.

- $n_0 = 1$, since the unique numerical semigroup of genus 0 is $\mathbb{N}_0$
- $n_1 = 1$, since the unique numerical semigroup of genus 1 is



- $n_2 = 2$. Indeed the unique numerical semigroups of genus 2 are





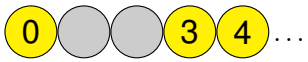
Counting semigroups by genus

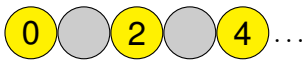
Let n_g denote the number of numerical semigroups of genus g.

- $n_0 = 1$, since the unique numerical semigroup of genus 0 is $\mathbb{N}_0$
- $n_1 = 1$, since the unique numerical semigroup of genus 1 is



- $n_2 = 2$. Indeed the unique numerical semigroups of genus 2 are





- $n_3 = 4$
- $n_4 = 7$
- $n_5 = 12$
- $n_6 = 23$
- $n_7 = 39$
- $n_8 = 67$

  ⋮

Conjecture

[B. 2008]

1. $n_g \geqslant n_{g-1} + n_{g-2}$
2.
   - $\lim_{g\to\infty} \frac{n_{g-1}+n_{g-2}}{n_g} = 1$
   - $\lim_{g\to\infty} \frac{n_g}{n_{g-1}} = \phi$

Counting semigroups by genus

Conjecture

[B. 2008]

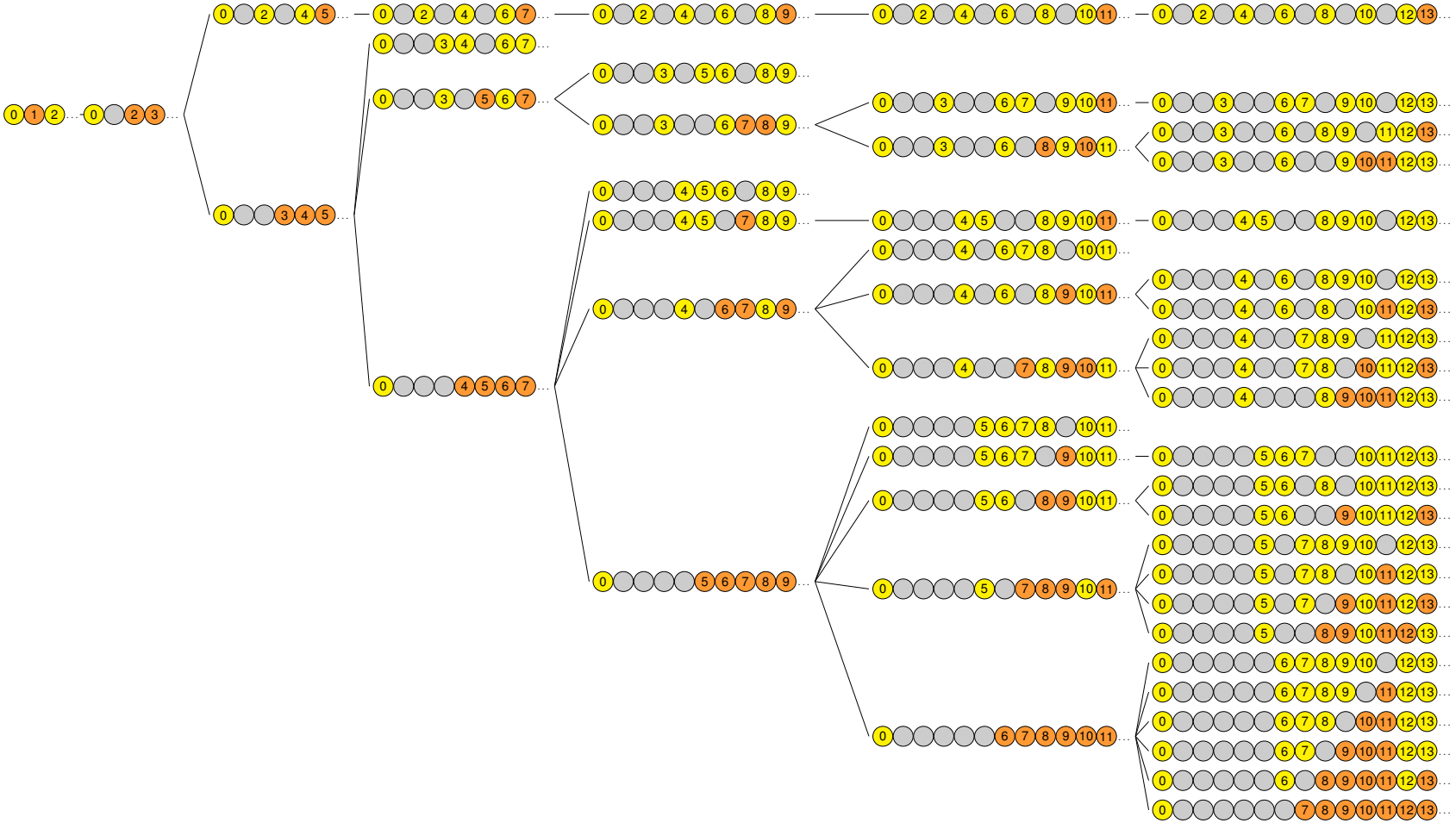
1. $n_g \geqslant n_{g-1} + n_{g-2}$
2. - $\lim_{g\to\infty} \frac{n_{g-1}+n_{g-2}}{n_g} = 1$
   - $\lim_{g\to\infty} \frac{n_g}{n_{g-1}} = \phi$

Weaker unsolved conjecture

[B. 2007] $n_g \leqslant n_{g+1}$



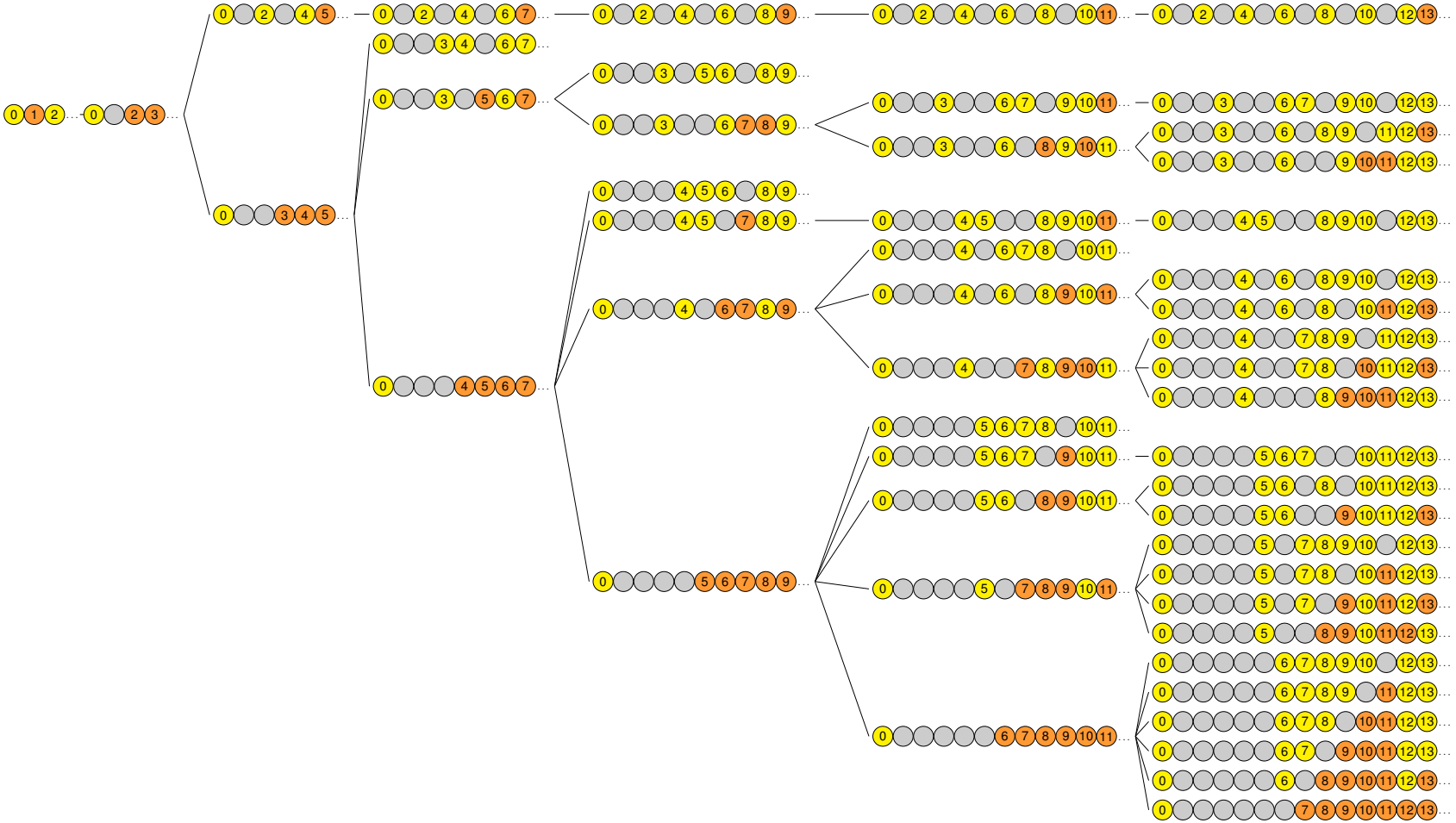
One main tool: Tree $\mathcal{T}$ of numerical semigroups



J. C. Rosales, P. A. García-Sánchez, J. I. García-García, and J. A. Jiménez-Madrid. Fundamental gaps in numerical semigroups. J. Pure Appl. Algebra, 2004.

The parent of Λ is obtained adjoining $F(\Lambda)$.

One main tool: Tree $\mathcal{T}$ of numerical semigroups



J. C. Rosales, P. A. García-Sánchez, J. I. García-García, and J. A. Jiménez-Madrid. Fundamental gaps in numerical semigroups. J. Pure Appl. Algebra, 2004.

The parent of Λ is obtained adjoining $F(\Lambda)$.

The children of Λ are obtained removing generators larger than $F(\Lambda)$.

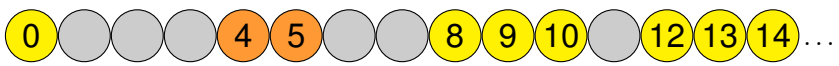
Tree $\mathcal{T}$ of numerical semigroups

If children$(\Lambda) \neq \varnothing$ for all Λ, then $n_g \leqslant n_{g+1}$ would follow immediately.

Tree $\mathcal{T}$ of numerical semigroups

If children$(\Lambda) \neq \varnothing$ for all Λ, then $n_g \leqslant n_{g+1}$ would follow immediately.

Observe:

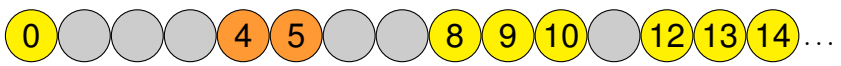


... has 0 descendants

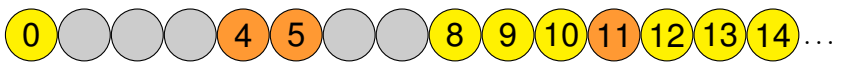
Tree $\mathcal{T}$ of numerical semigroups

If children(Λ) $\neq \varnothing$ for all Λ, then $n_g \leqslant n_{g+1}$ would follow immediately.

Observe:



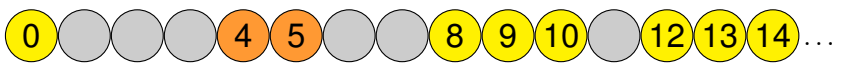
has 0 descendants



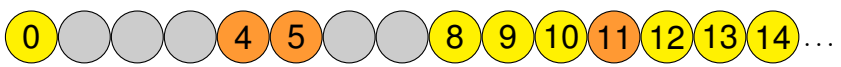
has 1 descendants

If children(Λ) $\neq \varnothing$ for all Λ, then $n_g \leqslant n_{g+1}$ would follow immediately.

Observe:



has 0 descendants



has 1 descendants

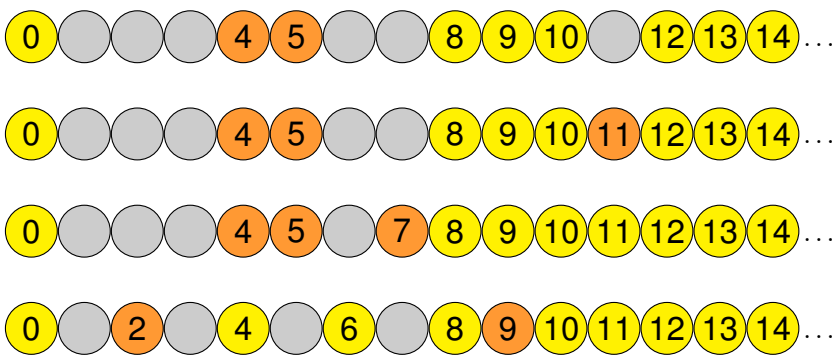


has 2 descendants

Tree $\mathcal{T}$ of numerical semigroups

If children$(\Lambda) \neq \varnothing$ for all Λ, then $n_g \leqslant n_{g+1}$ would follow immediately.

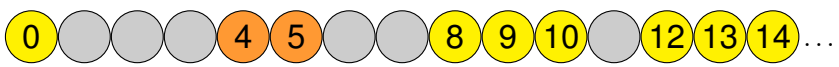
Observe:



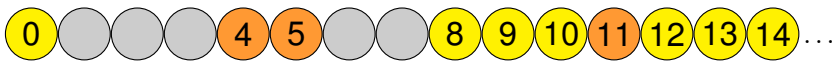
Tree $\mathcal{T}$ of numerical semigroups

If children$(\Lambda) \neq \varnothing$ for all Λ, then $n_g \leqslant n_{g+1}$ would follow immediately.

Observe:



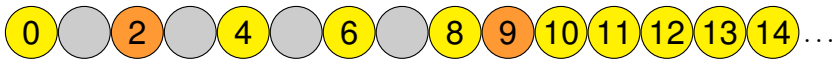
has 0 descendants



has 1 descendants



has 2 descendants



has ∞ descendants

Questions:

1. characterize infinite chains in the tree,
2. number of children of a node in terms of the number of siblings

What is known

- All terms up to $n_{80} = 19958375738706738 7 \simeq 2 \cdot 10^{17}$
  Last terms by Delgado, Eliahou, Fromentin, 2023, and B.-Torra, 2026.

What is known

- All terms up to $n_{80} = 19958375738706738 7 \simeq 2 \cdot 10^{17}$

  Last terms by Delgado, Eliahou, Fromentin, 2023, and B.-Torra, 2026.

  On-line encyclopedia of integer sequences: A007323

What is known

- All terms up to $n_{80} = 19958375738706738 7 \simeq 2 \cdot 10^{17}$

  Last terms by Delgado, Eliahou, Fromentin, 2023, and B.-Torra, 2026.

  On-line encyclopedia of integer sequences: A007323

- $\lim_{g\to\infty} \frac{n_g}{n_{g-1}} = \phi$

  Alex Zhai (2013) with important contributions of Nathan Kaplan and Yufei Zhao.

Counting semigroups by genus

- Semigroups can be represented by Dyck paths $\Longrightarrow n_g \leqslant \frac{1}{g+1}\binom{2g}{g}$

  B., A. de Mier: Representation of Numerical Semigroups by Dyck Paths, Semigroup Forum, 2007.

Counting semigroups by genus

- Semigroups can be represented by Dyck paths $\Longrightarrow n_g \leqslant \frac{1}{g+1}\binom{2g}{g}$

  B., A. de Mier: Representation of Numerical Semigroups by Dyck Paths, Semigroup Forum, 2007.

- $2F_g \leqslant n_g \leqslant 1 + 3 \cdot 2^{g-3}$

  B. Bounds on the Number of Numerical Semigroups of a Given Genus, Journal of Pure and Applied Algebra, 2009.

Counting semigroups by genus

- Semigroups can be represented by Dyck paths $\Longrightarrow n_g \leqslant \frac{1}{g+1}\binom{2g}{g}$

  B., A. de Mier: Representation of Numerical Semigroups by Dyck Paths, Semigroup Forum, 2007.

- $2F_g \leqslant n_g \leqslant 1 + 3 \cdot 2^{g-3}$

  B. Bounds on the Number of Numerical Semigroups of a Given Genus, Journal of Pure and Applied Algebra, 2009.

- $n_g \leqslant c_g$, where $\sum_{g \geqslant 1} c_g t^g = t\frac{2-3t+t^2-4t^3+3t^4-2t^5+t(1-t-t^3)\sqrt{(1+2t)/(1-2t)}}{2(1-3t+3t^2-3t^3+4t^4-3t^5+2t^6)}$

  S. Elizalde. Improved Bounds on the Number of Numerical Semigroups of a Given Genus, Journal of Pure and Applied Algebra, 2010.

Counting semigroups by genus

- Semigroups can be represented by Dyck paths $\Longrightarrow n_g \leqslant \frac{1}{g+1}\binom{2g}{g}$

  B., A. de Mier: Representation of Numerical Semigroups by Dyck Paths, Semigroup Forum, 2007.

- $2F_g \leqslant n_g \leqslant 1 + 3 \cdot 2^{g-3}$

  B. Bounds on the Number of Numerical Semigroups of a Given Genus, Journal of Pure and Applied Algebra, 2009.

- $n_g \leqslant c_g$, where $\sum_{g \geqslant 1} c_g t^g = t\frac{2-3t+t^2-4t^3+3t^4-2t^5+t(1-t-t^3)\sqrt{(1+2t)/(1-2t)}}{2(1-3t+3t^2-3t^3+4t^4-3t^5+2t^6)}$

  S. Elizalde. Improved Bounds on the Number of Numerical Semigroups of a Given Genus, Journal of Pure and Applied Algebra, 2010.

- $\#\{\text{num. semigr. of genus } g \text{ satisfying } F(S) < 2m(S)\} = F_{g+1}$.

  Y. Zhao. Constructing numerical semigroups of a given genus, Semigroup Forum, 2010.

Counting semigroups by genus

- Semigroups can be represented by Dyck paths $\Longrightarrow n_g \leqslant \frac{1}{g+1}\binom{2g}{g}$

  B., A. de Mier: Representation of Numerical Semigroups by Dyck Paths, Semigroup Forum, 2007.

- $2F_g \leqslant n_g \leqslant 1 + 3 \cdot 2^{g-3}$

  B. Bounds on the Number of Numerical Semigroups of a Given Genus, Journal of Pure and Applied Algebra, 2009.

- $n_g \leqslant c_g$, where $\sum_{g\geqslant 1} c_g t^g = t\frac{2-3t+t^2-4t^3+3t^4-2t^5+t(1-t-t^3)\sqrt{(1+2t)/(1-2t)}}{2(1-3t+3t^2-3t^3+4t^4-3t^5+2t^6)}$

  S. Elizalde. Improved Bounds on the Number of Numerical Semigroups of a Given Genus, Journal of Pure and Applied Algebra, 2010.

- $\#\{\text{num. semigr. of genus } g \text{ satisfying } F(S) < 2m(S)\} = F_{g+1}$.

  Y. Zhao. Constructing numerical semigroups of a given genus, Semigroup Forum, 2010.

- $\lim_{g\to\infty} \frac{\#\{\text{num. semigr. of genus } g \text{ satisfying } F(S)<3m(S)\}}{n_g} = 1$

  Conjectured by Y. Zhao, proved by A. Zhai.

  A. Zhai. Fibonacci-like growth of numerical semigroups of a given genus, Semigroup Forum, 2013

Counting semigroups by genus

- $\lim_{g\to\infty} \frac{n_g}{n_{g-1}} = \phi$

  A. Zhai. Fibonacci-like growth of numerical semigroups of a given genus, Semigroup Forum, 2013

Counting semigroups by genus

- $\lim_{g\to\infty} \frac{n_g}{n_{g-1}} = \phi$

  A. Zhai. Fibonacci-like growth of numerical semigroups of a given genus, Semigroup Forum, 2013

- If $2g < 3m$, then $n_{m,g} = n_{m-1,g-1} + n_{m-1,g-2}$

  N. Kaplan. Counting numerical semigroups by genus and some cases of a question of Wilf, 2012.

Counting semigroups by genus

- $\lim_{g\to\infty} \frac{n_g}{n_{g-1}} = \phi$

  A. Zhai. Fibonacci-like growth of numerical semigroups of a given genus, Semigroup Forum, 2013

- If $2g < 3m$, then $n_{m,g} = n_{m-1,g-1} + n_{m-1,g-2}$

  N. Kaplan. Counting numerical semigroups by genus and some cases of a question of Wilf, 2012.

- If $F + 1 \leqslant 3m$, then $n_{F,m,g} = n_{F-2,m-1,g-1} + n_{F-2,m-1,g-2}$

  B.- Torra. Multiparameter counting of numerical semigroups by Frobenius number, genus, and multiplicity, arXiv.

Counting semigroups by genus

- $\lim_{g\to\infty} \frac{n_g}{n_{g-1}} = \phi$

  A. Zhai. Fibonacci-like growth of numerical semigroups of a given genus, Semigroup Forum, 2013

- If $2g < 3m$, then $n_{m,g} = n_{m-1,g-1} + n_{m-1,g-2}$

  N. Kaplan. Counting numerical semigroups by genus and some cases of a question of Wilf, 2012.

- If $F + 1 \leqslant 3m$, then $n_{F,m,g} = n_{F-2,m-1,g-1} + n_{F-2,m-1,g-2}$

  B.- Torra. Multiparameter counting of numerical semigroups by Frobenius number, genus, and multiplicity, arXiv.

- $\lim_{g\to\infty} \frac{\#\{\text{numerical semigroups of genus } g \text{ and } h \text{ children}\}}{n_g} = \phi^{-h-2}$

  E. O'Dorney. Degree asymptotics of the numerical semigroup tree, 2013

Counting semigroups by genus

- $\lim_{g\to\infty} \frac{n_g}{n_{g-1}} = \phi$

  A. Zhai. Fibonacci-like growth of numerical semigroups of a given genus, Semigroup Forum, 2013

- If $2g < 3m$, then $\quad n_{m,g} = n_{m-1,g-1} + n_{m-1,g-2}$

  N. Kaplan. Counting numerical semigroups by genus and some cases of a question of Wilf, 2012.

- If $F + 1 \leqslant 3m$, then $\quad n_{F,m,g} = n_{F-2,m-1,g-1} + n_{F-2,m-1,g-2}$

  B.- Torra. Multiparameter counting of numerical semigroups by Frobenius number, genus, and multiplicity, arXiv.

- $\lim_{g\to\infty} \frac{\#\{\text{numerical semigroups of genus } g \text{ and } h \text{ children}\}}{n_g} = \phi^{-h-2}$

  E. O'Dorney. Degree asymptotics of the numerical semigroup tree, 2013

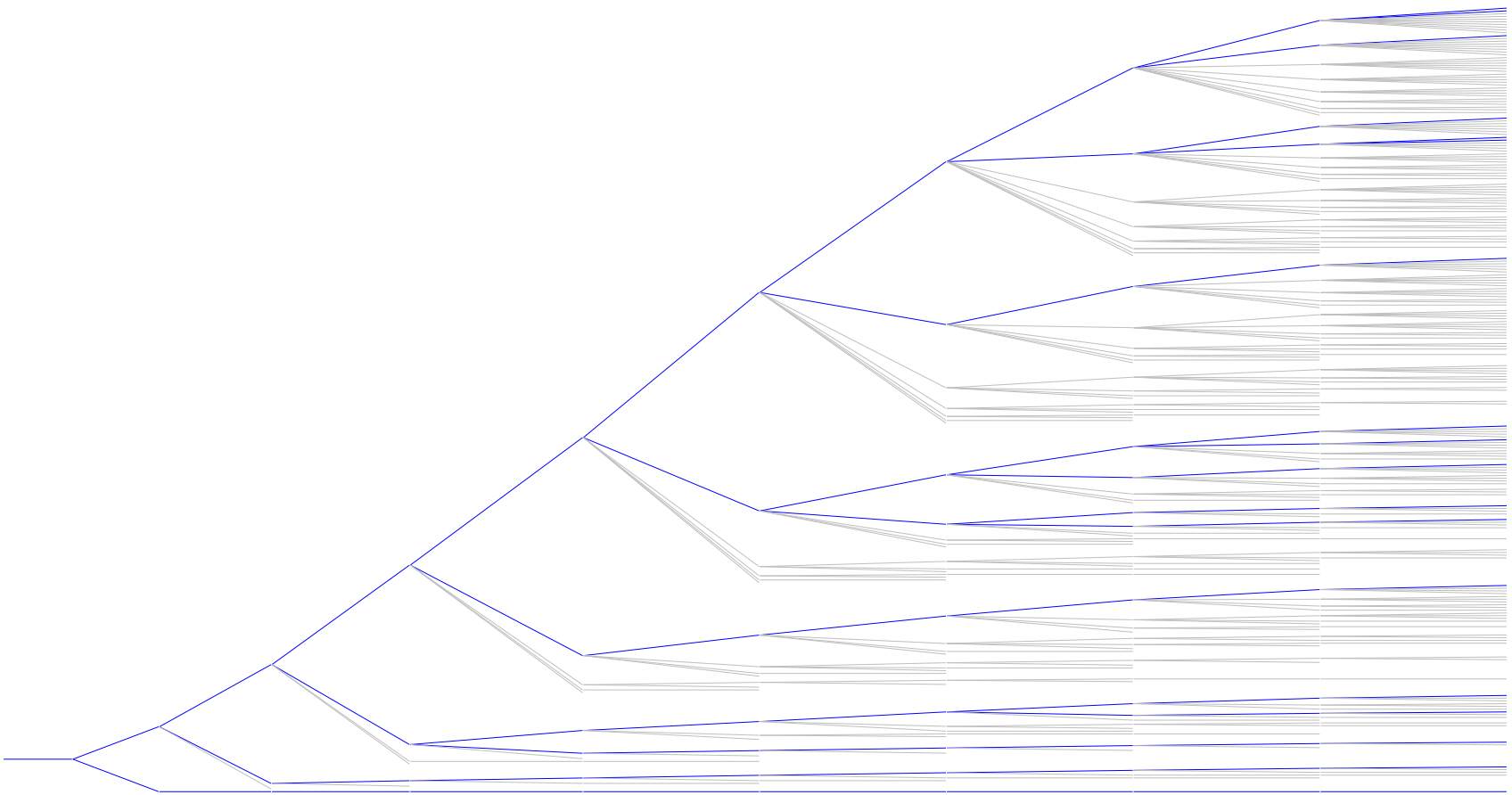
Since $\sum_{h\geqslant 0} h\phi^{-h-2} = \phi$, this implies again

$$\begin{aligned}\lim_{g\to\infty} \frac{n_{g+1}}{n_g} &= \lim_{g\to\infty} \sum_{h\geqslant 0} \frac{h \cdot \#\{\text{numerical semigroups of genus } g \text{ and } h \text{ children}\}}{n_g} \\ &= \sum_{h\geqslant 0} h \cdot \phi^{-h-2} = \phi\end{aligned}$$

Counting semigroups by genus

- $\lim_{g\to\infty} \frac{\#\{\text{numerical semigroups of genus } g \text{ in infinite chains}\}}{n_g} = 0$

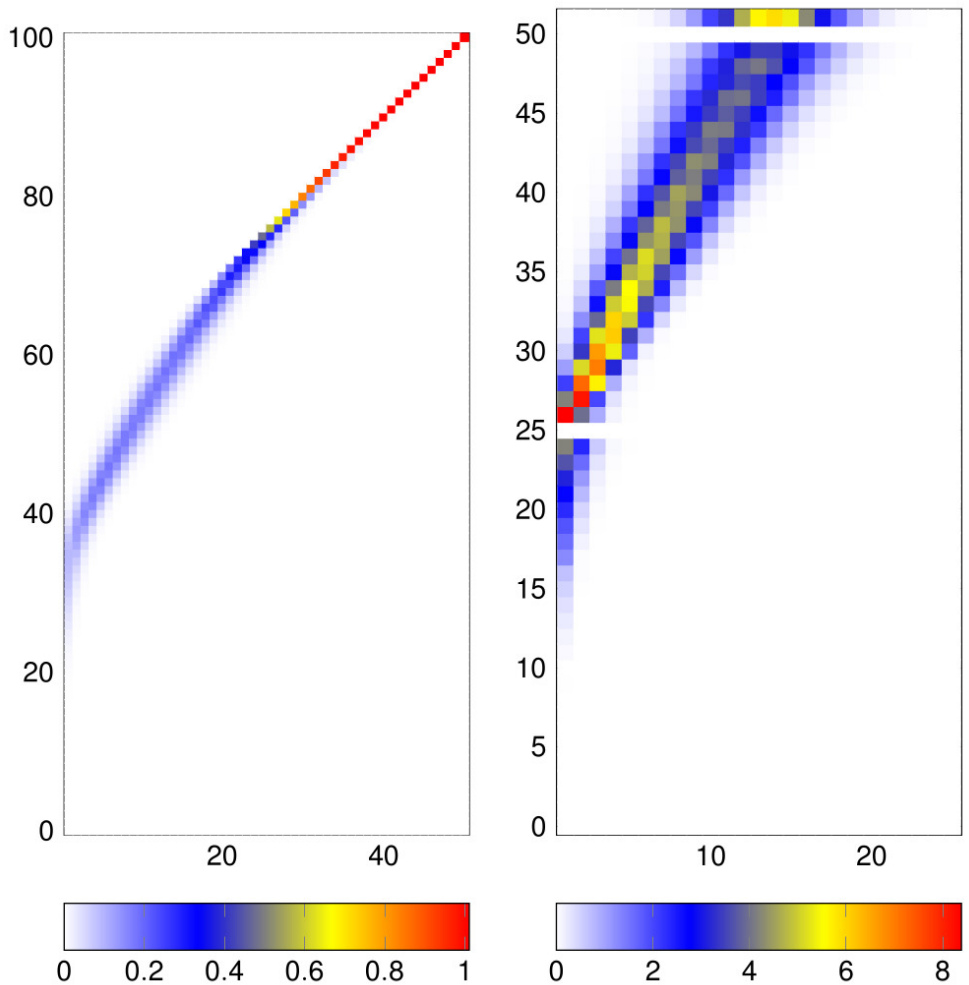
  B - M. Rosas-Ribeiro. Rarity of the infinite chains in the tree of numerical semigroups, Semigroup Forum, 2026.



Counting semigroups by genus

- Study of the asymptotic behavior of numerical semigroups

  B. and N. Kaplan D. Singhal. The shape of a random numerical semigroup, arXiv.



Counting semigroups by genus

Many efforts to compute n_g for large g:

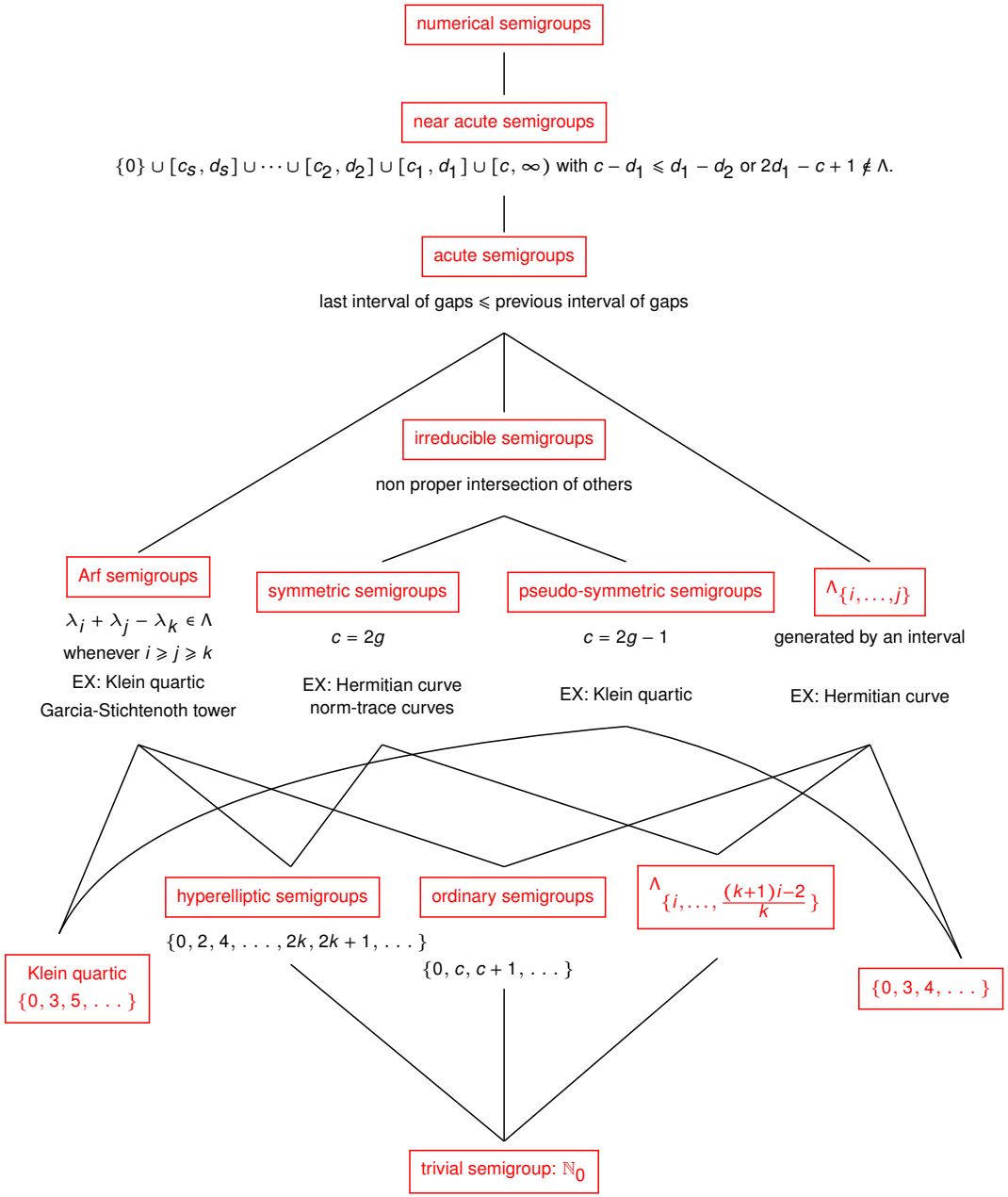
- N. Medeiros, B. (2008), M. Delgado: Brute approach
- B. (2009): Need to check only one new generator
- J.Fromentin-F.Hivert(2016): Decomposition numbers, parallelization, DFS
- B. - J. Fernández-González (2018): Seeds
- B. - J. Fernández-González (2020): Right-generators descendant
- B. (2024): Seeds revisited with n_{ggc}, bitwise ops, parallelization, DFS
- M. Delgado, S. Eliahou, J. Fromentin (2025): Distributed massive computation
- B. (2027): Unleaved tree with gcd-shrinking
- B.-V. Torra: Unleaved tree with seeds

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Classification



ν sequence

Given a numerical semigroup Λ define its ν sequence as

$$\nu_i = \#\{j \in \mathbb{N}_0 : \lambda_i - \lambda_j \in \Lambda\}$$

Given a numerical semigroup Λ define its ν sequence as

$$\nu_i = \#\{j \in \mathbb{N}_0 : \lambda_i - \lambda_j \in \Lambda\}$$

Example

Hermitian curve

i	λ_i	ν_i	
0	0	1	$\{0\}$
1	4	2	$\{0, 4\}$
2	5	2	$\{0, 5\}$
3	8	3	$\{0, 4, 8\}$
4	9	4	$\{0, 4, 5, 9\}$
5	10	3	$\{0, 5, 10\}$
6	12	4	$\{0, 4, 8, 12\}$
7	13	6	$\{0, 4, 5, 8, 9, 13\}$
8	14	6	$\{0, 4, 5, 9, 10, 14\}$
9	15	4	$\{0, 5, 10, 15\}$
10	16	5	$\{0, 4, 8, 12, 16\}$
$\vdots$	$\vdots$	$\vdots$	

τ sequence

Given a numerical semigroup Λ define its τ sequence as

$$\tau_i = \max\{j \in \mathbb{N}_0 : \text{ exists } k \text{ with } j \leqslant k \text{ and } \lambda_j + \lambda_k = \lambda_i\}$$

Given a numerical semigroup Λ define its τ sequence as

$$\tau_i = \max\{j \in \mathbb{N}_0 : \text{ exists } k \text{ with } j \leqslant k \text{ and } \lambda_j + \lambda_k = \lambda_i\}$$

Example

Hermitian curve

i	λ_i	τ_i	
0	0	0	$\{0\}$
1	4	0	$\{0, 4\}$
2	5	0	$\{0, 5\}$
3	8	1	$\{0, 4, 8\}$
4	9	1	$\{0, 4, 5, 9\}$
5	10	2	$\{0, 5, 10\}$
6	12	1	$\{0, 4, 8, 12\}$
7	13	2	$\{0, 4, 5, 8, 9, 13\}$
8	14	2	$\{0, 4, 5, 9, 10, 14\}$
9	15	2	$\{0, 5, 10, 15\}$
10	16	3	$\{0, 4, 8, 12, 16\}$
$\vdots$	$\vdots$	$\vdots$	

Semigroup characterization

Theorem

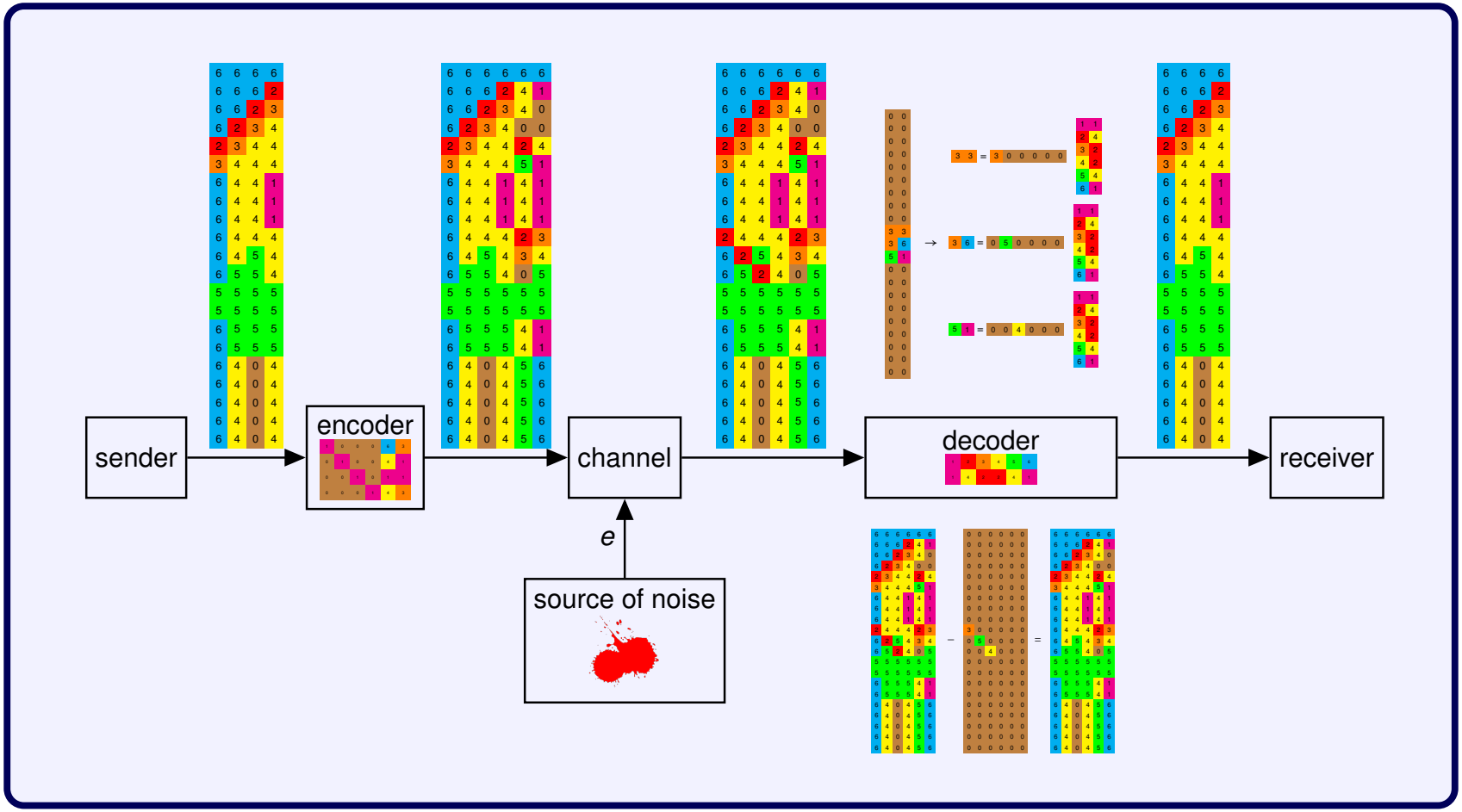
- *A numerical semigroup is completely determined by its*
  - ν *values*
  - τ *values*
- *No numerical semigroup can be determined by any finite subset of*
  - ν *values*
  - τ *values*

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

A Reed-Solomon code



Generalization

	Reed-Solomon codes	Algebraic-geometry codes (Goppa)
$\mathbb{Z}_p$	$\mathbb{F}_{q^d} = \mathbb{Z}_q[x]/m(x) = \mathbb{F}_q(\alpha)$	$\mathcal{X}(\mathbb{F}_{q^d})$
$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & (p-1) \\ 1^2 & 2^2 & \dots & (p-1)^2 \\ \vdots & \vdots & \vdots & \vdots \\ 1^r & 2^r & \dots & (p-1)^r \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^0 & \alpha^1 & \dots & \alpha^\ell \\ (\alpha^0)^2 & (\alpha^1)^2 & \dots & (\alpha^\ell)^2 \\ \vdots & \vdots & \vdots & \vdots \\ (\alpha^0)^r & (\alpha^1)^r & \dots & (\alpha^\ell)^r \end{pmatrix}$	$\begin{pmatrix} f_0(P_1) & f_0(P_2) & \dots & f_0(P_n) \\ f_1(P_1) & f_1(P_2) & \dots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \dots & f_2(P_n) \\ \vdots & \vdots & \vdots & \vdots \\ f_r(P_!) & f_r(P_2) & \dots & f_r(P_n) \end{pmatrix}$

Reed-Solomon codes

Reed-Solomon codes have been the most popular, historically and nowadays:

- Storage (CD, DVD, etc.)
- Space transmissions
- Mobile communications
- QR codes



1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Definition

Consider

- χ a projective curve without singularities over $\mathbb{F}_q$
- P a rational point in χ
- A the ring of functions on χ with poles only at P
- Λ the Weierstrass semigroup at P
- λ enumeration of Λ $(\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \ldots\})$

Definition

Consider

- χ a projective curve without singularities over $\mathbb{F}_q$
- P a rational point in χ
- A the ring of functions on χ with poles only at P
- Λ the Weierstrass semigroup at P
- λ enumeration of Λ $(\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \ldots\})$
- $\{f_i : i \in \mathbb{N}_0, f_i \in A, -v_P(f_i) = \lambda_i\}$.

Definition

Consider

- χ a projective curve without singularities over $\mathbb{F}_q$
- P a rational point in χ
- A the ring of functions on χ with poles only at P
- Λ the Weierstrass semigroup at P
- λ enumeration of Λ $(\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \ldots\})$
- $\{f_i : i \in \mathbb{N}_0, f_i \in A, -v_P(f_i) = \lambda_i\}$.
- $P_1, P_2, \ldots, P_n$ rational points in χ different from P

Definition

Consider

- χ a projective curve without singularities over $\mathbb{F}_q$
- P a rational point in χ
- A the ring of functions on χ with poles only at P
- Λ the Weierstrass semigroup at P
- λ enumeration of Λ $(\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \ldots\})$
- $\{f_i : i \in \mathbb{N}_0, f_i \in A, -v_P(f_i) = \lambda_i\}$.
- $P_1, P_2, \ldots, P_n$ rational points in χ different from P
- $ev : A \longrightarrow \mathbb{F}_q^n,\ f \mapsto (f(P_1), \ldots, f(P_n))$.

Definition

Consider

- χ a projective curve without singularities over $\mathbb{F}_q$
- P a rational point in χ
- A the ring of functions on χ with poles only at P
- Λ the Weierstrass semigroup at P
- λ enumeration of Λ $(\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \ldots\})$
- $\{f_i : i \in \mathbb{N}_0, f_i \in A, -v_P(f_i) = \lambda_i\}$.
- $P_1, P_2, \ldots, P_n$ rational points in χ different from P
- $ev : A \longrightarrow \mathbb{F}_q^n,\ f \mapsto (f(P_1), \ldots, f(P_n))$.

Define

$C_i = \{ev(f) : f \in A, -v_P(f) \leqslant \lambda_i\}^{\perp}$ for $i \in \mathbb{N}_0$ (standard)

Definition

Consider

- χ a projective curve without singularities over $\mathbb{F}_q$
- P a rational point in χ
- A the ring of functions on χ with poles only at P
- Λ the Weierstrass semigroup at P
- λ enumeration of Λ $(\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \ldots\})$
- $\{f_i : i \in \mathbb{N}_0, f_i \in A, -v_P(f_i) = \lambda_i\}$.
- $P_1, P_2, \ldots, P_n$ rational points in χ different from P
- $ev : A \longrightarrow \mathbb{F}_q^n,\ f \mapsto (f(P_1), \ldots, f(P_n))$.

Define

$$C_i = \{ev(f) : f \in A, -v_P(f) \leqslant \lambda_i\}^\perp \quad \text{for } i \in \mathbb{N}_0 \text{ (standard)}$$
$$= \{ev(f) : f \in L(\lambda_i P)\}^\perp$$

Definition

Consider

- χ a projective curve without singularities over $\mathbb{F}_q$
- P a rational point in χ
- A the ring of functions on χ with poles only at P
- Λ the Weierstrass semigroup at P
- λ enumeration of Λ $(\Lambda = \{\lambda_0 = 0 < \lambda_1 < \lambda_2 \ldots\})$
- $\{f_i : i \in \mathbb{N}_0, f_i \in A, -v_P(f_i) = \lambda_i\}$.
- $P_1, P_2, \ldots, P_n$ rational points in χ different from P
- $ev : A \longrightarrow \mathbb{F}_q^n,\ f \mapsto (f(P_1), \ldots, f(P_n))$.

Define

$$C_i = \{ev(f) : f \in A, -v_P(f) \leqslant \lambda_i\}^\perp \quad \text{for } i \in \mathbb{N}_0 \text{ (standard)}$$
$$= \{ev(f) : f \in L(\lambda_i P)\}^\perp$$

$$C_R = \langle ev(f_i) : i \in R\rangle^\perp \quad \text{for } R \subseteq \mathbb{N}_0$$

Example

Consider $\mathbb{F}_{4^2} = \mathbb{Z}_2[x]/(x^4 + x + 1)$. Let α be the class of x.

The Hermitian curve with affine equation $x^5 = y^4 + y$ over $\mathbb{F}_{4^2}$ has one point P at infinity and 64 more affine points

$P_1 = (0, 0)$ $P_2 = (0, 1)$ $P_3 = (0, \alpha^5)$ $P_4 = (0, \alpha^{10})$

$P_5 = (1, \alpha)$ $P_6 = (1, \alpha^2)$ $P_7 = (1, \alpha^4)$ $P_8 = (1, \alpha^8)$

$P_9 = (\alpha^3, \alpha)$ $P_{10} = (\alpha^3, \alpha^2)$ $P_{11} = (\alpha^3, \alpha^4)$ $P_{12} = (\alpha^3, \alpha^8)$

$P_{13} = (\alpha^{12}, \alpha)$ $P_{14} = (\alpha^{12}, \alpha^2)$ $P_{15} = (\alpha^{12}, \alpha^4)$ $P_{16} = (\alpha^{12}, \alpha^8)$

...

In this case, the basis functions are

$f_0 = 1$, $f_1 = x$, $f_2 = y$, $f_3 = x^2$, $f_4 = xy$, $f_5 = y^2$, $f_6 = x^3$, $f_7 = x^2y$, $f_8 = xy^2$, $f_9 = y^3 \ldots$

Then

$$\begin{pmatrix} ev(f_0) \\ ev(f_1) \\ ev(f_2) \\ ev(f_3) \\ ev(f_4) \\ ev(f_5) \\ ev(f_6) \\ ev(f_7) \\ ev(f_8) \\ ev(f_9) \\ \vdots \end{pmatrix} = \begin{pmatrix} ev(1) \\ ev(x) \\ ev(y) \\ ev(x^2) \\ ev(xy) \\ ev(y^2) \\ ev(x^3) \\ ev(x^2y) \\ ev(xy^2) \\ ev(y^3) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \ldots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^{12} & \alpha^{12} & \alpha^{12} & \alpha^{12} & \ldots \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \ldots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \ldots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^4 & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha & \alpha^5 & \ldots \\ 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \ldots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \ldots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^7 & \alpha^8 & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{11} & \alpha^{13} & \alpha^2 & \ldots \\ 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^4 & \alpha^{14} & \alpha & \alpha^5 & \alpha^{13} & \ldots \\ 0 & 1 & 1 & 1 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \ldots \\ & & & & & & & & \vdots & & & & & & & & \end{pmatrix}$$

Example

C_3 is the code with parity check matrix

$$\begin{pmatrix} ev(f_0) \\ ev(f_1) \\ ev(f_2) \\ ev(f_3) \\ ev(f_4) \\ ev(f_5) \\ ev(f_6) \\ ev(f_7) \\ ev(f_8) \\ ev(f_9) \\ \vdots \end{pmatrix} = \begin{pmatrix} ev(1) \\ ev(x) \\ ev(y) \\ ev(x^2) \\ ev(xy) \\ ev(y^2) \\ ev(x^3) \\ ev(x^2y) \\ ev(xy^2) \\ ev(y^3) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^{12} & \alpha^{12} & \alpha^{12} & \alpha^{12} & \dots \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^4 & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha & \alpha^5 & \dots \\ 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^7 & \alpha^8 & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{11} & \alpha^{13} & \alpha^2 & \dots \\ 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^4 & \alpha^{14} & \alpha & \alpha^5 & \alpha^{13} & \dots \\ 0 & 1 & 1 & 1 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \dots \\ & & & & & & & & \vdots & & & & & & & & \end{pmatrix}$$

For $R = \{0, 3, 4, 6\}$, C_R is the code with parity check matrix

$$\begin{pmatrix} ev(f_0) \\ ev(f_1) \\ ev(f_2) \\ ev(f_3) \\ ev(f_4) \\ ev(f_5) \\ ev(f_6) \\ ev(f_7) \\ ev(f_8) \\ ev(f_9) \\ \vdots \end{pmatrix} = \begin{pmatrix} ev(1) \\ ev(x) \\ ev(y) \\ ev(x^2) \\ ev(xy) \\ ev(y^2) \\ ev(x^3) \\ ev(x^2y) \\ ev(xy^2) \\ ev(y^3) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^{12} & \alpha^{12} & \alpha^{12} & \alpha^{12} & \dots \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^4 & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha & \alpha^5 & \dots \\ 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^7 & \alpha^8 & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{11} & \alpha^{13} & \alpha^2 & \dots \\ 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^4 & \alpha^{14} & \alpha & \alpha^5 & \alpha^{13} & \dots \\ 0 & 1 & 1 & 1 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \dots \\ & & & & & & & & \vdots & & & & & & & & \end{pmatrix}$$

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Generic errors

The points $P_{i_1}, \ldots, P_{i_t}$ are generically distributed if no element $f \in A$ with $-v_P(f) < \lambda_t$ vanishes in all of them.

The points $P_{i_1}, \ldots, P_{i_t}$ are generically distributed if no element $f \in A$ with $-v_P(f) < \lambda_t$ vanishes in all of them.

Example

In the Hermitian curve, non-generically distributed sets of points are: 2 points if they lie in the same horizontal line.



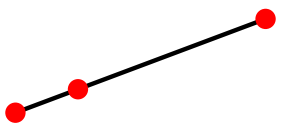
The points $P_{i_1}, \ldots, P_{i_t}$ are generically distributed if no element $f \in A$ with $-v_P(f) < \lambda_t$ vanishes in all of them.

Example

In the Hermitian curve, non-generically distributed sets of points are:
2 points if they lie in the same horizontal line.



3 points if they lie in a line of any kind (colinear)



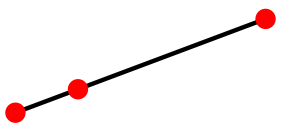
The points $P_{i_1}, \ldots, P_{i_t}$ are generically distributed if no element $f \in A$ with $-v_P(f) < \lambda_t$ vanishes in all of them.

Example

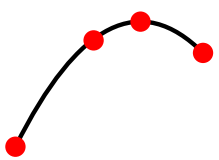
In the Hermitian curve, non-generically distributed sets of points are:
2 points if they lie in the same horizontal line.



3 points if they lie in a line of any kind (colinear)



4 point if they lie in a quadric of the form $ax^2 + bx + cy + d = 0$.



Generic errors

Definition

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

Generic errors

Definition

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

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

Generic errors

Definition

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

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

By restricting the errors to be corrected to generic errors one has weaker decoding requirements and still can correct almost all errors.

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Correction capability of Berlekamp-Massey-Sakata algorithm with majority voting

Theorem

[Feng, Rao, 1995]
All error vectors of weight t can be corrected by C_R if R contains all i with $\nu_i < 2t + 1$.

In particular, $d(C) \geqslant \delta(C) := \min\{\nu_i : i \notin R\}$ (order bound).

Correction capability of Berlekamp-Massey-Sakata algorithm with majority voting

Theorem

[Feng, Rao, 1995]
All error vectors of weight t can be corrected by C_R if R contains all i with $\nu_i < 2t + 1$.

In particular, $d(C) \geqslant \delta(C) := \min\{\nu_i : i \notin R\}$ (order bound).

Theorem

[Bras-Amorós, O'Sullivan, 2006]
All generic error vectors of weight t can be corrected by C_R if R contains all i with $\tau_i < t$.

Correction capability optimized codes

Codes for correcting t errors of any kind

Take R equal to

$\widetilde{R}(t) = \{i \in \mathbb{N}_0 : \nu_i < 2t + 1\}$ (Feng–Rao improved codes)

$R(t) = \{i \in \mathbb{N}_0 : i \leqslant i(t)\}$, where $i(t) = \max \widetilde{R}(t)$ (standard)

Example of Hermitian codes

Suppose we want to correct $t = 2$ errors of any kind.

i	λ_i	ν_i	
0	0	1	←
1	4	2	←
2	5	2	←
3	8	3	←
4	9	4	←
5	10	3	←
6	12	4	←
7	13	6	
8	14	6	
9	15	4	←
10	16	5	
...	...	...	

We can take

$\widetilde{R}(t) = \{i : \nu_i < 5\} = \{0, 1, 2, 3, 4, 5, 6, 9\}$

or the standard code C_9.

$$\begin{pmatrix} ev(f_0) \\ ev(f_1) \\ ev(f_2) \\ ev(f_3) \\ ev(f_4) \\ ev(f_5) \\ ev(f_6) \\ ev(f_7) \\ ev(f_8) \\ ev(f_9) \\ \vdots \end{pmatrix} = \begin{pmatrix} ev(1) \\ ev(x) \\ ev(y) \\ ev(x^2) \\ ev(xy) \\ ev(y^2) \\ ev(x^3) \\ ev(x^2y) \\ ev(xy^2) \\ ev(y^3) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^{12} & \alpha^{12} & \alpha^{12} & \alpha^{12} & \dots \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^4 & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha & \alpha^5 & \dots \\ 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^7 & \alpha^8 & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{11} & \alpha^{13} & \alpha^2 & \dots \\ 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^4 & \alpha^{14} & \alpha & \alpha^5 & \alpha^{13} & \dots \\ 0 & 1 & 1 & 1 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \dots \\ & & & & & & & & \vdots & & & & & & & & \end{pmatrix}$$

$$\begin{pmatrix} ev(f_0) \\ ev(f_1) \\ ev(f_2) \\ ev(f_3) \\ ev(f_4) \\ ev(f_5) \\ ev(f_6) \\ ev(f_7) \\ ev(f_8) \\ ev(f_9) \\ \vdots \end{pmatrix} = \begin{pmatrix} ev(1) \\ ev(x) \\ ev(y) \\ ev(x^2) \\ ev(xy) \\ ev(y^2) \\ ev(x^3) \\ ev(x^2y) \\ ev(xy^2) \\ ev(y^3) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^{12} & \alpha^{12} & \alpha^{12} & \alpha^{12} & \dots \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^4 & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha & \alpha^5 & \dots \\ 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^7 & \alpha^8 & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{11} & \alpha^{13} & \alpha^2 & \dots \\ 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^4 & \alpha^{14} & \alpha & \alpha^5 & \alpha^{13} & \dots \\ 0 & 1 & 1 & 1 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \dots \\ & & & & & & & & \vdots & & & & & & & & \end{pmatrix}$$

Correction capability optimized codes

Codes for correcting t generic errors

Take R equal to

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

$R^*(t) = \{i \in \mathbb{N}_0 : i \leqslant i^*(t)\}$, where $i^*(t) = \max \widetilde{R}^*(t)$ (standard)

Example of Hermitian codes

Suppose we want to correct $t = 2$ errors of generic type.

i	λ_i	τ_i	
0	0	0	←
1	4	0	←
2	5	0	←
3	8	1	←
4	9	1	←
5	10	2	
6	12	1	←
7	13	2	
8	14	2	
9	15	2	
10	16	3	
...	...	...	

We can take

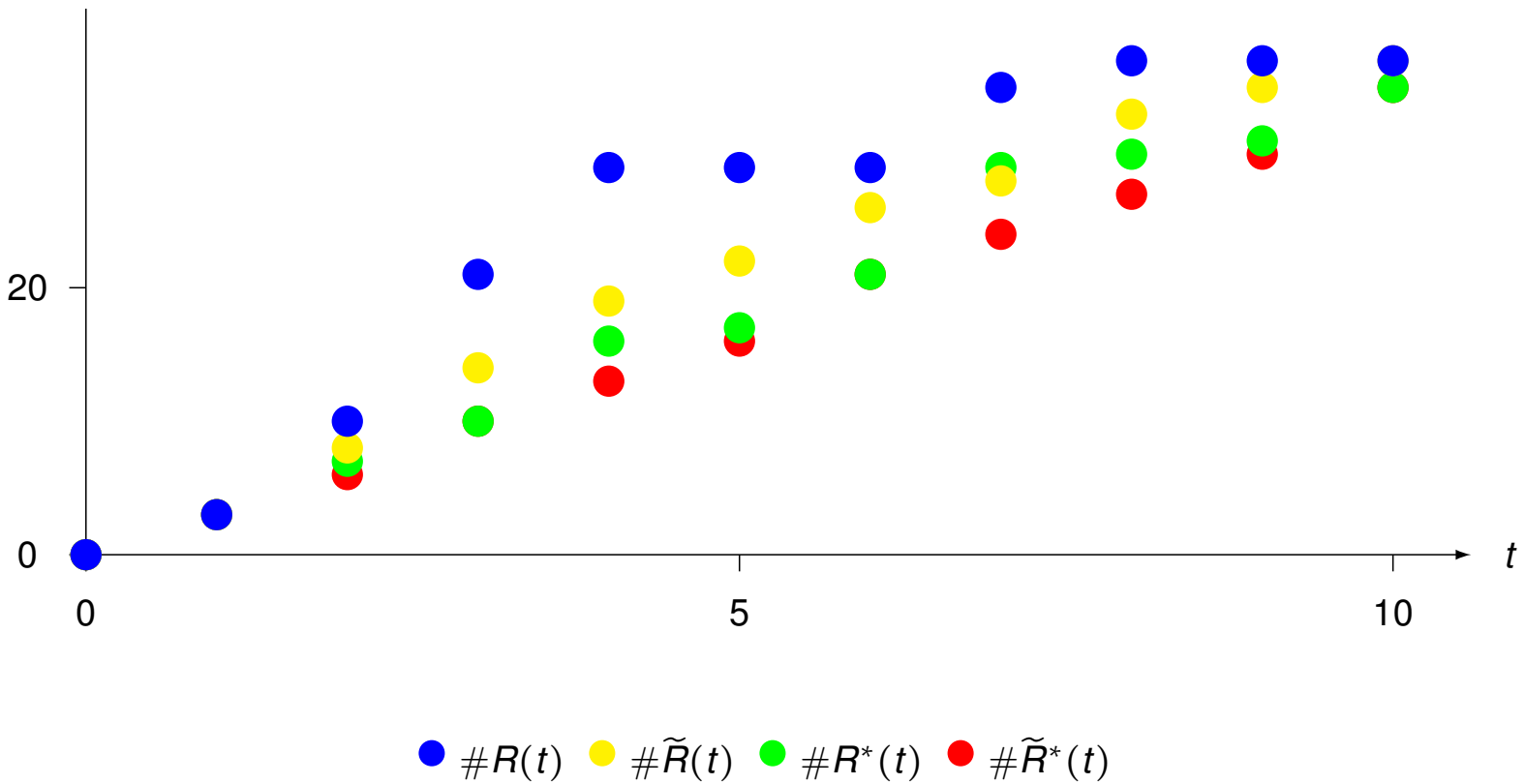
$\widetilde{R}^*(t) = \{i : \tau_i < 2\} = \{0, 1, 2, 3, 4, 6\}$

or the standard code C_6.

$$\begin{pmatrix} ev(f_0) \\ ev(f_1) \\ ev(f_2) \\ ev(f_3) \\ ev(f_4) \\ ev(f_5) \\ ev(f_6) \\ ev(f_7) \\ ev(f_8) \\ ev(f_9) \\ \vdots \end{pmatrix} = \begin{pmatrix} ev(1) \\ ev(x) \\ ev(y) \\ ev(x^2) \\ ev(xy) \\ ev(y^2) \\ ev(x^3) \\ ev(x^2y) \\ ev(xy^2) \\ ev(y^3) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^{12} & \alpha^{12} & \alpha^{12} & \alpha^{12} & \dots \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^4 & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha & \alpha^5 & \dots \\ 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^7 & \alpha^8 & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{11} & \alpha^{13} & \alpha^2 & \dots \\ 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^4 & \alpha^{14} & \alpha & \alpha^5 & \alpha^{13} & \dots \\ 0 & 1 & 1 & 1 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \dots \\ & & & & & & & & \vdots & & & & & & & & \end{pmatrix}$$

$$\begin{pmatrix} ev(f_0) \\ ev(f_1) \\ ev(f_2) \\ ev(f_3) \\ ev(f_4) \\ ev(f_5) \\ ev(f_6) \\ ev(f_7) \\ ev(f_8) \\ ev(f_9) \\ \vdots \end{pmatrix} = \begin{pmatrix} ev(1) \\ ev(x) \\ ev(y) \\ ev(x^2) \\ ev(xy) \\ ev(y^2) \\ ev(x^3) \\ ev(x^2y) \\ ev(xy^2) \\ ev(y^3) \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^3 & \alpha^{12} & \alpha^{12} & \alpha^{12} & \alpha^{12} & \dots \\ 0 & 1 & \alpha^5 & \alpha^{10} & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^4 & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^{13} & \alpha^{14} & \alpha & \alpha^5 & \dots \\ 0 & 1 & \alpha^{10} & \alpha^5 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \dots \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^9 & \alpha^6 & \alpha^6 & \alpha^6 & \alpha^6 & \dots \\ 0 & 0 & 0 & 0 & \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^7 & \alpha^8 & \alpha^{10} & \alpha^{14} & \alpha^{10} & \alpha^{11} & \alpha^{13} & \alpha^2 & \dots \\ 0 & 0 & 0 & 0 & \alpha^2 & \alpha^4 & \alpha^8 & \alpha & \alpha^5 & \alpha^7 & \alpha^{11} & \alpha^4 & \alpha^{14} & \alpha & \alpha^5 & \alpha^{13} & \dots \\ 0 & 1 & 1 & 1 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^9 & \dots \\ & & & & & & & & \vdots & & & & & & & & \end{pmatrix}$$

Hermitian codes redundancy ($\mathbb{F}_{72}$)



Correction capability optimized codes

Increasingness of ν	$\longleftrightarrow$	Compare $\widetilde{R}(t)$ and $R(t)$
Increasingness of τ	$\longleftrightarrow$	Compare $\widetilde{R}^*(t)$ and $R^*(t)$
Compare $\lfloor \frac{\nu-1}{2} \rfloor$ and τ	$\longleftrightarrow$	Compare $\widetilde{R}^*(t)$ and $\widetilde{R}(t)$

Correction capability optimized codes

$$
\begin{array}{rcl}
\text{Increasingness of } \nu & \longleftrightarrow & \text{Compare } \widetilde{R}(t) \text{ and } R(t) \\
\text{Increasingness of } \tau & \longleftrightarrow & \text{Compare } \widetilde{R}^*(t) \text{ and } R^*(t) \\
\text{Compare } \lfloor \frac{\nu-1}{2} \rfloor \text{ and } \tau & \longleftrightarrow & \text{Compare } \widetilde{R}^*(t) \text{ and } \widetilde{R}(t)
\end{array}
$$

Study of $\nu \longleftrightarrow$ order bound: $d(C) \geqslant \delta(C) := \min\{\nu_i : i \notin R\}$

Increasingness of ν and τ

Theorem

- *The unique semigroups for which ν is non-decreasing are ordinary semigroups.*
- *The unique semigroups for which τ is non-decreasing are ordinary semigroups.*

Consequently,

- $R(t) = \widetilde{R}(t)$ for all $t \geqslant 0$ if and only if Λ is ordinary
- $R^*(t) = \widetilde{R}^*(t)$ for all $t \geqslant 0$ if and only if Λ is ordinary

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.

Lemma

- $\tau_i \geqslant \left\lfloor \frac{\nu_i - 1}{2} \right\rfloor$ for all $i \in \mathbb{N}_0$
- $\tau_i = \left\lfloor \frac{\nu_i - 1}{2} \right\rfloor$ for all $i \geqslant 2c - g - 1$
- $\tau_i = \left\lfloor \frac{\nu_i - 1}{2} \right\rfloor$ 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* $t \in \mathbb{N}_0$ *if and only if the associated numerical semigroup is Arf.*

Furthermore, it can be proved that $\widetilde{R}^*(t) = \widetilde{R}(t)$ for all $t \geqslant c - g$.

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Length of codes

The length of one-point AG codes (and AG codes in general) is bounded by the number of rational points over $\mathbb{F}_q$ of the defining curve.

- Bound depending on the genus of the curve:
  - Serre-Hasse-Weil:

$$N_q(g) \leqslant q + 1 + g\lfloor 2\sqrt{q} \rfloor$$

Length of codes

The length of one-point AG codes (and AG codes in general) is bounded by the number of rational points over $\mathbb{F}_q$ of the defining curve.

- Bound depending on the genus of the curve:
  - Serre-Hasse-Weil:

$$N_q(g) \leqslant q + 1 + g\lfloor 2\sqrt{q} \rfloor$$

- Bounds depending on Weierstrass semigroups:
  - Lewittes:

$$N_q(\Lambda) \leqslant L_q(\Lambda) = q\lambda_1 + 1$$

  - Geil-Matsumoto:

$$N_q(\Lambda) \leqslant GM_q(\Lambda) = \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1$$

A closed formula for GM bound for semigroups with two generators

Lemma

The Geil-Matsumoto bound for the semigroup generated by a and b with $a < b$ is:

$$
\begin{aligned}
GM_q(\langle a, b\rangle) &= 1 + \sum_{n=0}^{a-1} \min\left(q, \left\lceil \frac{q-n}{a} \right\rceil \cdot b\right) \\
&= \begin{cases} 1 + qa & \text{if } q \leqslant \lfloor \frac{q}{a} \rfloor b \\ 1 + (q \bmod a)q + (a - (q \bmod a))\lfloor \frac{q}{a} \rfloor b & \text{if } \lfloor \frac{q}{a} \rfloor b < q \leqslant \lceil \frac{q}{a} \rceil b \\ 1 + ab\lceil \frac{q}{a} \rceil - (a - (q \bmod a))b & \text{if } q > \lceil \frac{q}{a} \rceil b \end{cases}
\end{aligned}
$$

Lemma

It holds

$$GM_q(\langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle) = L_q(\langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle) = q\lambda_1 + 1$$

if and only if $q(\lambda_i - \lambda_1) \in \Lambda$ for all i with $2 \leqslant i \leqslant n$

Lemma

If $q \leqslant \left\lfloor \frac{q}{\lambda_1} \right\rfloor \lambda_2$ then

$$GM_q(\langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle) = L_q(\langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle) = q\lambda_1 + 1$$

1. **Basic notions**
   - Genus, Frobenius number, multiplicity, gapsets
   - Gapsets
   - Weierstrass semigroup
   - Classical problems
   - Counting by genus

2. **Classification and characterization of numerical semigroups**
   - Classification
   - Characterization by ν and τ

3. **Error correcting codes**
   - The coding paradigm
   - One-point AG codes
   - Generic errors
   - Correction capability, ν sequence, τ sequence, code dimension
   - Geil-Matsumoto bound and the length of AG codes
   - Isometry-dual flags of one-point AG codes

Isometric linear codes

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

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

Two linear 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

$\{(0,0,0,0),(0,0,1,2),(0,0,2,1),(1,2,0,0),(1,2,1,2),(1,2,2,1),(2,1,0,0),(2,1,1,2),(2,1,2,1)\}$
$\{(0,0,0,0),(0,0,1,1),(0,0,2,2),(1,1,0,0),(1,1,1,1),(1,1,2,2),(2,2,0,0),(2,2,1,1),(2,2,2,2)\}$
are $(1,2,1,2)$-isometric In $\mathbb{F}_3^4$.

Sequences of pairwise isometric codes

$$C_0 \subseteq C_1 \subseteq \ldots \subseteq C_{n-1} \subseteq C_n$$

Sequences of pairwise isometric codes

$$C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{n-1} \subseteq C_n$$

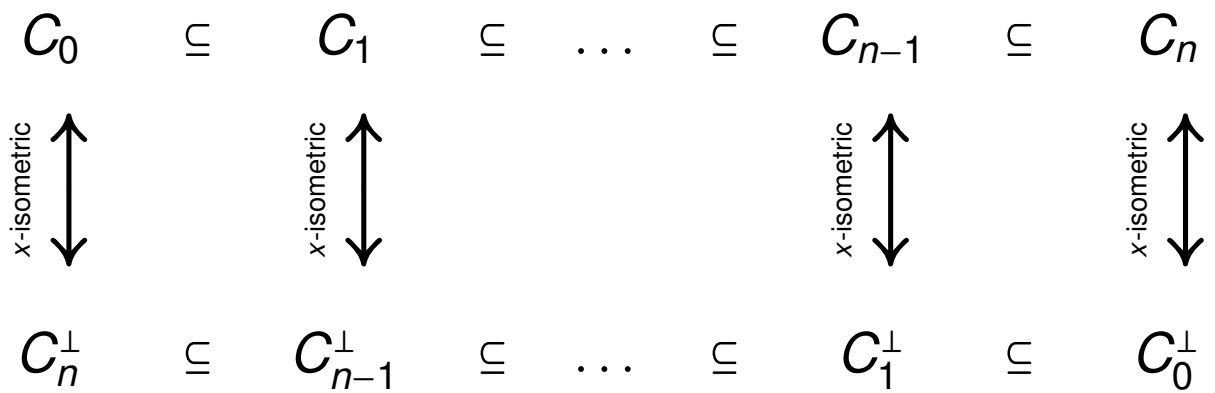
$$C_n^{\perp} \subseteq C_{n-1}^{\perp} \subseteq \cdots \subseteq C_1^{\perp} \subseteq C_0^{\perp}$$

Sequences of pairwise isometric codes

$$
\begin{array}{ccccccccc}
C_0 & \subseteq & C_1 & \subseteq & \cdots & \subseteq & C_{n-1} & \subseteq & C_n \\
\updownarrow & & \updownarrow & & & & \updownarrow & & \updownarrow \\
C_n^{\perp} & \subseteq & C_{n-1}^{\perp} & \subseteq & \cdots & \subseteq & C_1^{\perp} & \subseteq & C_0^{\perp}
\end{array}
$$

x-isometric

Sequences of pairwise isometric codes



A sequence of codes

$$C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{n-1} \subseteq C_n$$

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.

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.

$L(mQ)$ is the set of functions that only have poles in Q of order at most m.

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.

$L(mQ)$ is the set of functions that only have poles in Q of order at most m.

$$L(0Q) \subseteq L(1Q) \subseteq L(2Q) \subseteq L(3Q) \ldots$$

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.

$L(mQ)$ is the set of functions that only have poles in Q of order at most m.

$$L(0Q) \subseteq L(1Q) \subseteq L(2Q) \subseteq L(3Q) \ldots$$

Define

$$C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\}$$

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.

$L(mQ)$ is the set of functions that only have poles in Q of order at most m.

$$L(0Q) \subseteq L(1Q) \subseteq L(2Q) \subseteq L(3Q) \ldots$$

Define

$$C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\}$$

C_m is a linear code

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.

$L(mQ)$ is the set of functions that only have poles in Q of order at most m.

$$L(0Q) \subseteq L(1Q) \subseteq L(2Q) \subseteq L(3Q) \ldots$$

Define

$$C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\}$$

C_m is a linear code

We consider the sequence of codes

$$C_0 \subseteq C_1 \subseteq C_2 \subseteq C_3 \ldots$$

Sequences of pairwise isometric one-point AG codes

The Weierstrass semigroup at Q is now

$$\Lambda = \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\}.$$

Sequences of pairwise isometric one-point AG codes

The Weierstrass semigroup at Q is now

$$\Lambda = \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\}.$$

Consider

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

Sequences of pairwise isometric one-point AG codes

The Weierstrass semigroup at Q is now

$$\Lambda = \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\}.$$

Consider

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

Obviously, $\Lambda^* \subseteq \Lambda$.

Sequences of pairwise isometric one-point AG codes

The Weierstrass semigroup at Q is now

$$\Lambda = \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\}.$$

Consider

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

Obviously, $\Lambda^* \subseteq \Lambda$.

Theorem (Geil, Munuera, Ruano, Torres)

If $n > 2g + 2$, then

- $\Lambda + (\Lambda \setminus \Lambda^*) \subseteq (\Lambda \setminus \Lambda^*)$,

Sequences of pairwise isometric one-point AG codes

The Weierstrass semigroup at Q is now

$$\Lambda = \{0\} \cup \{m \in \mathbb{N} : L(mQ) \neq L((m-1)Q)\}.$$

Consider

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

Obviously, $\Lambda^* \subseteq \Lambda$.

Theorem (Geil, Munuera, Ruano, Torres)

If $n > 2g + 2$, then

- $\Lambda + (\Lambda \setminus \Lambda^*) \subseteq (\Lambda \setminus \Lambda^*)$,
- $\{0\}, C_{m_1}, \ldots, C_{m_n}$ *satisfies the isometry-dual condition* $\Leftrightarrow$ $\#\Lambda^* + 2g - 1 \in \Lambda^*$.

Theorem (Bras-Amorós, Hong, Duursma)

Let the sequence of one-point AG codes $\{0\}, C_{m_1}, \ldots, C_{m_n}$ *satisfy the isometry-dual condition and let* $m = m_n$*. Then the following holds.*

(a) $n \geqslant m + 1 - 2g$ *and the equality holds if* $m \geqslant 4g$*.*

(b) $n \leqslant \frac{m}{2} + \frac{3}{2}$ *if* $m \leqslant 4g - 1$*.*

Theorem (Bras-Amorós, Hong, Duursma)

Let the sequence of one-point AG codes $\{0\}, C_{m_1}, \ldots, C_{m_n}$ *satisfy the isometry-dual condition and let* $m = m_n$*. Then the following holds.*

(a) $n \geqslant m + 1 - 2g$ *and the equality holds if* $m \geqslant 4g$*.*

(b) $n \leqslant \dfrac{m}{2} + \dfrac{3}{2} \leqslant 2g + 1$ *if* $m \leqslant 4g - 1$*.*

Theorem (Bras-Amorós, Hong, Duursma)

Let the sequence of one-point AG codes $\{0\}, C_{m_1}, \ldots, C_{m_n}$ *satisfy the isometry-dual condition and let* $m = m_n$*. Then the following holds.*

(a) $n \geqslant m + 1 - 2g$ *and the equality holds if* $m \geqslant 4g$*.*

(b) $n \leqslant \dfrac{m}{2} + \dfrac{3}{2} \leqslant 2g + 1$ *if* $m \leqslant 4g - 1$*.*

So, $n \geqslant 2g + 2 \Longrightarrow m \geqslant 4g \Longrightarrow m = n - 1 + 2g$

Theorem (Bras-Amorós, Hong, Duursma)

Let the sequence of one-point AG codes $\{0\}, C_{m_1}, \ldots, C_{m_n}$ *satisfy the isometry-dual condition and let* $m = m_n$*. Then the following holds.*

(a) $n \geqslant m + 1 - 2g$ *and the equality holds if* $m \geqslant 4g$*.*

(b) $n \leqslant \dfrac{m}{2} + \dfrac{3}{2} \leqslant 2g + 1$ *if* $m \leqslant 4g - 1$*.*

So, $n \geqslant 2g + 2 \Longrightarrow m \geqslant 4g \Longrightarrow m = n - 1 + 2g$

Remark

The proof of the theorem uses a short semigroup argument.

Theorem (Bras-Amorós, Hong, Duursma)

Let the sequence of one-point AG codes $\{0\}, C_{m_1}, \ldots, C_{m_n}$ satisfy the isometry-dual condition and let $m = m_n$. Then the following holds.

(a) $n \geqslant m + 1 - 2g$ *and the equality holds if* $m \geqslant 4g$.

(b) $n \leqslant \frac{m}{2} + \frac{3}{2} \leqslant 2g + 1$ *if* $m \leqslant 4g - 1$.

So, $n \geqslant 2g + 2 \Longrightarrow m \geqslant 4g \Longrightarrow m = n - 1 + 2g$

Remark

The proof of the theorem uses a short semigroup argument. This theorem proves the previous theorem under the weaker condition $n \geqslant 2g + 2$.

Theorem (Bras-Amorós, Hong, Duursma)

Let the sequence of one-point AG codes $\{0\}, C_{m_1}, \ldots, C_{m_n}$ *satisfy the isometry-dual condition and let* $m = m_n$*. Then the following holds.*

(a) $n \geqslant m + 1 - 2g$ *and the equality holds if* $m \geqslant 4g$*.*

(b) $n \leqslant \frac{m}{2} + \frac{3}{2} \leqslant 2g + 1$ *if* $m \leqslant 4g - 1$*.*

So, $n \geqslant 2g + 2 \Longrightarrow m \geqslant 4g \Longrightarrow m = n - 1 + 2g$

Remark

The proof of the theorem uses a short semigroup argument.
This theorem proves the previous theorem under the weaker condition $n \geqslant 2g + 2$*.*
This last condition can not be improved: there exist sequences with $n = 2g + 1$ *and* $m < n + 2g - 1$*.*

Case genus $g = 3$ of Theorem [B-A,H,D]

All pairs (n, m) that pass the conditons of the theorem do occur. Pairs that occur for the Hermitian curve are marked $*$. Among the remaining pairs, pairs $*$ occur with a hyperelliptic curve. The remaining pairs $*$ occur with the Klein curve. [1]

	$m =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$n =$	1	*													
	2			*	*	*	*	*	*						
	3					*	*	*	*	*					
	4							*	*	*	*				
	5								*	*	*	*			
	6										*	*	*		
	7												*	*	
	8														*

[1] $(2, 6)$ uses the Klein curve over $GF(64)$

Puncturing a linear code C at position i is obtaining the linear code

$$C_i = \{(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) : c \in C\}.$$

Puncturing a linear code C at position i is obtaining the linear code

$$C_i = \{(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) : c \in C\}.$$

In general, puncturing of a code is the repetitive puncturing of the code at different positions.

Goal

Puncturing a linear code C at position i is obtaining the linear code

$$C_i = \{(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) : c \in C\}.$$

In general, puncturing of a code is the repetitive puncturing of the code at different positions.

Our goal: Analyze the effect of puncturing a sequence of AG codes satisfying the isometry-dual property in terms of the inheritance of this property.

Maximum sparse ideals of numerical semigroups

An ideal of a n.s. S is a subset of $I \subseteq S$ such that $I + S \subseteq I$.

Maximum sparse ideals of numerical semigroups

An ideal of a n.s. S is a subset of $I \subseteq S$ such that $I + S \subseteq I$.

Frobenius number or leader of $I = \max(\mathbb{N}_0 \setminus I)$.

Maximum sparse ideals of numerical semigroups

An ideal of a n.s. S is a subset of $I \subseteq S$ such that $I + S \subseteq I$.

Frobenius number or leader of $I = \max(\mathbb{N}_0 \setminus I)$.

Lemma

(BA, Lee, Vico-Oton) Frobenius number of $I \leqslant 2g - 1 + \#(S \setminus I)$.

Maximum sparse ideals of numerical semigroups

An ideal of a n.s. S is a subset of $I \subseteq S$ such that $I + S \subseteq I$.

Frobenius number or leader of $I = \max(\mathbb{N}_0 \setminus I)$.

Lemma

(BA, Lee, Vico-Oton) Frobenius number of $I \leqslant 2g - 1 + \#(S \setminus I)$.

I is a maximum sparse ideal if it attains this bound.

Maximum sparse ideals of numerical semigroups

An ideal of a n.s. S is a subset of $I \subseteq S$ such that $I + S \subseteq I$.

Frobenius number or leader of I $=\max(\mathbb{N}_0 \setminus I)$.

Lemma

(BA, Lee, Vico-Oton) Frobenius number of $I \leqslant 2g - 1 + \#(S \setminus I)$.

I is a maximum sparse ideal if it attains this bound.

Theorem (Geil, Munuera, Ruano, Torres, (revisited))

If $n > 2g + 2$, then

- $\Lambda \setminus \Lambda^*$ *is an ideal of* Λ,
- $\{0\}, C_{m_1}, \ldots, C_{m_n}$ *satisfies the isometry-dual condition* $\Leftrightarrow$ $\Lambda \setminus \Lambda^*$ *is maximum sparse.*

Maximum sparse ideals of numerical semigroups

An ideal of a n.s. S is a subset of $I \subseteq S$ such that $I + S \subseteq I$.

Frobenius number or leader of $I = \max(\mathbb{N}_0 \setminus I)$.

Lemma

(BA, Lee, Vico-Oton) Frobenius number of $I \leqslant 2g - 1 + \#(S \setminus I)$.

I is a maximum sparse ideal if it attains this bound.

Theorem (Geil, Munuera, Ruano, Torres, (revisited))

If $n \geqslant 2g + 2$, then

- $\Lambda \setminus \Lambda^*$ *is an ideal of* Λ,
- $\{0\}, C_{m_1}, \ldots, C_{m_n}$ *satisfies the isometry-dual condition* $\Leftrightarrow \Lambda \setminus \Lambda^*$ *is maximum sparse.*

Maximum sparse numerical semigroups

Theorem

Suppose I, I' are maximum sparse ideals of S, with leaders $\lambda_i, \lambda_{i'}$, the following are equivalent:

(1) $I' \supseteq I$

(2) $S \setminus I' \subseteq S \setminus I$

(3) $\lambda_i - \lambda_{i'} \in S$

(4) $\#(S \setminus I) - \#(S \setminus I') \in S$

Puncturing sequences of isometry-dual one-point AG codes

Theorem

Suppose that $\Lambda^* = \{m_0 = 0, m_1, \ldots, m_n\}$ *and suppose that the sequence* $\{0\}, C_{m_1}, C_{m_2}, \ldots, C_{m_n}$ *as just defined satisfies the isometry-dual condition.*

Puncturing sequences of isometry-dual one-point AG codes

Theorem

Suppose that $\Lambda^* = \{m_0 = 0, m_1, \ldots, m_n\}$ *and suppose that the sequence* $\{0\}, C_{m_1}, C_{m_2}, \ldots, C_{m_n}$ *as just defined satisfies the isometry-dual condition.*
Let $\{P_{i_1}, \ldots, P_{i_{n'}}\} \subseteq \{P_1, \ldots, P_n\}$, *with* $2g + 2 \geqslant n' < n$.

Puncturing sequences of isometry-dual one-point AG codes

Theorem

Suppose that $\Lambda^* = \{m_0 = 0, m_1, \ldots, m_n\}$ *and suppose that the sequence* $\{0\}, C_{m_1}, C_{m_2}, \ldots, C_{m_n}$ *as just defined satisfies the isometry-dual condition.*
Let $\{P_{i_1}, \ldots, P_{i_{n'}}\} \subseteq \{P_1, \ldots, P_n\}$, *with* $2g + 2 \geqslant n' < n$.
Define

$$C'_m = \{(f(P_{i_1}), \ldots, f(P_{i_{n'}})) : f \in L(mQ)\}$$

Puncturing sequences of isometry-dual one-point AG codes

Theorem

Suppose that $\Lambda^* = \{m_0 = 0, m_1, \ldots, m_n\}$ *and suppose that the sequence* $\{0\}, C_{m_1}, C_{m_2}, \ldots, C_{m_n}$ *as just defined satisfies the isometry-dual condition.*
Let $\{P_{i_1}, \ldots, P_{i_{n'}}\} \subseteq \{P_1, \ldots, P_n\}$, *with* $2g + 2 \geqslant n' < n$.
Define

$$C'_m = \{(f(P_{i_1}), \ldots, f(P_{i_{n'}})) : f \in L(mQ)\}$$

and

$$(\Lambda^*)' = \{0\} \cup \{m \in \mathbb{N}, m > 0 : C'_m \neq C'_{m-1}\} = \{m'_1 = 0, m'_2, \ldots, m'_{n'}\}.$$

Puncturing sequences of isometry-dual one-point AG codes

Theorem

Suppose that $\Lambda^* = \{m_0 = 0, m_1, \ldots, m_n\}$ *and suppose that the sequence* $\{0\}, C_{m_1}, C_{m_2}, \ldots, C_{m_n}$ *as just defined satisfies the isometry-dual condition.*
Let $\{P_{i_1}, \ldots, P_{i_{n'}}\} \subseteq \{P_1, \ldots, P_n\}$, *with* $2g + 2 \geqslant n' < n$.
Define

$$C'_m = \{(f(P_{i_1}), \ldots, f(P_{i_{n'}})) : f \in L(mQ)\}$$

and

$$(\Lambda^*)' = \{0\} \cup \{m \in \mathbb{N}, m > 0 : C'_m \neq C'_{m-1}\} = \{m'_1 = 0, m'_2, \ldots, m'_{n'}\}.$$

If the sequence $\{0\}, C'_{m'_1}, C'_{m'_2}, \ldots, C_{m'_{n'}}$ *satisfies the isometry-dual condition, then* $n - n' \in \Lambda$.

Hermitian curve $\mathcal{H}/\mathbb{F}_{q^2}$ $(x^{q+1} = y^q + y)$

$\mathbb{F}_4 = \mathbb{F}[\alpha] = (\mathbb{F}_2[x])/(x^2 + x + 1)$.

$\mathcal{H}/\mathbb{F}_4 = \{P_1 = (0,0), P_2 = (\alpha,\alpha), P_3 = (\alpha+1,\alpha), P_4 = (1,\alpha), P_5 = (\alpha,\alpha+1), P_6 = (\alpha+1,\alpha+1), P_7 = (1,\alpha+1), P_8 = (0,1)\} \cup \{P_\infty\}$.

$\Lambda_{P_\infty} = \{0, 2, 3, 4, 5, 6, \dots\}$

Basis of $\cup_{m\geqslant 0} L(mP_\infty) =$
$\{1, x, y, x^2, xy, x^3, x^2y, x^4, x^3y, x^5, x^4y, x^6, x^5y, x^7, x^6y, x^8, x^7y, \dots\}$.

For each $\mathcal{P} \subseteq \{P_1, \dots, P_8\}$ analyze whether $\#\mathcal{P} + 2g - 1 \in (\Lambda^*)'$.

If $n \geqslant 2g + 2$ this corresponds to the isometry-dual condition.

Hermitian curve $\mathcal{H}/\mathbb{F}_{q^2}$ $(x^{q+1} = y^q + y)$

